MANUAL

Manual de legislación europea en materia de la protección de datos

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

El manuscrito de este manual fue finalizado en abril de 2014.
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 y en la página web del Tribunal Europeo de Derechos Humanos en el menú Jurisprudencia en: echr.coe.int.

Europe Direct es un servicio que le ayudará a encontrar respuestas a sus preguntas sobre la Unión Europea

Número de teléfono gratuito (*):

00 800 6 7 8 9 10 11

(*) Tanto la información como la mayoría de las llamadas (excepto desde algunos operadores, cabinas u hoteles) son gratuitas.

Fotografía (Cubierta e interior): © iStockphoto

Más información sobre la Unión Europea, en el servidor Europa de Internet (http://europa.eu).

Al final de la obra figura una ficha catalográfica.

Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2014

ISBN 978-92-871-9948-5 (CdE)
ISBN 978-92-9239-330-4 (FRA)
doi:10.2811/53770

Printed in Belgium

Impreso en papel reciclado sin cloro (PCF)

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

Manual de legislación europea en materia de la protección de datos

Preámbulo

El presente manual de legislación europea en materia de protección de datos ha sido preparado conjuntamente por la Agencia de los Derechos Fundamentales de la Unión Europea (FRA) y la Secretaría del Tribunal Europeo de Derechos Humanos. Se trata del tercer ejemplar de una serie de manuales jurídicos conjuntamente elaborados por la FRA y el Consejo de Europa. En marzo de 2011, se publicó un primer manual de legislación europea contra la discriminación y, en junio de 2013, fue publicado un segundo manual de legislación europea en materia de asilo, inmigración y fronteras.

Decidimos proseguir nuestra colaboración en relación con este tema de candente actualidad que nos afecta diariamente a todos, en concreto, en materia de la protección de los datos personales. Europa goza de uno de los sistemas de mayor protección en este ámbito, sistema que está basado en el Convenio nº 108 del Consejo de Europa, los instrumentos de la Unión Europea (UE), así como en la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) y del Tribunal de Justicia de la Unión Europea (TJUE).

El propósito del presente documento es contribuir a concienciar y mejorar el conocimiento sobre las normas en materia de protección de datos en la Unión Europea y los Estados miembros del Consejo de Europa, y servir como el principal punto de referencia al que pueden acudir los lectores. Está destinado a profesionales jurídicos no especializados, jueces, autoridades nacionales encargadas de la protección de datos y otras personas que trabajan en el ámbito de la protección de datos.

Con la entrada en vigor del Tratado de Lisboa en diciembre de 2009, la Carta de Derechos Fundamentales de la UE pasó a ser jurídicamente vinculante y, con ello, se elevó el derecho a la protección de los datos personales a la categoría de derecho fundamental independiente. Para la protección de este derecho fundamental, resulta crucial contar con una mejor comprensión del Convenio nº 108 del Consejo de Europa y de los instrumentos de la UE, que prepararon el camino para la protección de datos en Europa, así como la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos.

Nos gustaría agradecer al Instituto Ludwig Boltzmann de Derechos Humanos por su contribución en la redacción de este manual. Asimismo expresamos nuestra gratitud al Supervisor Europeo de Protección de Datos por sus comentarios en el proceso de redacción del texto. Agradecemos especialmente a la Unidad de Protección de

Datos de la Comisión Europea por su apoyo durante la preparación de este manual. Finalmente, nos gustaría agradecer también a la Agencia Española de Protección de Datos, que llevó a cabo la revisión de la traducción del manual al español.

Philippe Boillat
Director General
de Derechos Humanos
y el Estado de Derecho
Consejo de Europa

Morten Kjaerum
Director
de la Agencia de los Derechos
Fundamentales
de la Unión Europea

Índice

PREÁMBULO 3

ABREVIATURAS Y ACRÓNIMOS 9

CÓMO UTILIZAR ESTE MANUAL 11

1. CONTEXTO Y ANTECEDENTES DE LA LEGISLACIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS 13
   - 1.1. El derecho a la protección de los datos 14
   - Puntos clave 14
     - 1.1.1. El Convenio Europeo de Derechos Humanos 14
     - 1.1.2. Convenio nº 108 del Consejo de Europa 15
     - 1.1.3. Legislación sobre protección de datos de la Unión Europea 18
   - 1.2. Ponderación entre derechos 22
   - Puntos clave 22
     - 1.2.1. Libertad de expresión 24
     - 1.2.2. Acceso a los documentos 28
     - 1.2.3. Libertad de las artes y de las ciencias 32
     - 1.2.4. Protección de la propiedad 34

2. TERMINOLOGÍA DE PROTECCIÓN DE DATOS 37
   - 2.1. Datos personales 38
   - Puntos clave 38
     - 2.1.1. Principales aspectos del concepto de datos personales 39
     - 2.1.2. Categorías especiales de datos personales 46
     - 2.1.3. Datos anonimizados y pseudonimizados 47
   - 2.2. Tratamiento de datos 50
   - Puntos clave 50
   - 2.3. Los usuarios de los datos personales 52
   - Puntos clave 52
     - 2.3.1. Responsables del tratamiento y encargados del tratamiento 53
     - 2.3.2. Destinatarios y terceros 59
   - 2.4. Consentimiento 60
   - Puntos clave 60
     - 2.4.1. Los elementos del consentimiento válido 61
     - 2.4.2. El derecho a revocar el consentimiento en cualquier momento 66

3. PRINCIPIOS CLAVE DE LA LEGISLACIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS 67
3.1. El principio de tratamiento lícito 68
Puntos clave 68
3.1.1. Los requisitos para una injerencia justificada con arreglo al CEDH 69
3.1.2. Las condiciones de las limitaciones lícitas con arreglo a la Carta de la UE 72
3.2. Los principios de finalidad y de limitación de la finalidad 74
Puntos clave 74
3.3. Principios de calidad de los datos 77
Puntos clave 77
3.3.1. El principio de pertinencia de los datos 77
3.3.2. El principio de exactitud de los datos 78
3.3.3. El principio de conservación de los datos 80
3.4. El principio de tratamiento leal 80
Puntos clave 80
3.4.1. Transparencia 81
3.4.2. Establecer confianza 82
3.5. El principio de rendición de cuentas 83
Puntos clave 83

4. LAS NORMAS DE LA LEGISLACIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS 85
4.1. Normas relativas al tratamiento lícito 87
Puntos clave 87
4.1.1. Tratamiento lícito de los datos no sensibles 87
4.1.2. Tratamiento lícito de los datos sensibles 94
4.2. Normas relativas a la seguridad del tratamiento 97
Puntos clave 97
4.2.1. Elementos de la seguridad de datos 98
4.2.2. Confidencialidad 101
4.3. Normas relativas a la transparencia del tratamiento 103
Puntos clave 103
4.3.1. Información 104
4.3.2. Notificación 107
4.4. Normas para promover el cumplimiento 108
Puntos clave 108
4.4.1. Controles previos 108
4.4.2. Delegados de protección de datos personales 109
4.4.3. Códigos de conducta 110

5. LOS DERECHOS DEL INTERESADO Y SU APLICACIÓN 113
5.1. Los derechos de los interesados 115
Puntos clave 115
5.1.1. Derecho de acceso 116
5.1.2. Derecho de oposición 123
5.2. Supervisión independiente 125
Puntos clave 125
5.3. Recursos y sanciones 130
Puntos clave 130
5.3.1. Peticiones al responsable del tratamiento 131
5.3.2. Reclamaciones ante una autoridad de supervisión 132
5.3.3. Interposición de una reclamación ante un tribunal 134
5.3.4. Sanciones 139

6. FLUJOS TRANSFRONTERIZOS DE DATOS 141
6.1. Naturaleza de los flujos transfronterizos de datos 142
Puntos clave 142
6.2. Libre circulación de datos entre los Estados miembros o entre las Partes Contratantes 144
Puntos clave 144
6.3. Libre circulación de datos a terceros países 145
Puntos clave 145
6.3.1. Libre circulación de datos debido a la existencia de una protección adecuada 146
6.3.2. Libre circulación de datos en casos específicos 148
6.4. Circulación limitada de datos a terceros países 149
Puntos clave 149
6.4.1. Cláusulas contractuales 150
6.4.2. Normas Corporativas Vinculantes 152
6.4.3. Acuerdos internacionales especiales 152

7. PROTECCIÓN DE DATOS EN EL CONTEXTO DE LA POLICÍA Y JUSTICIA PENAL 157
7.1. Derecho del CdE sobre la protección de datos en los asuntos de la policía y justicia penal 158
Puntos clave 158
7.1.1. La Recomendación sobre la policía 159
7.1.2. El Convenio de Budapest sobre la Ciberdelincuencia 162
7.2. Derecho de la UE sobre la protección de datos en asuntos policiales y penales 163
Puntos clave 163

7.2.1. La Decisión marco de protección de datos 164
7.2.2. Instrumentos jurídicos más específicos en materia de protección de datos en la cooperación transfronteriza en materia policial y de aplicación de la ley 166
7.2.3. La protección de datos en EUROPOL y EUROJUST 168
7.2.4. Protección de datos en los sistemas comunes de información a escala de la UE 171

8. OTRAS LEGISLACIONES EUROPEAS ESPECÍFICAS EN MATERIA DE PROTECCIÓN DE DATOS 181
8.1. Comunicaciones electrónicas 182
Puntos clave 182
8.2. Datos de empleo 187
Puntos clave 187
8.3. Datos médicos 190
Puntos clave 190
8.4. Tratamiento de datos con fines estadísticos 193
Puntos clave 193
8.5. Datos financieros 196
Puntos clave 196

BIBLIOGRAFÍA RECOMENDADA 199

JURISPRUDENCIA 205
Jurisprudencia seleccionada del Tribunal Europeo de Derechos Humanos 205
Jurisprudencia seleccionada del Tribunal de Justicia de la Unión Europea 209

ÍNDICE DE JURISPRUDENCIA 213

Abreviaturas y acrónimos

ACC	Autoridad Común de Control
AELC	Asociación Europea de Libre Comercio
AEVM	Autoridad Europea de Valores y Mercados
BCR	Normas corporativas vinculantes
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
CETS	Series de Tratados del Consejo de Europa
CIS	Sistema de Información Aduanera
Convenio nº 108	Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Consejo de Europa)
CRM	Gestión de relaciones con clientes
C-SIS	Sistema Central de Información de Schengen
DUDH	Declaración Universal de Derechos Humanos
EEE	Espacio Económico Europeo
ENISA	Agencia Europea de Seguridad de las Redes y de la Información
eTEN	Redes transeuropeas de telecomunicación
eu-LISA	Agencia europea para la gestión de sistemas informáticos de gran magnitud
EuroPriSe	Sello europeo de privacidad
FRA	Agencia de los Derechos Fundamentales de la Unión Europea
GPS	Sistema de posicionamiento global
N-SIS	Sistema Nacional de Información de Schengen

OEDE	Orden Europea de Detención y Entrega
ONU	Organización de las Naciones Unidas
ONG	Organización no gubernamental
OCDE	Organización de Cooperación y Desarrollo Económicos
PIN	Número de identificación personal
PNR	Registro de Nombres de Pasajeros
SEPA	Zona única de pagos en euros
SEPD	Supervisor Europeo de Protección de Datos
SIS	Sistema de Información de Schengen
SWIFT	Sociedad de Telecomunicaciones Interbancarias Mundiales
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TJUE	Tribunal de Justicia de la Unión Europea (antes de diciembre de 2009, se llamaba Tribunal de Justicia Europeo, TJE)
TUE	Tratado de la Unión Europea
UE	Unión Europea
UNE	Unidad Nacional de Europol
VIS	Sistema de Información de Visados

Cómo utilizar este manual

En este manual se brinda una perspectiva general de la legislación aplicable en materia de protección de datos en relación con la Unión Europea (UE) y el Consejo de Europa (CdE).

Está destinado a ayudar a los profesionales del Derecho no especializados en el ámbito de la protección de datos, a los abogados, jueces y otros profesionales, así como a las personas que trabajan para otros organismos, incluidas las organizaciones no gubernamentales (ONG), a quienes pueden planteárseles preguntas jurídicas relacionadas con la protección de los datos.

Constituye un primer punto de referencia tanto para la legislación europea como para el Convenio Europeo de Derechos Humanos (CEDH) sobre la protección de datos y explica el modo en que se regula este ámbito, al amparo de la legislación europea y del CEDH, así como del Convenio del CdE para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio nº 108) y otros instrumentos del CdE. Cada capítulo presenta, en primer lugar, un único recuadro con las disposiciones jurídicas aplicables, en el cual se incluye la jurisprudencia seleccionada destacada, al amparo de los dos sistemas jurídicos europeos separados. A continuación, se presentan las correspondientes normativas de estos dos ordenamientos europeos, uno detrás del otro, según la materia para la que resulten aplicables. Esto permite al lector ver las diferencias y las similitudes entre los dos sistemas jurídicos.

En los recuadros del inicio de cada capítulo se enumeran los temas que se abordan en dicho capítulo y se especifican las disposiciones jurídicas aplicables, así como el resto de materiales pertinentes, como la jurisprudencia. Si se considera pertinente para realizar una presentación concisa del contenido del capítulo, podrá modificarse ligeramente el orden de los temas en relación con la estructura del texto del capítulo. Los recuadros contemplan tanto el Derecho del CdE como de la UE, lo cual ayuda a que los usuarios encuentren la información clave relacionada con su situación, en especial si únicamente quedan sujetos a la legislación del CdE.

Los abogados de los Estados no miembros que sean Estados miembros del CdE y partes del CEDH y el Convenio nº 108 pueden acceder a la información correspondiente a su propio país, consultando directamente los apartados relativos al CdE. 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. Las personas que precisen más información sobre un tema en

particular, podrán encontrar una lista de referencias de material más especializado en el apartado «Bibliografía recomendada» del manual.

El Derecho del CdE se presenta mediante breves referencias a los asuntos seleccionados del Tribunal Europeo de Derechos Humanos (TEDH), que han sido elegidos entre el gran número de sentencias y resoluciones del TEDH existentes en materia de protección de datos.

El Derecho de la UE está compuesto por las medidas legislativas que han sido adoptadas, en las correspondientes disposiciones de los Tratados y en la Carta de los Derechos Fundamentales de la Unión Europea, tal como han sido interpretadas por la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE), cuya denominación antes de 2009, era Tribunal de Justicia Europeo (TJE).

La jurisprudencia citada o descrita en este manual ofrece ejemplos del importante corpus de jurisprudencia del TEDH y del TJEU. Las directrices incluidas al final del presente manual tienen por objeto ayudar al lector en sus búsquedas de jurisprudencia en línea.

Además, en los recuadros de texto se ofrecen ejemplos prácticos con situaciones hipotéticas, para ilustrar mejor la aplicación práctica de las normas europeas en materia de protección de datos, en especial cuando no existe una jurisprudencia específica en la materia del TEDH ni del TJUE.

El manual comienza con una breve descripción del papel de los dos sistemas jurídicos, tal como establece el TEDH y en la legislación europea (capítulo 1). En los capítulos 2 a 8 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 normas de la legislación europea en materia de protección de datos;
- los derechos de los interesados y su observancia;
- los flujos transfronterizos de datos;
- la protección de datos en el contexto de la policía y justicia penal;
- otras legislaciones europeas específicas en materia de protección de datos.

1

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

UE	Materias cubiertas	CdE
Derecho a la protección de los datos		
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 de protección de datos*), DO 1995 L 281		CEDH, artículo 8 (derecho al respeto a la vida privada y familiar, el domicilio y la correspondencia) Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio nº 108)
Ponderación entre derechos		
TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen*, 2010	En general	
TJUE, asunto C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy y Satamedia Oy*, 2008	Libertad de expresión	TEDH, *Axel Springer AG contra Alemania*, 2012 TEDH, *Mosley contra el Reino Unido*, 2011
	Libertad de las artes y de las ciencias	TEDH, *Vereinigung bildender Künstler contra Austria*, 2007
TJUE, asunto C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU*, 2008	Protección de la propiedad	
TJUE, asunto C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd*, 2010	Acceso a los documentos	TEDH, *Társaság a Szabadságjogokért contra Hungría*, 2009

1.1. El derecho a la protección de los datos

Puntos clave

- De conformidad con el artículo 8 del CEDH, el derecho a la protección contra la recopilación y el uso de los datos personales forma parte del derecho al respeto a la vida privada y familiar, el domicilio y la correspondencia.
- El Convenio nº 108 del CdE es el primer instrumento internacional jurídicamente vinculante que aborda explícitamente la protección de datos.
- En el Derecho de la UE, la protección de datos fue regulada por primera vez en la Directiva de protección de datos.
- En el Derecho de la UE, la protección de datos ha sido reconocida como un derecho fundamental.

En el artículo 12 de la Declaración Universal de Derechos Humanos (DUDH) de las Naciones Unidades de 1948, sobre el respeto a la vida privada y familiar, se estableció por primera vez en un instrumento jurídico internacional un derecho a la protección de la esfera privada de las personas frente a la intrusión de otros, especialmente del Estado.[1] La DUDH influyó en el desarrollo de otros instrumentos de derechos humanos en Europa.

1.1.1. El Convenio Europeo de Derechos Humanos

El Consejo de Europea se formó después de la Segunda Guerra Mundial con el fin de reunir a los Estados de Europa para promocionar el Estado de derecho, la democracia, los derechos humanos y el desarrollo social. Para ello, adoptó el Convenio Europeo de Derechos Humanos (CEDH) en 1950, el cual entró en vigor en 1953.

Los Estados tienen la obligación internacional de cumplir el CEDH. Todos los Estados miembros del CdE ya han incorporado o aplicado el CEDH en su legislación nacional, lo cual les exige que actúen de conformidad con las disposiciones del Convenio.

Para garantizar que las Partes Contratantes cumplan sus obligaciones de conformidad con el CEDH, se creó en 1959 el Tribunal Europeo de Derechos Humanos (TEDH) en Estrasburgo, Francia. El TEDH garantiza que los Estados cumplen sus obligaciones,

1 Declaración Universal de Derechos Humanos (DUDH) de las Naciones Unidas (ONU), 10 de diciembre de 1948.

de conformidad con el Convenio, considerando las demandas de personas físicas, grupos de personas físicas, ONG o personas jurídicas que denuncian violaciones del Convenio. En 2013, el Consejo de Europa estaba compuesto por 47 Estados miembros, 28 de los cuales también son Estados miembros de la UE. No es necesario que los demandantes ante el TEDH sean nacionales de uno de los Estados miembros. El TEDH también puede examinar asuntos interestatales presentados por uno o más Estados miembros del CdE contra otro Estado miembro.

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 vida privada y familiar, el domicilio y la correspondencia y determina las condiciones bajo las cuales podrían ser aceptables las limitaciones a ese derecho.[2]

En toda su jurisprudencia, el TEDH ha examinado muchas situaciones en las cuales se planteó la cuestión de la protección de datos, en particular aquellas relacionadas con la intercepción de las comunicaciones,[3] diversas formas de vigilancia[4] y la protección contra el almacenamiento de datos personales por parte de las autoridades públicas.[5] 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 sino también que, en determinadas circunstancias, tienen la obligación positiva de garantizar activamente el respeto efectivo a la vida privada y familiar.[6] En los correspondientes capítulos, se hará una referencia detallada a muchos de estos asuntos.

1.1.2. Convenio nº 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, que hacen referencia al artículo 8 del

2 Consejo de Europa, Convenio Europeo de Derechos Humanos, CETS nº 005, 1950.

3 Véase, por ejemplo, TEDH, *Malone contra el Reino Unido*, nº 8691/79, de 2 de agosto de 1984; TEDH, *Copland contra el Reino Unido*, nº 62617/00, de 3 de abril de 2007.

4 Véase, por ejemplo, TEDH, *Klass y otros contra Alemania*, nº 5029/71, de 6 de septiembre de 1978; TEDH, *Uzun contra Alemania*, nº 35623/05, de 2 de septiembre de 2010.

5 Véase, por ejemplo, TEDH, *Leander contra Suecia*, nº 9248/81, de 26 de marzo de 1987; TEDH, *S. and Marper contra el Reino Unido*, nº 30562/04 y 30566/04, de 4 de diciembre de 2008.

6 Véase, por ejemplo, TEDH, *I. contra Finlandia*, nº 20511/03, de 17 de julio de 2008; TEDH, *K.U. contra Finlandia*, nº 2872/02, de 2 de diciembre de 2008.

CEDH.[7] 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 (Convenio nº 108).[8] El Convenio nº 108 fue, y sigue siendo, el único instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos.

El Convenio nº 108 se aplica a todo el procesamiento de datos llevado a cabo tanto por el sector privado como público, por ejemplo el procesamiento de datos que realizan las autoridades judiciales y policiales. Protege a las personas físicas contra los abusos que pueden conllevar la recogida y el tratamiento de datos personales, a la vez que busca regular los flujos transfronterizos de datos. Por lo que a la recopilación y al tratamiento de datos personales se refiere, los principios establecidos en el Convenio afectan, en particular, a la recogida y al tratamiento automatizado leales y lícitos, a que los datos sean almacenados para fines específicos legítimos y no para un uso con fines incompatibles con estas finalidades y a que no sean conservados durante un periodo más largo de lo necesario. También conciernen a la calidad de los datos, en particular que deben ser adecuados, pertinentes y no excesivos (proporcionalidad), así como exactos.

Además de proporcionar garantías relacionadas con la recopilación y el tratamiento de datos personales, prohíbe, si no se dan garantías jurídicas adecuadas, el tratamiento de los datos «sensibles», tales 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, que puedan obtener su rectificación. Las limitaciones de los derechos establecidos en el Convenio únicamente son posibles cuando estén en juego intereses superiores, como la seguridad o la defensa del Estado.

Aunque el Convenio establece la libre circulación de los datos personales entre los Estados Parte del Convenio, también impone algunas limitaciones a los flujos dirigidos a Estados en que la normativa legal no establece una protección equivalente.

7 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 respecto de los bancos de datos electrónicos en el sector público, de 20 de septiembre de 1974.

8 Consejo de Europa, Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Consejo de Europa, CETS nº 108, 1981.

Para un mayor desarrollo de los principios generales y las normas establecidas en el Convenio nº 108, el Comité de Ministros del CdE ha adoptado diversas recomendaciones que no son jurídicamente vinculantes (véanse los capítulos 7 y 8).

Todos los Estados miembros de la Unión Europea han ratificado el Convenio nº 108. En 1999, el Convenio nº 108 fue modificado para permitir que la UE fuera Parte del mismo.[9] En 2001, se adoptó un Protocolo Adicional al Convenio nº 108, que introdujo disposiciones sobre los flujos transfronterizos de datos a los Estados no parte, los denominados terceros países, y sobre el establecimiento obligatorio de autoridades nacionales de supervisión de la protección de los datos.[10]

Perspectivas

A raíz de la decisión de modernizar el Convenio nº 108, la consulta pública realizada en 2011 hizo posible confirmar los dos objetivos principales de dicho trabajo, a saber, reforzar la protección de la privacidad en el ámbito digital y fortalecer el mecanismo de seguimiento del convenio.

El Convenio nº 108 está abierto a la adhesión de los Estados no miembros del CdE, incluidos los países no europeos. El potencial del Convenio como norma universal y su carácter abierto podrían servir como base para promover la protección de datos a escala mundial.

Hasta el momento, 45 de las 46 Partes Contratantes del Convenio nº 108 son Estados miembros del CdE. Uruguay, fue el primer país no europeo que se adhirió en agosto de 2013 y Marruecos, a quien el Comité de Ministros ha invitado a adherirse al Convenio nº 108, está en proceso de formalizar su adhesión.

9 Consejo de Europa, Modificaciones del Convenio para la protección de las personas en relación con el tratamiento automatizado de datos de carácter personal (CETS nº 108) para permitir la adhesión de las Comunidades Europeas, adoptado por el Comité de Ministros, en Estrasburgo, el 15 de junio de 1999; artículo 23, apartado 2, del Convenio nº 108 en su forma modificada.

10 Consejo de Europa, Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencia de datos, en lo que respecta a las autoridades de control y los flujos transfronterizos de datos, CETS nº 181, 2001.

1.1.3. Legislación sobre protección de datos de la Unión Europea

El Derecho de la UE está compuesto por los Tratados y el Derecho europeo derivado. Los tratados, en concreto el Tratado de la Unión Europea (TUE) y el Tratado de Funcionamiento de la Unión Europea (TFUE), han sido aprobados por todos los Estados miembros de la UE; también se les denomina el «Derecho primario de la Unión Europea». Los reglamentos, las directivas y las decisiones de la UE han sido adoptados por las instituciones de la UE, a las cuales se les ha concedido dicha autoridad en virtud de los tratados; a estos instrumentos también se les denomina «Derecho derivado de la UE».

El principal instrumento jurídico de la UE en materia de protección de datos es 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 de protección de datos*).[11] Fue adoptada en 1995, en un momento en que diversos Estados miembros ya habían adoptado legislaciones nacionales en materia de protección de datos. La libre circulación de bienes y servicios, capitales y personas en el mercado interior exige la libre circulación de datos, la cual no podría llevarse a cabo salvo que los Estados miembros puedan confiar en un nivel elevado y uniforme de protección de datos.

Dado que el objetivo de adoptar la Directiva de protección de datos fue la armonización[12] de la legislación en materia de protección de datos a escala nacional, la Directiva presenta un grado de especificidad comparable al de las legislaciones existentes (en aquel entonces) en materia de protección de datos. Para el TJUE, "la Directiva 95/46 tiene por objeto (...) equiparar el nivel de protección de los derechos y libertades de las personas por lo que se refiere al tratamiento de datos personales en todos los Estados miembros. (...) La aproximación de las legislaciones nacionales en la materia no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Unión. Desde este punto de vista, (...) la armonización de dichas legislaciones nacionales no se limita a una armonización mínima, sino que constituye,

11 Directiva de protección de datos, DO 1995 L 281, p. 31.

12 Véase, por ejemplo, la Directiva de protección de datos, considerandos 1, 4, 7 y 8.

en principio, una armonización completa".[13] Por consiguiente, los Estados miembros únicamente tienen un limitado margen de maniobra a la hora de aplicar la Directiva.

La Directiva de protección de datos está diseñada para dar contenido a los principios del derecho a la privacidad ya contemplados en el Convenio nº 108, así como para ampliarlos. El hecho de que, en 1995, todos los 15 Estados miembros de la UE también fueran Partes Contratantes del Convenio nº 108 excluye la adopción de normas contradictorias entre estos dos instrumentos jurídicos. La Directiva de protección de datos, sin embargo, ofrece la posibilidad, contemplada en el artículo 11 del Convenio nº 108, de añadir instrumentos de protección. En particular, la introducción de una supervisión independiente como instrumento de mejora del cumplimiento de las normas de protección de datos demostró ser una importante aportación al eficaz funcionamiento de la legislación europea en materia de protección de datos. (Por consiguiente, esta característica fue adoptada en el Derecho del CdE en 2001 a través del Protocolo adicional al Convenio nº 108).

La aplicación territorial de la Directiva de protección de datos se amplía más allá de los 28 Estados miembros de la UE, incluyendo también a los Estados no miembros de la UE que forman parte del Espacio Económico Europeo (EEE)[14] – en concreto, Islandia, Liechtenstein y Noruega.

El TJUE de Luxemburgo tiene competencia para establecer si un Estado miembro ha cumplido sus obligaciones con arreglo a la Directiva de protección de datos y para pronunciarse con carácter prejudicial respecto de la validez y la interpretación de la Directiva, a fin de garantizar su aplicación uniforme y efectiva en los Estados miembros. Una excepción importante a la aplicabilidad de la Directiva de protección de datos es la denominada excepción doméstica, en concreto, el tratamiento de datos personales por parte de particulares con fines exclusivamente personales o domésticos.[15] Dicho tratamiento se considera, por lo general, parte de las libertades de los particulares.

En consonancia con el Derecho primario de la UE vigente en el momento de la adopción de la Directiva de protección de datos, el ámbito de aplicación material de la Directiva se limita a las cuestiones del mercado interior. Las cuestiones que quedan

13 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*, de 24 de noviembre de 2011, apdos. 28-29.

14 Acuerdo sobre el Espacio Económico Europeo, DO 1994 L 1, el cual entró en vigor el 1 de enero de 1994.

15 Directiva de protección de datos, artículo 3, apartado 2, segundo guión.

fuera de su ámbito de aplicación son, en su mayoría, asuntos de la cooperación en materia de policía y justicia penal. La protección de datos en relación con estas cuestiones deriva de distintos instrumentos jurídicos, que se describen detalladamente en el capítulo 7.

Dado que la Directiva de protección de datos solo podía estar dirigida a los Estados miembros de la UE, era necesario adoptar un instrumento jurídico adicional para establecer la protección de datos para el tratamiento de datos personales por parte de las instituciones y organismos de la UE. El Reglamento (CE) nº 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.[16]

De forma adicional, incluso en los ámbitos amparados por la Directiva de protección de datos, se necesitan con frecuencia disposiciones en materia de protección de datos más detalladas para conseguir la claridad necesaria a la hora de ponderar otros intereses legítimos. Dos ejemplos son 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 (*Directiva sobre la privacidad y las comunicaciones electrónicas*)[17] y la Directiva 2006/24/CE sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (*Directiva sobre la conservación de datos,* invalidada el 8 de abril de 2014).[18] En el capítulo 8 se discutirán otros ejemplos. Dichas disposiciones deben ser conformes con la Directiva de protección de datos.

16 Reglamento (CE) nº 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.

17 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 privacidad y las comunicaciones electrónicas*), DO 2002 L 201.

18 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, *(Directiva de conservación de datos),* DO 2006 L 105), invalidada el 8 de abril de 2014.

La Carta de los Derechos Fundamentales de la Unión Europea

Los tratados originarios de las Comunidades Europeas no incluían ninguna referencia a los derechos humanos ni a su protección. Posteriormente se desarrolló, sin embargo, un nuevo enfoque gracias al hecho de que se presentaron asuntos ante el entonces Tribunal de Justicia Europeo (TJE) en los que se alegaban violaciones de los derechos humanos en materias incluidas en el ámbito del Derecho de la UE. Para conceder protección a las personas físicas, los derechos fundamentales fueron incorporados 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 garantizaría que el Derecho de la UE cumple con estos principios.

Reconociendo que sus políticas podrían tener un impacto sobre los derechos humanos y en un esfuerzo para que los ciudadanos se sientan «más cerca» de la UE, la UE proclamó en 2000 la Carta de Derechos Fundamentales de la Unión Europea (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 agrupan en seis secciones: dignidad, libertad, igualdad, solidaridad, ciudadanía y justicia.

Aunque en su origen la Carta era únicamente un documento político, pasó a ser jurídicamente vinculante[19] 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.[20]

El Derecho primario de la UE también incluye una competencia general de la UE para legislar en materia de protección de datos (artículo 16 del TFUE).

La Carta no solo garantiza el respeto a la vida privada y familiar (artículo 7), sino que también establece el derecho a la protección de datos (artículo 8), elevando explícitamente el nivel de dicha protección al de derecho fundamental en el Derecho de la UE. Tanto las instituciones de la UE como los Estados miembros deberán respetar y

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

20 Véanse las versiones consolidadas de las Comunidades Europeas (2012), el Tratado de la Unión Europea, DO 2012 C 326; y de las Comunidades Europeas (2012), TFUE, DO 2012 C 326.

garantizar este derecho, el cual también es aplicable a los Estados miembros cuando apliquen el Derecho de la Unión (artículo 51 de la Carta). Al haber sido formulado varios años después de la Directiva de protección de datos, debe entenderse que el artículo 8 de la Carta recoge la legislación de la UE preexistente en materia de protección de datos. Por lo tanto, la Carta no solo menciona expresamente un derecho a la protección de los datos en el artículo 8, apartado 1, sino que también hace referencia a los principios clave en materia de protección del apartado 2 de dicho artículo. Por último, el artículo 8, apartado 3, de la Carta garantiza el control de la aplicación de dichos principios por parte de una autoridad independiente.

Perspectivas

En enero de 2012, la Comisión Europea propuso un paquete legislativo de reforma de la protección de datos, manifestando que era necesario modernizar la actual normativa en materia de protección de datos, teniendo en cuenta los rápidos avances tecnológicos y la globalización. El paquete de reforma está compuesto por una propuesta de Reglamento general de protección de datos,[21] que tiene como fin sustituir a la Directiva de protección de datos, así como una nueva Directiva de protección de datos,[22] que proporcionará la protección de datos en el marco de la cooperación policial y judicial en materia penal. En el momento de publicación de este manual, seguían su curso las discusiones sobre el paquete de reforma.

1.2. Ponderación entre derechos

Puntos clave

- El derecho a la protección de datos no es un derecho absoluto sino que debe ponderarse con otros derechos.

21 Comisión Europea (2012), Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos), COM(2012) 11 final, Bruselas, 25 de enero de 2012.

22 Comisión Europea (2012), Propuesta de 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 a la libre circulación de dichos datos (Directiva general de protección de datos), COM(2012) 10 final, Bruselas, 25 de enero de 2012.

El derecho fundamental a la protección de los datos personales, con arreglo al artículo 8 de la Carta «sin embargo, [...] no constituye una prerrogativa absoluta, sino que debe ser considerado en relación con su función en la sociedad».[23] El artículo 52, apartado 1, de la Carta reconoce, por tanto, que pueden introducirse limitaciones al ejercicio de derechos como los consagrados en los artículos 7 y 8 de la misma, siempre que tales limitaciones estén establecidas por la ley, respeten el contenido esencial de dichos derechos y libertades, y respetando el 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.[24]

En el sistema del CEDH, la protección de datos queda garantizada en el artículo 8 (derecho al respeto de la vida privada y familiar) y, tal como ocurre en el sistema de la Carta, es necesario aplicar dicho derecho respetándose al mismo tiempo el ámbito de aplicación de otros derechos concurrentes. De conformidad con el artículo 8, apartado 2, del CEDH, «no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria [...] para la protección de los derechos y las libertades de los demás».

Por consiguiente, tanto el TEDH como el TJUE han afirmado reiteradamente que es necesario realizar un ejercicio de ponderación con otros derechos cuando se aplica e interpreta el artículo 8 del CEDH y el artículo 8 de la Carta.[25] Algunos ejemplos importantes ilustrarán cómo se alcanza dicho equilibrio.

23 Véase, por ejemplo, TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen*, de 9 de noviembre de 2010, apdo. 48.

24 *Ibid*., apdo. 50.

25 TEDH, *Von Hannover contra Alemania (nº 2) [GS]*, nos 40660/08 y 60641/08, de 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*, de 24 de noviembre de 2011, apdo. 48; TJUE, asunto C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU*, de 29 de enero de 2008, apdo. 68. Véase, asimismo, Consejo de Europa (2013) Case law of the European Court of Human Rights concerning the protection of personal data (Jurisprudencia del Tribunal Europeo de Derechos Humanos relativa a la protección de datos personales), documento de jurisprudencia DP (2013), disponible en: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf.

1.2.1. Libertad de expresión

Uno de los derechos que puede entrar en conflicto 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». 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 de que puede ser legítimamente objeto este derecho, que el artículo 11 de la Carta garantiza, no pueden, por lo tanto, sobrepasar las establecidas en el artículo 10, apartado 2, del CEDH, es decir, deben estar prescritas por la ley y deben ser necesarias en una sociedad democrática «para la protección [...] de los derechos y libertades ajenos». Este concepto abarca el derecho a la protección de los datos.

La relación entre la protección de los datos personales y la libertad de expresión está regulada por el artículo 9 de la Directiva de protección de datos, titulado «Tratamiento de datos personales y libertad de expresión».[26] De conformidad con dicho artículo, «los Estados miembros establecerán exenciones y excepciones, respecto del derecho fundamental a la protección de datos y, por lo tanto, respecto del derecho fundamental a la intimidad, especificado en los capítulos II, IV y VI de la Directiva. Dichas exenciones deben realizarse con fines exclusivamente periodísticos o de expresión artística o literaria que quedan dentro del ámbito de aplicación del derecho fundamental a la libertad de expresión, en la medida en que resulten necesarias para conciliar el derecho a la privacidad con las normas que rigen la libertad de expresión»».

> Ejemplo: En el asunto *Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy*,[27] se solicitó al TJUE que interpretase el artículo 9 de la Directiva de protección de datos y definiese la relación entre la protección de datos y la libertad de prensa. El Tribunal tuvo que examinar la difusión de los

26 Directiva de protección de datos, artículo 9.

27 TJUE, asunto C-73/07, *Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy*, de 16 de diciembre de 2008, apdos. 56, 61 y 62.

datos fiscales de Markkinapörssi y Satamedia relacionados con alrededor de 1 200 000 personas físicas, los cuales habían sido legítimamente obtenidos de la administración fiscal finlandesa. En particular, el Tribunal 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 concluir que las actividades de Satakunnan constituían un «tratamiento de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva de protección de datos, el Tribunal prosiguió con la interpretación del artículo 9 de la Directiva. El Tribunal destacó en primer lugar la importancia que tiene la libertad de expresión en toda sociedad democrática y sostuvo que los conceptos relacionados con ella, entre ellos el de periodismo, deben ser interpretados ampliamente. Para luego observar que, para obtener una ponderación de los dos derechos fundamentales, las excepciones y restricciones a la protección de los datos deben aplicarse solo dentro de los límites de lo que resulte estrictamente necesario. En dichas circunstancias, el Tribunal consideró que las actividades realizadas por Markkinapörssi y Satamedia relativas a datos procedentes de documentos que son públicos según la legislación nacional, pueden calificarse de «actividades periodísticas» si su finalidad es divulgar al público información, opiniones o ideas, con independencia del medio utilizado para trasmitirlas. El Tribunal 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 este asunto en particular.

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

Ejemplo: En el asunto *Axel Springer AG contra Alemania,*[28] el TEDH consideró que una prohibición impuesta por un tribunal nacional sobre el propietario de un diario que deseaba publicar un artículo sobre la detención y la condena de un reconocido actor vulneraba el artículo 10 del CEDH. El TEDH reiteró los criterios que había establecido en su jurisprudencia al ponderar la libertad de expresión con el derecho al respeto a la vida privada:

28 TEDH, *Axel Springer AG contra Alemania* [GS], nº 39954/08, 7 de febrero de 2012, apdos. 90 y 91.

- en primer lugar, si el evento sobre el que hablaba el artículo publicado en cuestión era de interés general: la detención y la condena de una persona era un hecho judicial público y, por tanto, de interés público;

- en segundo lugar, si la persona afectada era un personaje público: la persona afectada era un actor lo bastante conocido para ser considerado una figura pública; y

- en tercer lugar, el modo en que se obtuvo la información y si dicha información era fiable: la información había sido facilitada por la oficina del Ministerio Fiscal y la exactitud de la información incluida en ambas publicaciones no era motivo de desacuerdo entre las partes.

Por lo tanto, el TEDH resolvió que las limitaciones de publicación impuestas sobre 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: En el asunto *Von Hannover contra Alemania (nº 2)*,[29] el TEDH consideró que no había existido una violación del derecho al respeto de la vida privada contemplado en el artículo 8 del CEDH, cuando no se concedió a la Princesa Carolina de Mónaco una orden judicial contra la publicación de una fotografía de ella y de su marido, la cual había sido tomada durante unas vacaciones de esquí. La fotografía iba acompañada de un artículo que informaba, entre otros asuntos, del mal estado de salud del Príncipe Rainiero. El TEDH concluyó que los tribunales nacionales habían ponderado cuidadosamente el equilibrio entre la libertad de expresión de las empresas editoras y el derecho al respeto a su vida privada. La caracterización que hicieron los tribunales nacionales de la enfermedad del Príncipe Rainiero como acontecimiento de la sociedad contemporánea no pudo considerarse irrazonable y el TEDH pudo aceptar que la fotografía, considerada a la luz del artículo, contribuía, al menos en cierta medida, a un debate de interés general. El Tribunal concluyó que no había existido una violación del artículo 8 del CEDH.

29 TEDH, *Von Hannover contra Alemania (nº 2)* [GS], nos 40660/08 y 60641/08, de 7 de febrero de 2012, apdos. 118 y 124.

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

Ejemplo: En el asunto *Mosley contra el Reino Unido*,[30] un periódico nacional de edición semanal publicó fotografías íntimas del demandante. Dicho demandante alegó entonces una violación del artículo 8 del CEDH porque no había podido ejercitar una acción ante la publicación de las fotos en cuestión debido a la inexistencia de una obligación de notificación previa para el periódico en los casos de publicación de un material que pueda vulnerar el derecho a la privacidad. Aunque la difusión de dicho material se realizara, por lo general, con fines de entretenimiento en lugar de educación, dicha difusión se benefició indudablemente de la protección del artículo 10 del CEDH, la cual puede ceder ante las obligaciones contempladas en el artículo 8 del CEDH cuando la información tuviera un carácter privado e íntimo y no existiera un interés público en su difusión. Sin embargo, debe tenerse un especial cuidado a la hora de examinar las limitaciones, las cuales podrían funcionar como una forma de censura previa a la publicación. En relación con el efecto disuasorio que la obligación de notificación previa podría plantear, las dudas sobre su eficacia y el amplio margen de apreciación en dicho 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 el asunto *Biriuk contra Lituania*,[31] la demandante reclamaba una indemnización por daños y perjuicios a un diario por la publicación de un artículo en el cual se informaba de que era seropositiva. Dicha información había sido supuestamente confirmada por el personal médico del hospital local. El TEDH no consideró que el artículo en cuestión contribuyera a un debate de interés general y reiteró que la protección de datos personales, sobre todo los datos médicos, tenía una importancia fundamental en el disfrute del derecho al respeto de la vida privada y familiar de una persona, tal y como garantiza el artículo 8 del CEDH. El Tribunal atribuyó un significado particular al hecho de que, según el informe del periódico, el personal médico de un hospital había facilitado información sobre la infección por VIH de la demandante, incumpliendo de forma evidente su obligación al secreto profesional. Por consiguiente, el Estado

30 TEDH, *Mosley contra el Reino Unido*, nº 48009/08, de 10 de mayo de 2011, apdos. 129 y 130.

31 TEDH, *Biriuk contra Lituania*, nº 23373/03, de 25 de noviembre de 2008.

no había logrado asegurar el derecho al respeto a la vida privada de la demandante. El tribunal concluyó que había existido una violación del artículo 8.

1.2.2. Acceso a los documentos

La libertad de información con arreglo al artículo 11 de la Carta y el artículo 10 del CEDH protege el derecho no solo de facilitar información sino también de *recibirla*. Cada vez se es más consciente de la importancia que tiene la transparencia del gobierno para el funcionamiento de una sociedad democrática. Por consiguiente, en las últimas dos décadas, el derecho de acceso a los documentos conservados por las autoridades públicas ha sido reconocido como un importante derecho de todos los ciudadanos de la UE y de toda persona física o persona jurídica que reside o tiene 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 oficiales, los cuales inspiraron a los autores del Convenio para el Acceso a Documentos Oficiales (*Convenio nº 205*).[32] **Según el Derecho de la UE**, el derecho de acceso a los documentos está garantizado en el Regulation 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*).[33] 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». De conformidad con el artículo 52, apartado 2, de la Carta, el derecho de acceso a los documentos también se ejercerá en las condiciones y dentro de los límites previstos en el artículo 15, apartado 3, del TFUE. Este derecho puede entrar en conflicto con el derecho a la protección de datos si el acceso a un documento permite revelar los datos personales de terceros. Las solicitudes de acceso a los documentos o la información conservada por las autoridades públicas deberán ser, por tanto, ponderadas con el derecho a la protección de datos de las personas cuyos datos se incluyen en los documentos solicitados.

32 Consejo de Europa, Comité de Ministros (2002), Recomendación Rec(2002)2 a los Estados miembros sobre el acceso a los documentos oficiales, de 21 de febrero de 2002; Consejo de Europa, Convenio sobre el Acceso a los Documentos Públicos, CETS nº 205, de 18 de junio de 2009. El Convenio aún no ha entrado en vigor.

33 Reglamento (CE) nº 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.

Ejemplo: En el asunto *Comisión contra Bavarian Lager*,[34] el TJUE definió el ámbito de protección de los datos en el contexto del acceso a los documentos de las instituciones de la UE y la relación entre el Reglamento (CE) nº 1049/2001 (*Reglamento de acceso a los documentos*) y el Reglamento (CE) nº 45/2001 (*Reglamento de protección de datos*). Bavarian Lager, constituida en 1992, importa cerveza alemana embotellada al Reino Unido, con destino, principalmente, a los establecimientos de despacho de bebidas alcohólicas. La empresa se encontró con dificultades, sin embargo, puesto que 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 a adaptarlas 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. Dado que no quedó satisfecha con dicha postura, Bavarian Lager interpuso un recurso ante el Tribunal de Primera Instancia, quien anuló la decisión de la Comisión mediante sentencia de 8 de noviembre de 2007 (asunto T-194/04, *Bavarian Lager contra Comisión*), considerando en particular que la mera inclusión de los nombres de las personas en cuestión en la lista de personas que asistieron a la reunión en nombre del organismo que representaban no constituía un perjuicio para la protección de la vida privada ni ponía en peligro las vidas privadas de dichas personas.

En el recurso de casación interpuesto por la Comisión, el TJUE anuló la sentencia del Tribunal de Primera Instancia. El TJUE declaró 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

34 TJUE, asunto C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd.*, de 29 de junio de 2010, apdos. 60, 63, 76, 78 y 79.

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 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 conformidad con esta sentencia, la interferencia en el derecho de protección de datos respecto al acceso a los documentos precisa una razón específica y justificada. El derecho de acceso a los documentos no puede anular automáticamente el derecho a la protección de datos.[35]

En la siguiente sentencia del TEDH se abordó un aspecto especial de una solicitud de acceso.

Ejemplo: En el asunto *Társaság a Szabadságjogokért contra Hungría*,[36] la demandante, una ONG de derechos humanos, había solicitado al Tribunal Constitucional el acceso a la información relativa a un asunto pendiente. Sin consultar con el miembro del Parlamento que había remitido el caso ante él, el Tribunal Constitucional desestimó la solicitud de acceso basándose en que las reclamaciones presentadas ante él sólo podrían ponerse a disposición de personas

35 Véanse, sin embargo, las deliberaciones pormenorizadas en el documento del Supervisor Europeo de Protección de Datos (SEPD) (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling* (El acceso público a los documentos que incluyen datos personales después de la sentencia Bavarian Lager), Bruselas, de 24 de marzo de 2011, disponible en: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 TEDH, *Társaság a Szabadságjogokért contra Hungría*, nº 37374/05, de 14 de abril de 2009; véanse los apdos. 27, 36 a 38.

ajenas con la aprobación del demandante. Los tribunales nacionales mantuvieron esta denegación, basándose en que la protección de dichos datos personales no podría prevalecer sobre otros intereses legítimos, incluida la accesibilidad de la información pública. La demandante había actuado como un «vigilante social», cuyas actividades merecían una protección similar a la proporcionada a la prensa. Respecto de la libertad de prensa, el TEDH ha sostenido de forma reiterada que el público tiene derecho a recibir información de interés general. La información requerida por el demandante estaba «lista y disponible» y no exigía que se llevara a cabo una recogida de datos. En dichas circunstancias, el Estado tenía la obligación de no impedir el flujo de información requerida por el demandante. En resumen, el TEDH consideró que los obstáculos diseñados para obstaculizar el acceso a la información de interés público podrían desanimar a quienes trabajan en los medios de comunicación o en ámbitos relacionados de llevar a cabo su papel vital de «vigilante público». El Tribunal concluyó que había existido una violación del artículo 10.

Según el Derecho de la UE, ha quedado firmemente establecida la importancia de la transparencia. El principio de transparencia queda consagrado en los artículos 1 y 10 del TUE y en el artículo 15, apartado 1, del TFUE.[37] Según el considerando 2 del Reglamento (CE) nº 1049/2001, permite garantizar una mayor participación de los ciudadanos en el proceso de toma de decisiones, así como una mayor legitimidad, eficacia y responsabilidad de la administración para con los ciudadanos en un sistema democrático.[38]

Siguiendo este razonamiento, el Reglamento (CE) nº 1290/2005 sobre la financiación de la política agrícola común y el Reglamento (CE) nº 259/2008 de la Comisión por el que se establecen disposiciones para su aplicación exigen la publicación de información sobre los beneficiarios de determinados fondos de la UE en el sector agrícola y los importes recibidos por cada beneficiario.[39] La publicación debería

37 UE (2012), Versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea, DO 2012 C 326.

38 TJUE, asunto C-41/00 P, *Interporc Im- und Export GmbH contra Comisión de las Comunidades Europeas*, de 6 de marzo de 2003, apdo. 39; y TJUE, asunto C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd.*, de 29 de junio de 2010, apdo. 54.

39 Reglamento (CE) nº 1290/2005, de 21 de junio de 2005, sobre la financiación de la política agrícola común, DO 2005 L 209; y el Reglamento (CE) nº 259/2008 de la Comisión, de 18 de marzo de 2008, por el que se establecen disposiciones de aplicación del Reglamento (CE) nº 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.

contribuir al control público del uso adecuado de los fondos públicos por parte de la administración. La proporcionalidad de esta publicación fue impugnada por varios beneficiarios.

Ejemplo: En el asunto *Volker und Markus Schecke y Hartmut Eifert contra Land Hessen*,[40] 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.

El Tribunal, 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 Tribunal consideró que dicha interferencia 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. El Tribunal declaró entonces parcialmente nula la legislación de la UE sobre la publicación de información relacionada con los beneficiarios de los fondos agrícolas europeos.

1.2.3. Libertad de las artes y de las ciencias

Otro derecho que debe ponderarse con el derecho al respeto a la vida privada y a la protección de datos es la libertad de las artes y las ciencias, que se encuentra expresamente protegida en el artículo 13 de la Carta. Este derecho se infiere en primer lugar de las libertades de pensamiento y expresión y se ejerce en el respeto del artículo 1 de la Carta (Dignidad humana). El TEDH considera que la libertad de las artes está protegida con arreglo al artículo 10 del CEDH.[41] El derecho garantizado por

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

41 TEDH, *Müller y otros contra Suiza*, nº 10737/84, de 24 de mayo de 1988.

el artículo 13 de la Carta también puede estar sujeto a las limitaciones autorizadas por el artículo 10 del CEDH.[42]

Ejemplo: En el asunto *Vereinigung bildender Künstler contra Austria*,[43] los tribunales austriacos prohibieron a la asociación demandante que continuara exhibiendo una pintura que incluía fotos de las cabezas de diversas personalidades 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 tribunal nacional emitió un auto por el que se aceptaba su petición. El TEDH reiteró que el artículo 10 del CEDH resultaba aplicable a la comunicación de ideas que ofendan, sorprendan o perturben al Estado o a una parte de la población. Las personas que crearon, realizaron, distribuyeron o exhibieron obras de arte contribuyeron al intercambio de ideas y opiniones y el Estado tenía 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, lo cual obviamente no tenía por objeto ser un reflejo ni siquiera hacer una sugerencia sobre la realidad, el TEDH declaró asimismo que «difícilmente podría entenderse que la pintura aborda detalles de la vida privada [de la persona dibujada] sino que más bien está relacionada con su posición pública como político» y que «en dicha calidad [la persona dibujada] debería mostrar una mayor tolerancia ante las críticas». Al ponderar los distintos intereses en juego, 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.

Respecto de las ciencias, la legislación europea en materia de protección de datos es consciente del valor especial que la ciencia tiene para la sociedad. Por lo tanto, se reducen las limitaciones generales de uso de los datos personales. Tanto la Directiva de protección de datos como el Convenio nº 108 permiten la conservación de los datos para investigaciones científicas una vez que ya no son necesarios para la finalidad inicial para la que fueron recopilados. Asimismo, el uso posterior de los datos personales para investigaciones científicas no se considerará una finalidad incompatible. El Derecho nacional es el encargado de la tarea de desarrollar disposiciones

42 Explicaciones sobre la Carta de los Derechos Fundamentales, DO 2007 C 303.

43 TEDH, *Vereinigung bildender Künstler contra Austria*, nº 68345/01, de 25 de enero de 2007; véanse en especial los apdos. 26 y 34.

más detalladas, incluidas las garantías necesarias, para conciliar el interés en la investigación científica con el derecho a la protección de datos (véanse asimismo los apartados 3.3.3 y 8.4).

1.2.4. Protección de la propiedad

El derecho a la protección de la propiedad queda consagrado tanto en el artículo 1 del Protocolo Adicional del CEDH como en el artículo 17, apartado 1, de la Carta. Un aspecto importante del derecho a la propiedad es la protección de la propiedad intelectual, la cual se menciona expresamente en el artículo 17, apartado 2, de la Carta. En el ordenamiento jurídico de la UE podemos encontrar varias directivas que tienen como fin la protección efectiva de la propiedad intelectual, en particular, de 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 de forma equilibrada con la protección de otros derechos fundamentales, en particular, con el derecho a la protección de datos.[44] Ha habido casos en que las instituciones de protección de los derechos de autor han solicitado a los proveedores de Internet que revelasen la identidad de los usuarios de las plataformas de intercambio de archivos por Internet. Dichas plataformas con frecuencia ofrecen la posibilidad a los usuarios de Internet de descargar de forma gratuita títulos musicales incluso si están protegidos por derechos de autor.

Ejemplo: *Promusicae contra Telefónica de España*[45] hacía referencia a 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 esta presta un servicio de acceso a Internet. Promusicae solicitó que le fuera facilitada la información para poder ejercitar acciones civiles contra aquellas personas que, según manifestó, utilizaban un programa de intercambio de archivos que permitía el acceso a fonogramas cuyos derechos patrimoniales de explotación correspondían a los asociados de Promusicae.

44 TEDH, *Ashby Donald y otros contra Francia,* nº 36769/08, de 10 de enero de 2013.

45 TJUE, asunto C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU*, de 29 de enero de 2008, apdos. 54 y 60.

El tribunal español remitió la cuestión al TJUE, preguntándole 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 a las Directivas 2000/31, 2001/29 y 2004/48, leídas también a la luz de los artículos 17 y 47 de la Carta. El Tribunal 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.

El Tribunal 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 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.»[46]

46 *Ibid.*, apdos. 65 y 68; véase, asimismo, TJUE, asunto C-360/10, *SABAM contra Netlog N.V.*, de 16 de febrero de 2012.

2

Terminología de protección de datos

UE	Materias cubiertas	CdE
Datos personales		
Directiva de protección de datos, artículo 2, letra a) TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR (C-92/09) y Hartmut Eifert (C-93/09) contra Land Hessen*, de 9 de noviembre de 2010 TJUE, asunto C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU*, de 29 de enero de 2008	**Definición legal**	Convenio nº 108, artículo 2, letra a) TEDH, *Bernh Larsen Holding AS y otros contra Noruega*, nº 24117/08, de 14 de marzo de 2013
Directiva de protección de datos, artículo 8, apartado 1 TJUE, asunto C-101/01, *Bodil Lindqvist*, de 6 de noviembre de 2003	**Categorías especiales de datos personales (datos sensibles)**	Convenio nº 108, artículo 6
Directiva de protección de datos, artículo 6, apartado 1, letra e)	**Datos anonimizados y pseudonimizados**	Convenio nº 108, artículo 5, letra e) Convenio nº 108, Informe explicativo, artículo 42
Tratamiento de datos		
Directiva de protección de datos, artículo 2, letra b) TJUE, asunto C-101/01, *Bodil Lindqvist*, de 6 de noviembre de 2003	**Definiciones**	Convenio nº 108, artículo 2, letra c)

Usuarios de los datos		
Directiva de protección de datos, artículo 2, letra d)	**Responsable del tratamiento**	Convenio nº 108, artículo 2, letra d) Recomendación de perfilado, artículo 1, letra g)*
Directiva de protección de datos, artículo 2, letra e) TJUE, asunto C-101/01, *Bodil Lindqvist*, de 6 de noviembre de 2003	**Encargado del tratamiento**	Recomendación de perfilado, artículo 1, letra h)
Directiva de protección de datos, artículo 2, letra g)	**Destinatario**	Convenio nº 108, Protocolo adicional, artículo 2, apartado 1
Directiva de protección de datos, artículo 2, letra f)	**Tercero**	
Consentimiento		
Directiva de protección de datos, artículo 2, letra h) TJUE, asunto C-543/09, *Deutsche Telekom AG contra Alemania*, de 5 de mayo de 2011	**Definición y requisitos para el consentimiento válido**	Recomendación sobre datos médicos, artículo 6, y diversas recomendaciones posteriores

*Nota: * Consejo de Europa, Comité de Ministros (2010), Recomendación CM/Rec(2010) 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 de perfilado), de 23 de noviembre de 2010.*

2.1. Datos personales

Puntos clave

- Los datos son datos personales si están relacionados con una persona identificada o, al menos, identificable, el interesado.
- Una persona es identificable si puede obtenerse información adicional, sin tener que realizar esfuerzos poco razonables, que permita identificar al interesado.
- Autenticación significa demostrar que una determinada persona posee una determinada identidad y/o está autorizada para realizar determinadas actividades.
- Existen categorías especiales de datos, los denominados datos sensibles, enumerados en el Convenio nº 108 y en la Directiva 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 incluyen identificadores; en cambio, son pseudonimizados si los identificadores están encriptados.
- A diferencia de los datos anonimizados, los datos pseudonimizados son datos personales.

2.1.1. Principales aspectos del concepto de datos personales

De conformidad con el Derecho de la UE así como con el **Derecho del CdE**, los «datos personales» se definen como información sobre una persona física identificada o identificable,[47] es decir, información sobre una persona cuya identidad queda manifiestamente clara o que puede establecerse, como mínimo, obteniendo datos adicionales.

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

Una persona

El derecho a la protección de datos se desarrolló a partir del derecho al respeto a la vida privada. El concepto de vida privada está relacionado con los seres humanos. Las personas físicas son, por tanto, los principales beneficiarios de la protección de datos. Según el Dictamen del Grupo del artículo 29, además, la legislación europea en materia de protección de datos únicamente protege a los *seres vivos*.[48]

La jurisprudencia del TEDH relativa al artículo 8 del CEDH muestra que puede resultar difícil separar completamente los aspectos de la vida privada y de la vida profesional.[49]

Ejemplo: En el asunto *Amann contra Suiza,*[50] las autoridades interceptaron una llamada telefónica de negocios del demandante. Basándose en dicha llamada, las autoridades investigaron al demandante y abrieron una ficha sobre el

47 Directiva de protección de datos, artículo 2, letra a); Convenio nº 108, artículo 2, letra a).

48 Grupo del artículo 29 (2007), *Dictamen 4/2007 sobre el concepto de datos personales*, WP 136, de 20 de junio de 2007, p. 22.

49 Véase, por ejemplo, TEDH, *Rotaru contra Rumanía* [GS], nº 28341/95, de 4 de mayo de 2000, apdo. 43; TEDH, *Niemietz contra Alemania*, nº *13710/88*, de 16 de diciembre de 1992, apdo. 29.

50 TEDH, *Amann contra Suiza* [GS], nº 27798/95, de 16 de febrero de 2000, apdo. 65.

demandante para el fichero de seguridad nacional. Aunque la intercepción afectaba a una llamada telefónica de negocios, el TEDH consideró que el almacenamiento de datos sobre dicha llamada estaba relacionado con la vida privada del demandante. Señaló que el término «vida privada» no debía interpretarse de forma restrictiva, en particular, teniendo en cuenta que el respeto a la vida privada incluye el derecho a entablar y desarrollar relaciones con otros seres humanos. Además, no existía una razón de principio que justificara la exclusión de las actividades de carácter profesional o de negocios del concepto de «vida privada». Esta interpretación amplia se correspondía con aquella consagrada en el Convenio nº 108. El TEDH también consideró que la injerencia en el caso del demandante no había sido realizada en conformidad la ley dado que el Derecho nacional no incluía disposiciones específicas y detalladas sobre la obtención, el registro y el almacenamiento de información, por lo que concluyó que había existido una violación del artículo 8 del CEDH.

Asimismo, si los asuntos de la vida profesional también pueden estar sujetos a la protección de datos, parece cuestionable que la protección únicamente se ofrezca a las personas físicas. Los derechos contemplados en el CEDH se garantizan no solo a las personas físicas sino a todo el mundo.

Existe jurisprudencia del TEDH en las que dicho tribunal se pronuncia 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. Sin embargo, el tribunal examinó el asunto al amparo del derecho al respeto del domicilio y la correspondencia, en lugar de al amparo de la vida privada:

Ejemplo: El asunto *Bernh Larsen Holding AS y otros contra Noruega*[51] estaba relacionado con una reclamación 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 del servidor que las tres utilizaban conjuntamente.

El TEDH resolvió que tal obligación para las empresas demandantes constituía una injerencia en sus derechos al respeto al «domicilio» y la «correspondencia», a efectos de lo dispuesto en el artículo 8 del CEDH. Sin embargo, el Tribunal consideró que la administración fiscal disponía de garantías efectivas y

51 TEDH, *Bernh Larsen Holding AS y otros contra Noruega*, nº 24117/08, de 14 de marzo de 2013. Véase, asimismo, en cambio, TEDH, *Liberty y otros contra el Reino Unido*, nº 58243/00, de 1 de julio de 2008.

adecuadas contra los abusos: se había notificado con la suficiente antelación a las empresas demandantes, quienes habían estado presentes y habían podido presentar observaciones en las intervenciones sobre el terreno, y el material se destruiría una vez que la revisión fiscal finalizara. En dichas 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 trabajan 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 sostuvo que no había existido una violación del artículo 8.

Según el Convenio nº 108, la protección concierne, principalmente, a la protección de las personas físicas. Sin embargo, las partes contratantes podrán ampliar la protección de datos a las personas jurídicas, como las empresas y asociaciones comerciales, en su Derecho nacional. **La legislación de la UE en materia de protección de datos** no incluye, en general, la protección de las personas jurídicas en relación con el tratamiento de datos que les afectan. Los reguladores nacionales tienen libertad para regular sobre esta materia.[52]

Ejemplo: En el asunto *Volker und Markus Schecke y Hartmut Eifert contra Land Hessen*,[53] el TJUE, en relación con la publicación de los datos personales relacionados con 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 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 [...]».[54]

Carácter identificable de una persona

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

52 Directiva de protección de datos, considerando 24.

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

54 *Ibid*., apdo. 52.

- dicha información identifica a una persona física; o

- se describe a una persona física en dicha información, aunque no se la identifique, de forma que haga posible averiguar quién es el interesado si se lleva a cabo una mayor investigación.

Ambos tipos de información están protegidos del mismo modo por la legislación europea en materia de protección de datos. 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 nº 108, en especial por lo que se refiere a la condición de estar relacionado con personas identificadas o identificables.[55]

Las definiciones jurídicas de los datos personales no aclaran con más detalle el momento en que se considera identificada una persona.[56] Evidentemente, la identificación exige que se incluyan elementos que describan a una persona de tal modo que él o ella es distinguible de todas las demás personas y reconocible como un individuo. El nombre de la persona es el ejemplo paradigmático de dichos elementos de descripción. En casos excepcionales, otros identificadores pueden tener un efecto similar a un nombre. Por ejemplo, en el caso de las personalidades puede ser suficiente mencionar el puesto de la persona, por ejemplo, el Presidente de la Comisión Europea.

Ejemplo: En el asunto *Promusicae*,[57] el TJUE declaró que «tampoco 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 [...]. Esta comunicación de datos que, según Promusicae, almacena Telefónica – cuestión que ésta no niega –, constituye un tratamiento de datos personales en el sentido del artículo 2, primer párrafo, de la Directiva 2002/58, en relación con el artículo 2, letra b), de la Directiva 95/46».

55 TEDH, *Amann contra Suiza* [GS], nº 27798/95, de 16 de febrero de 2000, apdo. 65 *et al.*

56 Véase, asimismo, TEDH, *Odièvre contra Francia* [GS], nº 42326/98, de 13 de febrero de 2003; y TEDH, *Godelli contra Italia*, nº 33783/09, de 25 de septiembre de 2012.

57 TJUE, asunto C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU*, de 29 de enero de 2008, apdo. 45.

Dado que muchos nombres no son únicos, es posible que para establecer la identidad de una persona sean necesarios otros identificadores que garanticen que no se confunde a una persona con otra. Con frecuencia, se suele utilizar la fecha y el lugar de nacimiento. Además, en algunos países se han introducido números personalizados para distinguir mejor a los ciudadanos. Los datos biométricos, como las impresiones dactilares, las fotografías digitales o el escaneo del iris, son cada vez más importantes 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 necesario que la identificación del interesado sea de gran calidad, sino que basta que la persona en cuestión sea identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante datos que incluyen elementos de identificación.[58] De conformidad con el considerando 26 de la Directiva de protección de datos, el punto de referencia es la posibilidad de que medios razonables de identificación estén disponibles y sean utilizados por los usuarios previstos de la información, entre los que se incluyen los terceros destinatarios (véase el apartado 2.3.2).

Ejemplo: Una autoridad local decide obtener datos de los automóviles que circulan por las calles locales. 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. El interesado presenta una reclamación, alegando que la autoridad local no dispone de base jurídica con arreglo a la legislación en materia de protección de datos para dicha obtención de datos. La autoridad sostiene que no recopila datos personales, afirmando que las matrículas de los vehículos son datos sobre personas anónimas. La autoridad local no está autorizada a acceder al registro general de vehículos para descubrir la identidad del titular o del conductor del automóvil.

Este razonamiento no es conforme al considerando 26 de la Directiva de protección de datos. Dado que la finalidad de la recopilación de datos es claramente identificar y sancionar a los conductores que conducen a una velocidad excesiva, es previsible que se intente la identificación. Aunque las autoridades locales no disponen directamente de medios de identificación, estas transmiten los datos a la autoridad competente, la policía, quién sí dispone de los mismos. En el

58 Directiva de protección de datos, artículo 2, letra a).

considerando 26 también se incluye de manera expresa una situación en la que es previsible que otros destinatarios de los datos, distintos del usuario inmediato de los mismos, puedan intentar identificar a la persona física. A la luz de lo establecido en el considerando 26, la actuación de la autoridad local equivale a una obtención de 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.

Según el Derecho del CdE, el carácter identificable debe entenderse de un modo similar. El artículo 1, apartado 2, de la Recomendación de datos de los pagos,[59] por ejemplo, establece que no se considerará que una persona es «identificable» si su identificación requiere una cantidad de tiempo, coste o mano de obra poco razonables.

Autenticación

Se trata de un procedimiento mediante el cual una persona es capaz de demostrar que posee una determinada identidad y/o está autorizada para hacer determinadas cosas, como acceder a una zona de seguridad o retirar dinero de una cuenta bancaria. La autenticación puede lograrse mediante la comparación de datos biométricos, como una fotografía o las impresiones dactilares de un pasaporte, con los datos de la persona que se presenta, por ejemplo, en un control de inmigración; o solicitando información que únicamente puede ser conocida por la persona con una cierta identidad o autorización, como un número de identificación personal (PIN) o contraseña; o pidiendo que se presente un determinado token, que estará exclusivamente en posesión de la persona con una determinada identidad o autorización, como una tarjeta con chip especial o la llave de una caja fuerte de un banco. Aparte de las contraseñas o las tarjetas con chip, a veces junto con los PIN, las firmas electrónicas son unos instrumentos especialmente aptos para identificar y autenticar a una persona en las comunicaciones electrónicas.

Naturaleza de los datos

Cualquier tipo de información puede ser considerada dato personal siempre que haga referencia a una persona.

59 Consejo de Europa, Comité de Ministros (1990), Recomendación nº R Rec(90) 19 relativa a la protección de los datos personales utilizados para el pago y otras operaciones conexas, de 13 de septiembre de 1990.

Ejemplo: La evaluación del rendimiento de trabajo de un empleado por parte de un supervisor, que estaba almacenada en el expediente de personal del empleado, constituye datos personales sobre el empleado, incluso cuando solo refleja, en parte o en su totalidad, la opinión personal del superior, como: «el empleado no muestra una dedicación por su trabajo» y no hechos concretos, como: «el empleado se ha ausentado del trabajo durante cinco semanas en los últimos seis meses».

Los datos personales incluyen información relativa a la vida privada de una persona, así como información sobre su vida profesional o pública.

En el *asunto Amann*,[60] el TEDH interpretó que el término «datos personales» no se limitaba a las cuestiones del ámbito privado de una persona física (véase el apartado 2.1.1). Este significado del término «datos personales» también es relevante en el caso de la Directiva de protección de datos:

Ejemplo: En la sentencia *Volker und Markus Schecke y Hartmut Eifert contra Land Hessen*,[61] 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 que el término «vida privada» no debía ser interpretado de forma restrictiva y que «ninguna razón de principio permite excluir las actividades profesionales... del concepto de "vida privada"».

Los datos también se refieren a personas si el contenido de la información revela indirectamente datos sobre una persona. En algunos casos, cuando existe un vínculo estrecho entre el objeto o un acontecimiento, por un lado, por ejemplo, un teléfono móvil, un automóvil, un accidente y, por otro, una persona, por ejemplo, su titular, usuario, víctima, la información sobre un objeto o sobre el acontecimiento también debe ser considerada datos personales.

Ejemplo: En el asunto *Uzun contra Alemania,*[62] se sometió a vigilancia al demandante y a otro hombre mediante un dispositivo con sistema de posicionamiento

60 TEDH, *Amann contra Suiza*, nº 27798/95, de 16 de febrero de 2000, apdo. 65.

61 Asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen*, de 9 de noviembre de 2010, apdo. 59.

62 TEDH, *Uzun contra Alemania*, nº 35623/05, de 2 de septiembre de 2010.

global (GPS), que se había colocado en el automóvil del otro hombre, porque se sospechaba de su participación en atentados con bombas. En este caso, el TEDH sostuvo que la observación del demandante a través de GPS constituía una injerencia en su vida privada, tal como queda protegida en el artículo 8 del CEDH. Sin embargo, la vigilancia mediante GPS había sido realizada de conformidad con la ley, así como proporcionada para el fin legítimo de investigar varios cargos de intento de homicidio y, por lo tanto, resultaba necesaria en una sociedad democrática. El Tribunal concluyó que no había existido una violación del artículo 8 del CEDH.

Forma de presentación de los datos

El modo en que los datos personales se almacenan o utilizan es irrelevante para la aplicabilidad de la legislación en materia de protección de datos. Las comunicaciones escritas o habladas pueden incluir datos personales y también imágenes,[63] en particular las filmaciones[64] o sonidos[65] de circuito cerrado de televisión (CCTV). Pueden ser datos personales la información registrada de forma electrónica, así como la información en papel, incluso las muestras de células de tejido humano, ya que estas registran el ADN de una persona.

2.1.2. Categorías especiales de datos personales

Tanto según el Derecho de la UE como según el **Derecho del CdE**, existen categorías especiales de datos personales que, por su carácter, pueden suponer un riesgo para los interesados cuando son tratados y que necesitan una protección reforzada. El tratamiento de estas categorías especiales de datos («datos sensibles») deberá permitirse, por tanto, únicamente con garantías específicas.

En la definición de los datos sensibles, tanto el Convenio nº 108 (artículo 6) como la Directiva de protección de datos (artículo 8), mencionan las siguientes categorías:

- datos personales que revelan el origen racial o étnico;

63 TEDH, *Von Hannover contra Alemania*, nº 59320/00, de 24 de junio de 2004; TEDH, *Sciacca contra Italia*, nº 50774/99, de 11 de enero de 2005.

64 TEDH, *Peck contra el Reino Unido*, nº 44647/98, de 28 de enero de 2003; TEDH, *Köpke contra Alemania*, nº 420/07, de 5 de octubre de 2010.

65 Directiva de protección de datos, considerandos 16 y 17; TEDH, *P.G. y J.H. contra el Reino Unido*, nº 44787/98, de 25 de septiembre de 2001, apdos. 59 y 60; TEDH, *Wisse contra Francia*, nº 71611/01, de 20 de diciembre de 2005.

- datos personales que revelan opiniones políticas, creencias religiosas y otras creencias; y

- datos personales relativos a la salud o la vida sexual.

Ejemplo: En el asunto *Bodil Lindqvist*,[66] el TJUE declaró que «el hecho de que una persona se haya lesionado un pie y esté en situación de baja parcial constituye un dato personal relativo a la salud en el sentido del artículo 8, apartado 1, de la Directiva 95/46».

La Directiva de protección de datos incluye, además, la «afiliación sindical» como dato sensible, ya que esta información puede ser un sólido indicador de opinión o de afiliación política.

El Convenio nº 108 también considera como datos sensibles los datos personales relacionados con las condenas penales.

El artículo 8, apartado 7, de la Directiva de protección de datos establece que los Estados miembros «determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento».

2.1.3. Datos anonimizados y pseudonimizados

De conformidad con el principio de conservación de los datos, incluido tanto en la Directiva de protección de datos como en el Convenio nº 108 (el cual se abordará con más detalle en el capítulo 3), los datos deben ser conservados «en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se trate ulteriormente».[67] En consecuencia, los datos deben ser anonimizados si un responsable de tratamiento desea almacenarlos después de que hayan quedado obsoletos y ya no sirvan para su finalidad inicial.

66 TJUE, asunto C-101/01, *Bodil Lindqvist*, de 6 de noviembre de 2003, apdo. 51.

67 Directiva de protección de datos, artículo 6, apartado 1, letra e); y Convenio nº 108, artículo 5, letra e).

Datos anonimizados

Los datos son anonimizados si se han eliminado todos los elementos identificativos de un conjunto de datos personales. No puede dejarse en la información elementos que podrían, ejerciendo un esfuerzo razonable, servir para volver a identificar a la(s) persona(s) de que se trate.[68] En los casos en que los datos se hayan anonimizado con éxito, ya no serán datos personales.

Si los datos personales ya no sirven para su finalidad inicial aunque se conservan de una forma personalizada con fines históricos, estadísticos o científicos, la Directiva de protección de datos y el Convenio nº 108 permiten esta posibilidad, con la condición de que se hayan aplicado las garantías adecuadas contra el uso indebido.[69]

Datos pseudonimizados

La información personal incluye identificadores, como el nombre, la fecha de nacimiento, el sexo y la dirección. Cuando la información personal se pseudonimiza, los identificadores se sustituyen por un pseudónimo. La pseudonimización se logrará, por ejemplo, mediante la encriptación de los identificadores de los datos personales.

Los datos pseudonimizados no se mencionan de forma expresa en las definiciones jurídicas ni del Convenio nº 108 ni de la Directiva de protección de datos. Sin embargo, el Informe explicativo del Convenio nº 108 establece en su artículo 42 que «[e]l requisito [...] relativo a los plazos de almacenamiento de datos en su forma nominativa no significa que deban separarse, después de cierto tiempo, irrevocablemente del nombre de la persona a que hacen referencia, sino únicamente que no debe ser posible vincularlos fácilmente a los datos ni a los identificadores». Esto es un efecto que puede lograrse mediante la pseudonimización de los datos. Para quienes no dispongan de una clave de encriptado, los datos pseudonimizados pueden ser identificables con dificultad. Todavía existe un vínculo con la identidad en forma de pseudónimo, más la clave de encriptado. Además, aquellos que están autorizados a utilizar las claves de encriptado pueden conseguir más fácilmente una nueva identificación. El uso de las claves de encriptado por parte de personas no autorizadas deberá estar especialmente protegido.

68 *Ibid.*, considerando 26.

69 *Ibid.*, artículo 6, apartado 1, letra e); y Convenio nº 108, artículo 5, letra e).

La pseudonimización de los datos es uno de los medios más importantes de lograr la protección de datos a gran escala, cuando no es posible evitar completamente la utilización de los datos personales. La lógica y efectos de dicha acción deberán explicarse con más detalle.

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

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

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

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

Los usuarios que tienen acceso a estos datos pseudonimizados normalmente no podrán identificar «Charles Spencer, nacido el 3 de abril de 1967» con «324» o «YESz3201». Por lo tanto, es más probable que los datos pseudonimizados estén seguros frente a un uso indebido.

El primer ejemplo resulta, sin embargo, 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 pseudonimización afecta a la eficacia de la protección de datos.

Los datos personales con identificadores encriptados se utilizan en muchos contextos como una manera de conservar en secreto la identidad de las personas. Esto es especialmente útil cuando los responsables del tratamiento necesitan garantizar que están tratando datos de los mismos interesados aunque no exigen ni deberían disponer de 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 conoce únicamente el hospital en el que están siendo tratados, y de los que el investigador obtiene las historias clínicas pseudonimizadas. La pseudonimización es, por tanto, un sólido componente del conjunto de tecnologías de protección del derecho de la privacidad. Puede funcionar como un elemento importante al aplicar la privacidad por diseño, lo cual significa que la protección de datos se construye sobre la base de sistemas avanzados de tratamiento de datos.

2.2. Tratamiento de datos

Puntos clave

- El término «tratamiento» hace referencia principalmente al tratamiento automatizado.
- Al amparo del Derecho de la UE, el «tratamiento» se refiere, además, al tratamiento manual en sistemas de archivado estructurados.
- De conformidad con el Derecho del CdE, el significado de «tratamiento» puede ser ampliado por el Derecho nacional a fin de incluir el tratamiento manual.

La protección de datos al amparo del Convenio nº 108 y de la Directiva de protección de datos se centra principalmente en el tratamiento automatizado de datos.

Con arreglo al **Derecho del CdE**, la definición del tratamiento automatizado reconoce, sin embargo, que para algunas fases del uso manual de los datos personales puede ser necesario realizar operaciones automatizadas. De modo similar, de conformidad con el **Derecho de la Unión Europea**, se define el tratamiento automatizado de datos como «operaciones efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados».[70]

Ejemplo: En el asunto *Bodil Lindqvist*,[71] el TJUE sostuvo 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».

El tratamiento de datos manual también requiere protección de los datos.

La protección de datos **según el Derecho de la UE** no se limita en ningún caso al tratamiento de datos automatizado. De este modo, con arreglo a la legislación de la UE, la protección de datos se aplica al tratamiento de datos personales en un sistema de

70 Convenio nº 108, artículo 2, letra c); y Directiva de protección de datos, artículo 2, letra b) y artículo 3, apartado 1.

71 TJUE, asunto C-101/01, *Bodil Lindqvist*, de 6 de noviembre de 2003, apdo. 27.

archivado manual, es decir, en un fichero en papel especialmente estructurado.[72] El motivo de esta ampliación de la protección de datos es que:

- los ficheros en papel pueden estructurarse de un modo que faciliten una rápida búsqueda de información; y

- 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.[73]

Según el Derecho del CdE, el Convenio nº 108 regula principalmente el tratamiento de datos en ficheros automatizados de datos.[74] También establece, sin embargo, la posibilidad de ampliar la protección al tratamiento manual en el derecho nacional. Muchas Partes del Convenio nº 108 han utilizado esta posibilidad y han efectuado declaraciones en este sentido al Secretario General del Consejo de Europa.[75] La ampliación de la protección de datos en virtud de dicha declaración debe referirse a todos los datos manuales y no puede quedar limitada al tratamiento de los sistemas de archivado manual.[76]

En lo que atañe al carácter de las operaciones de tratamiento que están incluidas, el concepto de tratamiento es integral **tanto según el Derecho de la UE como el Derecho del CdE**: «"tratamiento de datos personales" [...] cualquier operación [...] como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción»[77] efectuada en datos personales. En el término «tratamiento» también se incluyen acciones en las cuales los datos dejan de estar bajo la responsabilidad de un responsable del tratamiento para pasar a estar bajo la responsabilidad de otro responsable del tratamiento.

72 Directiva de protección de datos, artículo 3, apartado 1.

73 *Ibid*., considerando 27.

74 Convenio nº 108, artículo 2, letra b).

75 Véanse las declaraciones efectuadas al amparo del Convenio nº 108, artículo 3, apartado 2, letra c).

76 Véase el texto del Convenio nº 108, artículo 3, apartado 2.

77 Directiva de protección de datos, artículo 2, letra b). Del mismo modo, véase también el Convenio nº 108, artículo 2, letra c).

Ejemplo: Los empresarios obtienen y tratan datos sobre sus empleados, incluida la información relativa a sus salarios. La base jurídica para llevar a cabo la acción anterior de forma legítima es el contrato de trabajo.

Los empresarios deben remitir los datos relativos a los salarios de su personal a la administración fiscal. Este envío de datos también se considerará «tratamiento» en el sentido que dicho término posee en el Convenio nº 108 y en la Directiva. Sin embargo, el fundamento jurídico de dicha difusión no es 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 está incluida normalmente en las disposiciones de las legislaciones fiscales nacionales. Si no existen dichas disposiciones, la transmisión de datos sería un tratamiento ilegal.

2.3. Los usuarios de los datos personales

Puntos clave

- Toda persona que decida tratar datos personales de otras personas se considerará un «responsable del tratamiento», en virtud de la legislación en materia de protección de datos; si son varias las personas que toman esta decisión, se les denominará «corresponsables».
- Un «encargado del tratamiento» es una entidad jurídicamente independiente que trata datos personales en nombre del responsable del tratamiento.
- Un encargado del tratamiento se convierte en un responsable del tratamiento si utiliza los datos para sus propios fines, sin seguir las instrucciones de ningún responsable del tratamiento.
- Cualquier persona que reciba datos de un responsable del tratamiento será un «destinatario».
- Un «tercero» es una persona física o jurídica que no actúa bajo las instrucciones de un responsable del tratamiento (y que no es un interesado).
- Los «terceros destinatarios» son personas o entidades jurídicamente independientes del responsable del tratamiento pero que reciben datos personales del mismo.

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 respectivas obligaciones, de conformidad con la legislación en materia de protección de datos. Solo aquellas personas que puedan ser responsables con arreglo a la legislación aplicable podrán asumir estos puestos. En el sector privado, estas suelen ser personas físicas o jurídicas, mientras que en el sector público, normalmente se trata de una autoridad. Otras entidades, como órganos o instituciones sin personalidad jurídica, podrán ser responsables del tratamiento o encargados del tratamiento únicamente si así queda establecido por disposiciones jurídicas específicas.

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 el departamento de marketing. El departamento de marketing no puede ser el responsable del tratamiento, ya que no posee una identidad jurídica independiente.

En los grupos de empresa, la empresa matriz y cada filial, dado que son personas jurídicas independientes, cuentan como responsables del tratamiento o encargados del tratamiento diferentes. Como consecuencia de este estatuto jurídicamente diferenciado, la transferencia de datos entre los miembros de un grupo de empresas precisará una base jurídica específica. No hay privilegios que permitan el intercambio de datos personales como tal entre entidades jurídicas distintas dentro de un grupo de empresas.

En este contexto, cabe mencionar el papel de los particulares. **Conforme al Derecho de la UE**, los particulares, al tratar datos sobre otras personas en el ejercicio de actividades exclusivamente particulares o domésticas, no entran en el ámbito de aplicación de la Directiva de protección de datos; no se consideran responsables del tratamiento.[78]

Sin embargo, la jurisprudencia ha considerado que la legislación en materia de protección de datos será aplicable, no obstante, cuando un particular, al utilizar Internet, publica datos sobre otros.

78 Directiva de protección de datos, considerando 12 y el artículo 3, apartado 2, último inciso.

Ejemplo: El TJUE sostuvo en el asunto *Bodil Lindqvist*[79] 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 95/46».[80]

Dicho tratamiento de datos personales no entra dentro del ámbito de aplicación de las actividades exclusivamente personales o domésticas, que quedan fuera del ámbito de aplicación de la Directiva de protección de datos, 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 determinado de personas».[81]

Responsable del tratamiento

Según el Derecho de la UE, se define al responsable del tratamiento como aquella persona que «solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales».[82] La decisión del responsable del tratamiento establecerá el motivo y el modo en que los datos serán tratados. **Según el Derecho del CdE**, la definición de «responsable del tratamiento» menciona, además, que el responsable del tratamiento decidirá qué categorías de datos personales deberán ser almacenadas.[83]

El Convenio nº 108 hace referencia en su definición de responsable del tratamiento a otro aspecto del control que merece tenerse en cuenta. Esta definición se refiere a la cuestión de quién puede tratar lícitamente ciertos datos para un fin determinado. Sin embargo, cuando se producen operaciones de tratamiento supuestamente ilegales y debe encontrarse al responsable del tratamiento, se considerará como responsable del tratamiento a la persona o entidad, como una empresa o una administración, que decidió que los datos debían ser tratados, con independencia de si estaba

79 TJUE, asunto C-101/01, *Bodil Lindqvist*, de 6 de noviembre de 2003.

80 *Ibid.*, apartado 27.

81 *Ibid.*, apartado 47.

82 Directiva de protección de datos, artículo 2, letra d).

83 Convenio nº 108, artículo 2, letra d).

legalmente autorizado o no para ello.[84] Por lo tanto, la solicitud de supresión siempre deberá ir dirigida al responsable del tratamiento «real».

Corresponsabilidad

La definición de «responsable del tratamiento» en la Directiva de protección de datos establece que puede haber varias entidades jurídicamente separadas que juntas o conjuntamente con otras actúen como responsable del tratamiento. Esto significa que deciden juntos tratar los datos para un fin común.[85] Esto es legalmente posible, sin embargo, solo en los casos en que una base jurídica específica establezca el tratamiento conjunto de datos con un fin común.

Ejemplo: Una base de datos desarrollada conjuntamente por varias entidades de crédito sobre sus clientes morosos es un ejemplo común de tratamiento conjunto de los datos. Cuando una persona solicita una línea de crédito de un banco que es uno de los responsables del tratamiento conjunto de los datos, la entidad bancaria comprueba la base de datos para que le ayude a tomar decisiones informadas sobre la solvencia del solicitante.

El Reglamento no indica expresamente si la corresponsabilidad exige que el fin compartido sea el mismo para cada uno de los responsables del tratamiento ni si resulta suficiente que sus fines se solapen solo parcialmente. Sin embargo, a escala europea aún no hay disponible jurisprudencia relevante ni tampoco existe claridad respecto de las consecuencias relacionadas con la responsabilidad. El Grupo del artículo 29 aboga por una interpretación más amplia del concepto de corresponsabilidad con el fin de permitir cierta flexibilidad que responda a la creciente complejidad de la actual realidad en materia de tratamiento de datos.[86] Un asunto que implicaba a la Sociedad de Telecomunicaciones Interbancarias Mundiales (*Society for Worldwide Interbank Financial Telecommunication* – SWIFT) ilustra la postura 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,

84 Véase, asimismo, el Grupo del artículo 29 (2010), *Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»*, WP 169, de 16 de febrero de 2010, p. 15.

85 Directiva de protección de datos, artículo 2, letra d).

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

para realizar transferencias de datos durante las transacciones bancarias. SWIFT comunicó dichos datos sobre transacciones bancarias, almacenados en un centro de servicio informático de Estados Unidos, al Departamento del Tesoro estadounidense, sin que las entidades bancarias europeas que utilizaban sus servicios le hubieran ordenado que lo hiciera. El Grupo del artículo 29 al evaluar la licitud de dicha situación, llegó a la conclusión de que las entidades bancarias que utilizan 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.[87] SWIFT, al decidir difundir los datos, asumió de manera ilícita la función de responsable del tratamiento; obviamente, las entidades bancarias habían incumplido su obligación de supervisar al encargado del tratamiento y, por lo tanto, no quedaban exonerados por completo de su responsabilidad como responsables del tratamiento conjunto de los datos. Esta situación da lugar a una corresponsabilidad sobre el tratamiento.

Encargado del tratamiento

Según el Derecho de la UE, el encargado del tratamiento se define como la persona que trata datos personales por cuenta del responsable del tratamiento.[88] Las actividades que le son atribuidas pueden limitarse a una tarea o contexto específicos o pueden ser bastante generales e integrales.

Según el Derecho del CdE, el significado de encargado del tratamiento coincide con el que proporciona el Derecho de la UE.

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

Ejemplos: La empresa Everready se especializa en el tratamiento de datos para la administración de datos sobre los recursos humanos para otras empresas. En esta función, Everready es un encargado del tratamiento.

87 Grupo 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, de 22 de noviembre de 2006.

88 Directiva de protección de datos, artículo 2, letra e).

En cambio, en los casos en que Everready trata los datos de sus propios empleados, actúa como responsable de las operaciones de tratamiento de datos para cumplir sus obligaciones como empresario.

La relación entre el responsable del tratamiento y el encargado del tratamiento

Tal como hemos visto, el responsable del tratamiento se define como aquella persona que determina los fines y los medios del tratamiento.

Ejemplo: El director de la empresa Sunshine decide que la empresa Moonlight, especialista en análisis de mercado, realizará un análisis de mercado de los datos de los clientes de Sunshine. Aunque la tarea de determinar los medios de tratamiento se delegue a Moonlight, la empresa Sunshine sigue siendo la responsable del tratamiento y Moonlight es únicamente la encargada del tratamiento, ya que, según el contrato, Moonlight podrá utilizar los datos de los clientes de la empresa Sunshine únicamente para los fines que esta última determine.

Si la facultad de determinar los medios de tratamiento se delega en el encargado del tratamiento, el responsable del tratamiento deberá, sin embargo, tener la posibilidad de interferir en las decisiones del encargado relacionadas con los medios del tratamiento. La responsabilidad general todavía queda en manos del responsable del tratamiento, quien deberá supervisar a los encargados del tratamiento para garantizar que sus decisiones cumplen con la legislación en materia de protección de datos. Es probable que se interprete que un contrato que prohíbe al responsable del tratamiento interferir en las decisiones del encargado del tratamiento deriva en una corresponsabilidad sobre el tratamiento, según la cual ambas partes comparten la responsabilidad legal propia del responsable del tratamiento.

Asimismo, si el encargado del tratamiento no respeta las limitaciones del uso de los datos establecidas por el responsable del tratamiento, se habrá convertido en el responsable del tratamiento, al menos en la medida en que haya incumplido las instrucciones. Lo más probable es que esto haga que el encargado del tratamiento se convierta en el responsable del tratamiento que actúa de forma ilícita. A su vez, el responsable del tratamiento inicial deberá explicar cómo el encargado del tratamiento ha podido incumplir su mandato. De hecho, el Grupo del artículo 29 tiende a presumir la existencia de una corresponsabilidad sobre el tratamiento en dichos

casos, ya que esto resulta ser la mejor protección de los intereses de los interesados.[89] Una importante consecuencia de la corresponsabilidad debería ser la responsabilidad solidaria por daños y perjuicios, lo cual proporciona a los interesados un abanico más amplio de recursos.

También pueden plantearse cuestiones relativas al reparto de la responsabilidad cuando el responsable del tratamiento es una pequeña empresa y el encargado del tratamiento es una gran empresa corporativa que tiene la facultad de dictar las condiciones de sus servicios. En dichas circunstancias, sin embargo, el Grupo del artículo 29 mantiene que el nivel de responsabilidad no debería disminuir, basándose en el desequilibrio económico y que debería mantenerse el significado del concepto de responsable del tratamiento.[90]

En aras de la claridad y la transparencia, los detalles de la relación entre el responsable del tratamiento y el encargado del tratamiento deberán quedar registrados mediante un contrato por escrito.[91] No disponer de tal contrato constituye un incumplimiento de la obligación del responsable del tratamiento de facilitar documentación por escrito de las responsabilidades mutuas, y podría conllevar la imposición de sanciones.[92]

Es posible que los encargados del tratamiento deseen delegar determinadas tareas a otros subencargados del tratamiento. Esto está permitido por la ley y dependerá de lo que se haya especificado en las cláusulas contractuales entre el responsable del tratamiento y el encargado del tratamiento, tanto si la autorización del responsable del tratamiento resulta necesaria en cada uno de los casos individuales, como si basta únicamente con informar de ello.

Según el Derecho del CdE, la interpretación de los conceptos de responsable del tratamiento y de encargado del tratamiento descrita anteriormente resulta

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

90 Grupo del artículo 29 (2010), *Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»*,WP 169, Bruselas, de 16 de febrero de 2010, p. 26.

91 Directiva de protección de datos, artículo 17, apartados 3 y 4.

92 Grupo del artículo 29 (2010), *Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»*, WP 169, Bruselas, de 16 de febrero de 2010, p. 27.

completamente aplicable, tal como demuestran las recomendaciones que se han desarrollado con arreglo al Convenio nº 108.[93]

2.3.2. Destinatarios y terceros

La diferencia entre estas dos categorías de personas o entidades, que fueron introducidas por la Directiva de protección de datos, reside principalmente en su relación con el responsable del tratamiento y, en consecuencia, en su autorización para acceder a los datos personales que dicho responsable conserva.

Un «tercero» es una persona que se distingue jurídicamente del responsable del tratamiento. La difusión de datos a un tercero, por lo tanto, siempre exigirá una base jurídica específica. De conformidad con el artículo 2, letra f), de la Directiva de protección de datos, un tercero es «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento». Esto significa que las personas que trabajan para otra organización, incluso si esta pertenece al mismo grupo o sociedad de cartera, serán en general «terceros» y, en cambio, las filiales de un banco que tratan las cuentas de los clientes bajo la autoridad directa de la sede no serían «terceros».[94]

El «destinatario» es un término más amplio que «tercero». En el sentido del artículo 2, letra g), de la Directiva de protección de datos, un destinatario es «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero». Este destinatario podrá ser, bien una persona externa al responsable del tratamiento o al encargado del tratamiento (en este último caso, estaríamos ante un tercero) o bien una persona de dentro de la organización del responsable del tratamiento o del encargado del tratamiento, como un empleado u otro departamento de la misma empresa o autoridad.

La distinción entre destinatarios y terceros resulta importante únicamente respecto de las condiciones de la difusión lícita de los datos. Los empleados del responsable del tratamiento o del encargado del tratamiento podrán, sin que sean necesarios otros requisitos legales, ser destinatarios de los datos personales si están implicados

93 Véase, por ejemplo, la Recomendación de creación de perfiles, artículo 1.

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

en las operaciones de tratamiento del responsable del tratamiento o del encargado del tratamiento. Por otro lado, un tercero, al ser jurídicamente independiente del responsable del tratamiento o del encargado del tratamiento, no está autorizado a utilizar los datos personales tratados por estos últimos, salvo por causas jurídicas específicas en un determinado caso. Por lo tanto, los «terceros destinatarios» de datos siempre necesitarán una base jurídica para recibir de forma lícita los datos personales.

Ejemplo: El empleado de un encargado del tratamiento que utilice datos personales para realizar las tareas que le han sido atribuidas por el empresario será un destinatario de los datos pero no un tercero, ya que utiliza los datos en nombre del encargado del tratamiento y conforme a sus instrucciones.

Si, en cambio, el mismo empleado decide utilizar los datos, a los que tiene acceso como empleado del encargado del tratamiento, para sus propios fines y los vende a otra empresa, entonces el empleado habrá actuado como un tercero y ya no estará siguiendo las órdenes del encargado del tratamiento (el empresario). Como tercero, el empleado necesitará una base jurídica para adquirir y vender los datos. En este ejemplo, el empleado no contaba ciertamente con dicha base jurídica, por lo que estas acciones son ilegales.

2.4. Consentimiento

Puntos clave

- El consentimiento como base jurídica para el tratamiento de datos personales debe ser libre, específico e informado.
- El consentimiento debe haberse dado de forma inequívoca. El consentimiento podrá darse tanto de forma expresa como implícita por medio de acciones que no dejen duda alguna de que el interesado ha accedido al tratamiento de sus datos.
- El tratamiento de datos sensibles sobre la base del consentimiento exige que este sea un consentimiento expreso.
- El consentimiento puede retirarse en cualquier momento.

El consentimiento significa «toda manifestación de voluntad, libre, específica e informada del interesado».[95] En numerosos casos, supone la base jurídica para un tratamiento de datos legítimo (véase el apartado 4.1).

2.4.1. Los elementos del consentimiento válido

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:

- no se debe haber sometido al interesado a ninguna presión para que diera su consentimiento;
- el interesado deberá haber sido debidamente informado sobre el objeto y las consecuencias de su consentimiento; y
- el ámbito de aplicación del consentimiento deberá ser razonablemente concreto.

El consentimiento será válido, en el sentido de la legislación en materia de protección de datos, únicamente si se cumplen todos estos requisitos.

El Convenio nº 108 no incluye una definición de consentimiento, sino que esta es una cuestión que se remite a la legislación nacional. Sin embargo, **según el Derecho del CdE**, los elementos del consentimiento válido coinciden con aquellos que se han citado anteriormente, tal como establecen las recomendaciones que han sido desarrolladas, con arreglo al Convenio nº 108.[96] Los requisitos del consentimiento son los mismos que los de una declaración de intenciones válida con arreglo al Derecho civil europeo.

Los requisitos adicionales con arreglo al Derecho civil para que el consentimiento sea válido, como la capacidad jurídica, se aplican evidentemente en el contexto de la protección de datos, puesto que dichos requisitos son requisitos legales previos fundamentales. El consentimiento no válido de las personas que no poseen capacidad jurídica tendrá como consecuencia la falta de base legal para el tratamiento de datos de dichas personas.

95 Directiva de protección de datos, artículo 2, letra h).

96 Véase, por ejemplo, el convenio nº 108, Recomendación sobre datos estadísticos, apdo. 6.

El consentimiento podrá darse de forma explícita[97] o no explícita. El primero no deja dudas sobre las intenciones del interesado y podrá formularse tanto oralmente como por escrito; el segundo se deriva de las circunstancias. Cada consentimiento debe darse de forma inequívoca.[98] Esto significa que no debería quedar ninguna duda razonable de que el interesado deseaba comunicar su aceptación para permitir el tratamiento de sus datos. La deducción del consentimiento de la simple inactividad no constituye un consentimiento inequívoco, por ejemplo. En los casos en que los datos que deben tratarse sean datos de carácter sensible, es obligatorio un consentimiento explícito, que deberá ser inequívoco.

Consentimiento libre

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».[99]

Ejemplo: En muchos aeropuertos, los pasajeros deben atravesar escáneres de personas para poder acceder a la zona de embarque.[100] Dado que los datos de los pasajeros se tratan en el momento en que tiene lugar el control, el tratamiento debe cumplir alguno de los fundamentos jurídicos previstos en el artículo 7 de la Directiva de protección de datos (véase el apartado 4.1.1). Atravesar los escáneres corporales se presenta a veces como una opción para los pasajeros, lo cual implica que el tratamiento podría justificarse por su consentimiento. Los pasajeros, sin embargo, podrían temer que su negativa a atravesar los escáneres corporales puede crear sospechas o dar lugar a controles adicionales como el cacheo. Muchos pasajeros consienten en ser escaneados porque así evitan posibles problemas o retrasos. Es presumible que este tipo de consentimiento no sea suficientemente libre.

Por lo tanto, un sólido fundamento legítimo únicamente puede encontrarse en un acto del legislador, basado en el artículo 7, letra e), de la Directiva de protección de datos, del que se deriva la obligación que tienen los pasajeros de cooperar debido a un interés público superior. Dicha legislación también podría prever

97 Directiva de protección de datos, artículo 8, apartado 2.

98 *Ibid.*, artículo 7, letra a), y artículo 26, apartado 1.

99 Véase asimismo el Grupo del artículo 29 (2011), *Dictamen 15/2011 sobre la definición de consentimiento*, WP 187, Bruselas, de 13 de julio de 2011, p. 12.

100 Este ejemplo se ha extraído de *Ibid.*, p. 15.

la elección por la persona entre el escáner y el control manual, pero solo con carácter complementario y como medida adicional del control fronterizo necesario en circunstancias específicas. Esto es lo que la Comisión Europea estableció en dos reglamentos relacionados con los escáneres de seguridad en 2011.[101]

El consentimiento libre también podría verse amenazado en las situaciones de subordinación, en las cuales existe un significativo desequilibrio, económico o de otro tipo, entre el responsable del tratamiento que solicita el consentimiento y el interesado que lo otorga.[102]

Ejemplo: Una gran empresa tiene pensado crear una base de datos que incluye los nombres de todos los empleados, su función en la empresa y sus direcciones profesionales, únicamente para mejorar las comunicaciones internas de la empresa. El jefe de personal propone añadir una fotografía de cada empleado a la base de datos para, por ejemplo, facilitar que los empleados se reconozcan en las reuniones. Los representantes de los trabajadores piden que esto se haga solo si los empleados individuales dan su consentimiento para ello.

En dicha situación, el consentimiento de un empleado debe ser reconocido como fundamento jurídico para el tratamiento de las fotografías en la base de datos porque queda claro que la publicación de una fotografía en la misma no tiene consecuencias negativas por sí misma y, además, resulta creíble que el empleado no tenga que enfrentarse a las repercusiones negativas emprendidas por el empresario si no accede a que se publique su fotografía en dicha base de datos.

Esto no significa, sin embargo, que el consentimiento nunca pueda ser válido en circunstancias en que la falta de consentimiento tuviera consecuencias negativas. Si,

101 Reglamento (UE) nº 1141/2011 de la Comisión, de 10 de noviembre de 2011, por el que se modifica el Reglamento (CE) nº 272/2009, que completa las normas básicas comunes sobre la seguridad de la aviación civil, en lo que respecta al uso de escáneres de seguridad en los aeropuertos de la UE, DO 2011 L 293, y el Reglamento de Ejecución (UE) nº 1147/2011, de 11 de noviembre de 2011, que modifica el Reglamento (UE) nº 185/2010, y por el que se desarrollan las normas básicas comunes sobre la seguridad de la aviación civil en lo que respecta al uso de escáneres de seguridad en los aeropuertos de la UE, DO 2011 L 294.

102 Véase, asimismo, Grupo del artículo 29 (2001), *Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral*, WP 48, Bruselas, de 13 de septiembre de 2001; y Grupo 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, de 25 de noviembre de 2005.

por ejemplo, la consecuencia de la falta de consentimiento para tener una tarjeta de cliente de un supermercado es solo que no se reciben descuentos en los precios de algunos productos, el consentimiento todavía constituirá una base jurídica válida para tratar los datos personales de los clientes que han dado su consentimiento para tener dicha tarjeta. No existe una situación de subordinación entre la empresa y el cliente y, las consecuencias de la falta de consentimiento no son lo suficientemente graves para evitar que el interesado escoja libremente.

Por otro lado, en los casos en que única y exclusivamente puedan obtenerse productos o servicios lo suficientemente importantes si determinados datos personales se difunden a terceros, el consentimiento a la difusión de sus datos por parte del interesado normalmente no se considerará una libre elección y, por tanto, no será válido con arreglo a la legislación en materia de protección de datos.

Ejemplo: El consentimiento que los pasajeros manifiestan a la compañía aérea, la cual transmite los denominados Registros de Nombres de Pasajeros (PNR), en concreto los datos sobre su identidad, hábitos alimentarios o problemas de salud a las 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 pasajeros no tienen elección si desean visitar este país. Si dichos datos se transfieren de forma lícita, se exigirá otra base jurídica distinta del consentimiento, la cual lo más probablemente sea una legislación específica.

Consentimiento informado

El interesado deberá contar con la suficiente información antes de tomar su decisión. El que la información sea suficiente sólo puede determinarse caso por caso. Normalmente, el consentimiento informado incluirá una descripción precisa y fácilmente comprensible de la cuestión que requiere dicho consentimiento y, además, un resumen de las consecuencias del consentimiento o de la falta del mismo. El lenguaje que se utiliza para facilitar la información debería adaptarse a los destinatarios previsibles de la información.

La información también debe estar fácilmente disponible para los interesados. La accesibilidad y la visibilidad de la información son elementos importantes. En un entorno en línea, puede que sea una buena solución colocar avisos de información

por capas de forma que el interesado pueda acceder no solo a una versión concisa de la información sino además a una versión más ampliada.

Consentimiento específico

Para que sea válido, el consentimiento también debe ser específico. Esto va estrechamente unido a la calidad de la información que se facilita sobre el objeto del consentimiento. En este contexto, serán relevantes 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 haber sido previsto razonablemente cuando se dio el consentimiento inicial.

Ejemplo: En el asunto *Deutsche Telekom AG*,[103] el TJUE abordó la cuestión de si un proveedor de telecomunicaciones que debía transmitir datos personales de los abonados, de conformidad con el artículo 12 de la *Directiva sobre la privacidad en las comunicaciones electrónicas*[104] precisaba que los interesados renovasen su consentimiento, ya que los destinatarios no habían sido mencionados inicialmente cuando se dio el consentimiento.

El TJUE sostuvo que en virtud de dicho artículo la renovación del consentimiento antes de transmitir los datos no era necesaria porque los interesados tenían, en virtud de esta disposición, la posibilidad de consentir únicamente para la finalidad del tratamiento, que es la publicación de sus datos, y no podían escoger entre diversas guías en las que podrían publicarse los datos.

Como el tribunal subrayó, «de una interpretación lógica y sistemática del artículo 12 de la Directiva la 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».[105] Además, «es la propia publicación de los datos de carácter personal en una guía con una

103 TJUE, en el asunto C-543/09, *Deutsche Telekom AG contra Alemania*, de 5 de mayo de 2011; véanse, en especial, los apdos. 53 y 54.

104 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*).

105 TJUE, asunto C-543/09, *Deutsche Telekom AG contra Alemania*, de 5 de mayo de 2011; véase, en especial, el apdo. 61.

finalidad particular lo que puede resultar perjudicial para un abonado»[106] y no quién es el autor de dicha publicación.

2.4.2. El derecho a revocar el consentimiento en cualquier momento

La Directiva de protección de datos no menciona un derecho general a revocar el consentimiento en cualquier momento. Se presume generalmente, sin embargo, que dicho derecho existe y que el interesado debe poder ejercerlo a su elección. No debería exigirse como requisito justificar la revocación ni debería haber ningún riesgo de consecuencias negativas más allá del hecho de que se terminen todos los beneficios que pudieran derivarse del uso de los datos previamente acordado.

Ejemplo: Un cliente acepta recibir correo promocional a la dirección que facilita a un responsable del tratamiento de datos. En caso de que el cliente revoque su consentimiento, el responsable del tratamiento deberá cesar inmediatamente de enviar este tipo de correo. No deberían imponerse consecuencias punitivas como cargos económicos.

Si el cliente recibía un 5 % de descuento en el coste de una habitación de hotel a cambio de la aceptación del uso de sus datos para correo promocional, la revocación del consentimiento para recibir dicho correo en un momento posterior no debería derivar en tener que devolver dichos descuentos.

106 *Ibid.*, véase, en particular, el apdo. 62.

3

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

UE	Materias cubiertas	CdE
Directiva de protección de datos, artículo 6, apartado 1, letras a) y b) TJUE, asunto C-524/06, *Huber contra Bundesrepublik Deutschland*, de 16 de diciembre de 2008 TJUE, asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR (C-92/09) y Hartmut Eifert (C-93/09) contra Land Hessen*, de 9 de noviembre de 2010	**El principio de tratamiento lícito**	Convenio nº 108, artículo 5, letras a) y b) TEDH, *Rotaru contra Rumanía* [GS], nº 28341/95, de 4 de mayo de 2000 TEDH, *Taylor-Sabori contra Reino Unido*, nº 47114/99, de 22 de octubre de 2002 TEDH, *Peck contra el Reino Unido*, nº 44647/98, de 28 de enero 2003 TEDH, *Khelili contra Suiza*, nº 16188/07, de 18 de octubre de 2011 TEDH, *Leander contra Suecia*, nº 9248/81, de 26 de marzo de 1987
Directiva de protección de datos, artículo 6, apartado 1, letra b)	**El principio de finalidad y principio de limitación de la finalidad**	Convenio nº 108, artículo 5, letra b)
	Los principios de calidad de los datos	
Directiva de protección de datos, artículo 6, apartado 1, letra c)	**Pertinencia de los datos**	Convenio nº 108, artículo 5, letra c)
Directiva de protección de datos, artículo 6, apartado 1, letra d)	**Exactitud de los datos**	Convenio nº 108, artículo 5, letra d)

Directiva de protección de datos, artículo 6, apartado 1, letra e)	**Conservación de los datos**	Convenio nº 108, artículo 5, letra e)
Directiva de protección de datos, artículo 6, apartado 1, letra e)	**Excepción para investigación científica y estadística**	Convenio nº 108, artículo 9, apartado 3
Directiva de protección de datos, artículo 6, apartado 1, letra a)	**El principio de tratamiento leal**	Convenio nº 108, artículo 5, letra a) TEDH, *Haralambie contra Rumanía*, nº 21737/03, de 27 de octubre de 2009 TEDH, *K.H. y otros contra Eslovaquia*, nº 32881/04, de 6 de noviembre 2009
Directiva de protección de datos, artículo 6, apartado 2	**El principio de rendición de cuentas**	

Los principios establecidos en el artículo 5 del Convenio nº 108 integran la esencia de la legislación europea en materia de protección de datos. También se contemplan en el artículo 6 de la Directiva de protección de datos como punto de partida para disposiciones más detalladas en los artículos posteriores de dicho instrumento. Toda la legislación posterior en materia de protección de datos tanto a escala de la UE como del Consejo de Europa deberá respetar estos principios, los cuales deberán tenerse en cuenta a la hora de interpretar dicha legislación. Todas las excepciones y limitaciones a estos principios fundamentales deberán establecerse a escala nacional;[107] deberán ser establecidas por la ley, servir a un fin legítimo y ser necesarias en una sociedad democrática. Deben cumplirse las tres condiciones.

3.1. El principio de tratamiento lícito

Puntos clave

- Para comprender el principio de tratamiento lícito, debemos hacer referencia a las condiciones de las limitaciones lícitas del derecho a la protección de los datos, a la luz del artículo 52, apartado 1, de la Carta, así como a los requisitos de las injerencias justificadas, de conformidad con el artículo 8, apartado 2, del CEDH.

107 Convenio nº 108, artículo 9, apartado 2; Directiva de protección de datos, artículo 13.

- De este modo, el tratamiento de datos personales será lícito únicamente si:
  - se realiza de conformidad con la ley;
  - sirve a un fin legítimo; y
  - es necesario en una sociedad democrática para lograr el fin legítimo.

De conformidad con la legislación en materia de protección de datos de la UE y del Consejo de Europa, el principio de tratamiento lícito es el principio que primero se nombra y se recoge casi de forma idéntica tanto en el artículo 5 del Convenio nº 108 como en el artículo 6 de la Directiva de protección de datos.

Ninguna de estas disposiciones incluye una definición de lo que constituye un «tratamiento lícito». Para comprender este término jurídico, es necesario hacer referencia a la injerencia justificada con arreglo al CEDH, tal como ha sido interpretado por la jurisprudencia del TEDH, y a las condiciones de las limitaciones legítimas al amparo del artículo 52 de la Carta.

3.1.1. Los requisitos para una injerencia justificada con arreglo al CEDH

El tratamiento de los datos personales puede constituir una injerencia en el derecho al respeto a la vida privada del interesado. Sin embargo, el respeto a la vida privada no es un derecho absoluto, sino que debe ponderarse y conciliarse con otros intereses legítimos, ya sean de otras personas (intereses privados) o de una sociedad en su conjunto (intereses públicos).

Las condiciones en que queda justificada la injerencia del Estado son las siguientes:

De conformidad con la ley

De conformidad con la jurisprudencia del TEDH, la injerencia se realizará de conformidad con la ley si está basada en una disposición del derecho nacional que posee determinadas características. La ley deberá ser «accesible para las personas a las cuales concierna y previsible en cuanto a sus efectos».[108] Una norma es previsible «si está formulada con la suficiente precisión como para permitir que cualquier persona

108 TEDH, *Amann contra Suiza* [GS], nº 27798/95, de 16 de febrero de 2000, apdo. 50; véase, asimismo, TEDH, *Kopp contra Suiza*, nº 23224/94, de 25 de marzo de 1998, apdo. 55 y TEDH, *Iordachi y otros contra Moldavia*, nº 25198/02, de 10 de febrero de 2009, apdo. 50.

– si es necesario, con adecuado asesoramiento – regule su comportamiento».[109] En este sentido, «el grado de precisión exigible de "la ley" dependerá de la materia en particular».[110]

Ejemplo: En el asunto *Rotaru contra Rumanía*,[111] el TEDH consideró que existía una violación del artículo 8 del CEDH porque la legislación rumana permitía la recopilación, el registro y el almacenamiento en archivos secretos de información que afecta a la seguridad nacional, sin establecer límites en el ejercicio de dichos poderes, los cuales quedaban a discreción de las autoridades. Por ejemplo, la legislación nacional no definía el tipo de información que podría ser tratada, ni las categorías de personas contra las que podrían adoptarse medidas de vigilancia, ni las circunstancias en las que dichas medidas podían adoptarse ni el procedimiento que debía seguirse. Debido a estas irregularidades, el Tribunal concluyó que la legislación nacional no cumplía el requisito de previsibilidad con arreglo al artículo 8 del CEDH y que se había infringido lo dispuesto en dicho artículo.

Ejemplo: En la sentencia *Taylor-Sabori contra el Reino Unido*,[112] el demandante había sido objeto de vigilancia por parte de la policía. Utilizando una «clon» del buscapersonas del demandante, la policía pudo interceptar los mensajes que se habían enviado a dicho demandante. Este fue posteriormente detenido y se le acusó 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 intercepción de comunicaciones transmitidas a través de un sistema de telecomunicaciones privado. La injerencia en sus derechos no había sido

109 TEDH, *Amann contra Suiza* [GS], nº 27798/95, de 16 de febrero de 2000, apdo. 56; véase, asimismo, TEDH, *Malone contra el Reino Unido*, nº 8691/79, de 26 de abril de 1985, apdo. 66; TEDH, *Silver y otros contra el Reino Unido*, nºs 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, de 25 de marzo de 1983, apdo. 88.

110 TEDH, *The Sunday Times contra el Reino Unido*, nº 6538/74, de 26 de abril de 1979, apdo. 49; véase, asimismo, TEDH, *Silver y otros contra el Reino Unido*, nºs 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, de 25 de marzo de 1983, apdo. 88.

111 TEDH, *Rotaru contra Rumanía* [GS], nº 28341/95, de 4 de abril de 2000, apdo. 57; véase, asimismo, TEDH, *Association for European Integration and Human Rights y Ekimdzhiev contra Bulgaria*, nº 62540/00, de 28 de junio de 2007; TEDH, *Shimovolos contra Rusia*, nº 30194/09, de 21 de junio de 2011; y TEDH, *Vetter contra Francia*, nº 59842/00, de 31 de mayo de 2005.

112 TEDH, *Taylor-Sabori contra el Reino Unido*, nº 47114/99, de 22 de octubre de 2002.

realizada, por lo tanto, «de conformidad con la ley». El TEDH concluyó que había existido una violación del artículo 8 del CEDH.

Perseguir un fin legítimo

El fin legítimo puede ser tanto uno de los intereses públicos mencionados o los derechos y libertades de otras personas.

Ejemplo: En el asunto *Peck contra el Reino Unido*,[113] el demandante había intentado suicidarse en la calle cortándose las muñecas, sin darse cuenta de que una cámara de CCTV le había filmado llevando a cabo dicho acto. Después de que la policía, que estaba vigilando las cámaras de vigilancia de circuito cerrado de televisión, le rescatara la autoridad policial transmitió la grabación a los medios de comunicación, quienes la publicaron sin ocultar la cara 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».[114]

Ejemplo: En el asunto *Khelili contra Suiza*,[115] durante un control policial, la policía encontró 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. Nº de teléfono [...]». La demandante alegó que, tras el descubrimiento, la policía introdujo su nombre en sus registros 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

113 TEDH, *Peck contra el Reino Unido*, nº 44647/98, de 28 de enero 2003, en especial, el apdo. 85.

114 TEDH, *Leander contra Suecia*, nº 9248/81, de 11 de julio de 1985, apdo. 58.

115 TEDH, *Khelili contra Suiza*, nº 16188/07, de 18 de octubre de 2011.

un primer momento que la conservación de los datos personales de un particular, sobre la base de que dicha persona podría cometer otro delito, podría ser proporcionado en determinadas circunstancias. Sin embargo, en el caso de la demandante, el argumento de prostitución ilícita parecía demasiado vago y general, no se apoyaba en hechos concretos ya que aquella no 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. Al considerar que esta era una cuestión para la cual las autoridades debían demostrar la exactitud de los datos almacenados sobre la demandante, así como la gravedad de la injerencia en los derechos de dicha 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.

Ejemplo: En el asunto *Leander contra Suecia*,[116] el TEDH resolvió que el control secreto de personas que solicitan puestos de importancia para la seguridad nacional no es contrario, en sí mismo, con el requisito de ser necesario en una sociedad democrática. Las garantías específicas establecidas en la legislación nacional para la protección de los intereses del interesado, por ejemplo, los controles ejercidos por el Parlamento y el Ministro de Justicia, derivaron en que el TEDH concluyera 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 disponible, el Estado demandado estaba autorizado a considerar que, en el asunto 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.

3.1.2. Las condiciones de las limitaciones lícitas con arreglo a la Carta de la UE

La estructura y el texto de la Carta son distintos de los del CEDH. La Carta no habla sobre las injerencias en los derechos garantizados aunque incluye una disposición sobre la(s) limitación(es) 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, por tanto, del ejercicio del

116 TEDH, *Leander contra Suecia*, nº 9248/81, de 11 de julio de 1985, apdos. 59 y 67.

derecho a la protección de los datos personales, como el tratamiento de datos personales, se admitirá únicamente si:

- está establecida por la ley;
- respeta el contenido esencial de dichos derechos y libertades;
- es necesaria, con arreglo al principio de proporcionalidad;
- responde efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

Ejemplos: En el asunto *Volker und Markus Schecke*,[117] el TJUE concluyó que al imponer una obligación de publicar los datos personales 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 han percibido 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) nº 1290/2005 y declarar inválido el Reglamento (CE) nº 259/2008 en su totalidad.[118]

A pesar de la distinta redacción, las condiciones del tratamiento lícito del artículo 52, apartado 1, de la Carta evocan las contempladas en el artículo 8, apartado 2, del CEDH. De hecho, debe considerarse que las condiciones que se enumeran en el artículo 52, apartado 1, de la Carta cumplen con lo dispuesto en el artículo 8, apartado 2, del CEDH, puesto que el artículo 52, apartado 3, de la Carta establece en su primera frase que «en la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección

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

118 Reglamento (CE) nº 1290/2005, de 21 de junio de 2005, sobre la financiación de la política agrícola común, DO 2005 L 209; Reglamento (CE) nº 259/2008 de la Comisión, de 18 de marzo de 2008, por el que se establecen disposiciones de aplicación del Reglamento (CE) nº 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.

de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio».

Sin embargo, de conformidad con el artículo 52, apartado 3, última frase, «esta disposición no impide que el Derecho de la Unión conceda una protección más extensa». En el contexto de la comparación entre el artículo 8, apartado 2, del CEDH y del artículo 52, apartado 3, frase primera, lo anterior únicamente puede significar que las condiciones para las injerencias justificadas con arreglo al artículo 8, apartado 2, del CEDH constituyen los requisitos mínimos para las limitaciones lícitas del derecho a la protección de datos con arreglo a la Carta. Por consiguiente, el tratamiento lícito de datos personales exige, con arreglo al Derecho de la UE, que se cumplan al menos las condiciones del artículo 8, apartado 2, del CEDH. Sin embargo, dicho Derecho podría establecer requisitos adicionales para casos específicos.

El artículo 6, apartado 3, del TUE apoya asimismo la correspondencia del principio de tratamiento lícito con arreglo al Derecho de la UE con las disposiciones pertinentes del CEDH, al establecer que «los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales [...], formarán parte del Derecho de la Unión como principios generales».

3.2. Los principios de finalidad y de limitación de la finalidad

Puntos clave

- La finalidad del tratamiento de datos deberá definirse de forma visible antes de que comience el tratamiento.
- De conformidad con el Derecho de la UE, la finalidad del tratamiento debe estar explícitamente definida ; con arreglo al Derecho del CdE, esta cuestión queda a discreción de la legislación nacional.
- El tratamiento con fines no definidos no es conforme con la legislación en materia protección de datos.
- Otros usos de los datos para una finalidad distinta requiere una base jurídica adicional si la nueva finalidad del tratamiento resulta incompatible con la finalidad original.
- La transferencia de datos a terceros es una nueva finalidad que exige la existencia de una base jurídica adicional.

En esencia, el principio de finalidad y el principio de limitación de la finalidad implican que la legitimidad del tratamiento de datos personales dependerá de la finalidad del tratamiento.[119] El responsable del tratamiento deberá especificar y hacer manifiesta la finalidad antes de que comience el tratamiento de datos.[120] De conformidad con el Derecho de la UE, esto debe llevarse a cabo mediante una declaración, en otras palabras, mediante notificación, dirigida a la autoridad de supervisión adecuada o, como mínimo, mediante documentación interna que debe ponerse a disposición por el responsable del tratamiento para su inspección por parte de las autoridades de supervisión y para su acceso por parte del interesado.

El tratamiento de los datos personales para finalidades no definidas y/o ilimitadas se considerará ilícito.

Cada nueva finalidad para el tratamiento de datos deberá contar con 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 nueva finalidad del tratamiento exigirá un fundamento jurídico nuevo e independiente. La comunicación de los datos a terceros deberá someterse a una consideración especialmente cuidadosa, ya que dicha comunicación normalmente constituye una nueva finalidad y, por tanto, exige un nuevo fundamento jurídico, distinto del de la obtención de datos.

Ejemplo: Una compañía aérea obtiene datos de sus pasajeros para hacer reservas para operar el vuelo de manera adecuada. La compañía aérea necesitará datos relativos a: los números de asiento de los pasajeros; las limitaciones físicas especiales, como la necesidad de una silla de ruedas; y las necesidades dietéticas especiales, como la comida kosher o halal. Si se solicita a las compañías aéreas que transmitan estos datos, que están incluidos en el PNR, a las autoridades de inmigración en el puerto de desembarque, estos datos se utilizarán para fines de control de la inmigración, los cuales son distintos de la finalidad inicial de la obtención de los datos. La transferencia de estos datos a la autoridad de inmigración exigirá, por lo tanto, un fundamento jurídico nuevo y autónomo.

119 Convenio nº 108, artículo 5, letra b); Directiva de protección de datos, artículo 6, apartado 1, letra b).

120 Véase, asimismo, Grupo del artículo 29 (2013), *Dictamen 3/2013 sobre la limitación a una finalidad específica*, WP 203, Bruselas, de 2 de abril de 2013.

Al considerar el alcance y los límites de una finalidad particular, el Convenio nº 108 y la Directiva de protección de datos recurren al concepto de compatibilidad: se permite el uso de los datos para fines compatibles sobre la base del fundamento jurídico inicial. Sin embargo, no se proporciona una definición de lo que significa «compatible» sino que dicho concepto es susceptible de interpretación caso por caso.

Ejemplo: La venta de los datos de los clientes de la empresa Sunshine, obtenidos durante la gestión de las relaciones con los clientes (CRM), a Moonlight, una empresa de marketing directo que desea utilizar dichos datos para ayudar a terceras empresas en sus campañas de marketing, constituye una nueva finalidad, que es incompatible con la CRM, la finalidad inicial para la cual la empresa Sunshine obtuvo los datos de los clientes. Por lo tanto, la venta de los datos a la empresa Moonlight precisa contar con un fundamento jurídico propio.

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

La Directiva de protección de datos declara expresamente que «no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas».[121]

Ejemplos: La empresa Sunshine ha recopilado y almacenado datos CRM sobre sus clientes. Se permitirá un uso posterior de dichos datos para un análisis estadístico del comportamiento de compra de sus clientes por parte de la empresa Sunshine, ya que las estadísticas son una finalidad compatible. No será necesario otro fundamento jurídico adicional, como el consentimiento de los interesados.

Si esos mismos datos se transmitieran a un tercero, la empresa Starlight, con fines exclusivamente estadísticos, dicha transmisión sería permisible sin que sea necesaria una base jurídica adicional, aunque únicamente con la condición de que se adopten las garantías oportunas, como el ocultamiento de la

121 Un ejemplo de dichas disposiciones nacionales es la Ley austriaca de protección de datos (*Datenschutzgesetz*), Diario de Legislación Federal I nº 165/1999, apdo. 46, disponible en inglés en: www.dsk.gv.at/DocView.axd?CobId=41936.

identidad de los interesados, puesto que, para fines estadísticos, no son necesarias las identidades.

3.3. Principios de calidad de los datos

Puntos clave

- El responsable del tratamiento deberá aplicar los principios de calidad de los datos en todas las operaciones de tratamiento.
- El principio de conservación de los datos obliga a suprimir los datos tan pronto como ya no sean necesarios para los fines para los que fueron recabados.
- Las excepciones al principio de conservación de los datos deberán estar establecidas por la ley y necesitan garantías específicas para la protección de los interesados.

3.3.1. El principio de pertinencia de los datos

Únicamente se tratarán los datos que sean «adecuados, pertinentes y no excesivos en relación con el fin para el que se obtienen o tratan».[122] Las categorías de datos seleccionados para ser tratados deberán ser necesarias para lograr el objetivo general declarado de las operaciones de tratamiento, y el responsable del tratamiento deberá limitar la obtención de datos estrictamente a la información que resulte directamente pertinente para la finalidad específica perseguida por el tratamiento.

En la sociedad contemporánea, debe hacerse una consideración adicional respecto del principio de pertinencia de los datos, puesto que al utilizar tecnologías especiales para la mejora de la privacidad a veces es posible evitar el uso total de datos personales o utilizar datos pseudonimizados, lo cual supone una solución respetuosa con el derecho a la privacidad. Esto es especialmente adecuado en sistemas de tratamiento más amplios.

Ejemplo: Un ayuntamiento ofrece una tarjeta con chip a los usuarios regulares del sistema de transporte público municipal por el 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

122 Convenio nº 108, artículo 5, letra c), y Directiva de protección de datos, artículo 6, apartado 1, letra c).

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 comprueban de forma electrónica en una base de datos que incluyen los nombres de las personas que han comprado la tarjeta de transporte.

Este sistema no es conforme de forma óptima con el principio de pertinencia, puesto que comprobar si una persona física puede utilizar las instalaciones de transporte podría llevarse a cabo sin tener que comparar los datos personales en el chip de la tarjeta con una base de datos. Bastaría, por ejemplo, con que existiera una imagen electrónica especial, como un código de barras, en el chip de la tarjeta que, al pasarlo frente al dispositivo de lectura, confirmase si la tarjeta es o no válida. Dicho sistema no registraría quién ha utilizado dicha instalación ni en qué momento. No se recopilaría ningún dato personal, lo cual es la solución óptima desde el punto de vista del principio de pertinencia, ya que este principio deriva en la obligación de reducir al mínimo la recopilación de datos.

3.3.2. El principio de exactitud de los datos

El responsable del tratamiento que disponga de información personal no la utilizará sin adoptar las medidas para garantizar, con una certeza razonable, que los datos son exactos y están actualizados.

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

Ejemplo: Una empresa de ventas de mobiliario recopiló datos sobre la identidad y la dirección de los clientes a efectos de la facturación. Seis meses más tarde, la misma empresa desea iniciar una campaña de marketing y, para ello, desea contactar con sus antiguos clientes. Para contactar con ellos, la empresa desea acceder al registro nacional de residentes, el cual es probable que incluya direcciones actualizadas, ya que los residentes están obligados legalmente a informar al registro de su dirección actual. El acceso a los datos de dicho registro se limita a las personas y entidades que pueden proporcionar una causa justificativa.

En esta situación, la empresa no puede utilizar el argumento de que los datos deben guardarse de forma exacta y actualizada para defender que está

autorizada a recopilar datos sobre las nuevas direcciones de todos sus clientes antiguos a partir del registro de residentes. Los datos se obtuvieron durante la facturación. Para esta finalidad la la dirección en el momento de la venta resulta pertinente. No existe base jurídica para recopilar datos sobre las nuevas direcciones, ya que el marketing no es un interés que prevalezca sobre el derecho a la protección de datos y, por tanto, no puede justificar el acceso a los datos del registro.

También habrá casos en que esté legalmente prohibido actualizar los datos almacenados, puesto que la finalidad de dicho almacenamiento es principalmente documentar los acontecimientos.

Ejemplo: El protocolo de una operación médica no debe ser modificado, en otras palabras «actualizado», incluso si las conclusiones incluidas en dicho protocolo resultan ser erróneas. En dichas circunstancias, únicamente podrán hacerse añadidos a las observaciones del protocolo, siempre que queden marcados con claridad como aportaciones realizadas en una fase posterior.

Por otro lado, hay situaciones en las que una comprobación regular de la exactitud de los datos, incluida una actualización, es una necesidad absoluta debido al daño potencial que podría causársele al interesado si los datos siguieran siendo inexactos.

Ejemplo: Si una persona desea celebrar un contrato con una institución bancaria, el banco normalmente comprobará la solvencia del posible cliente. A estos efectos, existen bases de datos específicas que incluyen datos sobre el historial de crédito de los particulares. Si dicha base de datos proporciona datos incorrectos u obsoletos sobre una persona física, dicha persona puede tener graves problemas. Los responsables del tratamiento de dichas bases de datos deberán hacer, por tanto, esfuerzos específicos para seguir el principio de exactitud.

Asimismo, los datos que no hacen referencia a hechos sino a sospechas, como las investigaciones penales, podrán ser recopilados y almacenados, siempre que el responsable del tratamiento disponga de una base jurídica para recopilar dicha información y tenga justificación suficiente para haber establecido dicha sospecha.

3.3.3. El principio de conservación de los datos

El artículo 6, apartado 1, letra e), de la Directiva de protección de datos y, de igual modo, el artículo 5, letra e), del Convenio nº 108 exigen a los Estados miembros para garantizar que los datos personales son «conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.». Por lo tanto, los datos deberán suprimirse cuando se hayan cumplido dichos fines.

En el asunto *S. and Marper*, el TEDH concluyó que los principios esenciales de los instrumentos pertinentes del Consejo de Europa, y la legislación y la práctica de 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.[123]

La limitación en el tiempo para el almacenamiento de los datos personales es aplicable, sin embargo, únicamente a los datos conservados de una forma que permita identificar a los interesados. El almacenamiento lícito de los datos que ya no resulte necesario podrá conseguirse, por lo tanto, mediante la anonimización o la pseudonimización de los datos.

La conservación de los datos con fines históricos, estadísticos o científicos queda expresamente excepcionada del principio de conservación de los datos en la Directiva de protección de datos.[124] Tales almacenamiento y uso continuado de los datos personales deberán, sin embargo, ir acompañados de garantías específicas de conformidad con la legislación nacional.

3.4. El principio de tratamiento leal

Puntos clave

- El tratamiento leal implica la transparencia del tratamiento, en especial respecto de los interesados.

123 TEDH, *S. y Marper contra el Reino Unido*, nº 30562/04 y 30566/04, de 4 de diciembre de 2008; véase, asimismo, por ejemplo, TEDH, *M.M. contra el Reino Unido*, nº 24029/07, de 13 de noviembre de 2012.

124 Directiva de protección de datos, artículo 6, apartado 1, letra e).

- Los responsables del tratamiento deberán informar a los interesados antes del tratamiento de sus datos, al menos respeto de la finalidad del tratamiento y sobre su identidad y su dirección.
- Salvo en los casos expresamente permitidos por la ley, el tratamiento de los datos personales no deberá ser secreto ni encubierto.
- Los interesados tendrán derecho a acceder a sus datos cuando estos estén siendo tratados.

El principio de tratamiento leal regula, fundamentalmente, la relación entre el responsable del tratamiento y el interesado.

3.4.1. Transparencia

El principio establece una obligación para el responsable del tratamiento de mantener informados a los interesados sobre el modo en que sus datos están siendo utilizados.

Ejemplo: En el asunto *Haralambie contra Rumanía*,[125] el demandante solicitó acceso al expediente que la organización del servicio secreto había almacenado sobre él, aunque su petición solo fue atendida cinco años más tarde. 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 proporcionar 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 el 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. Los interesados también tienen derecho a ser informados por el responsable del tratamiento sobre si sus datos están siendo tratados y, en su caso, cuáles son los datos objeto de dicho tratamiento.

125 TEDH, *Haralambie contra Rumanía*, nº 21737/03, de 27 de octubre de 2009.

3.4.2. Establecer confianza

Los responsables del tratamiento deberían documentar, tanto a los interesados como al público en general, que tratarán datos de forma lícita y transparente. Las operaciones de tratamiento no deben realizarse de forma secreta y no deben tener efectos negativos imprevisibles. Los responsables del tratamiento deberían garantizar que se informa a los consumidores, a los clientes o a los ciudadanos sobre el uso de sus datos. Además, los responsables del tratamiento, en la medida de lo posible, deberán actuar de un modo tal que satisfaga sin demora los deseos del interesado, en especial cuando su consentimiento constituya el fundamento jurídico del tratamiento de datos.

Ejemplo: En el asunto *K.H. y otros contra Eslovaquia*,[126] los 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 tribunales nacionales ordenaron a los hospitales que permitieran que las demandantes y sus representantes consultaran y redactaran resúmenes manuscritos de sus historias clínicas, pero denegaron sus peticiones de fotocopiar los documentos, presumiblemente para evitar un posible abuso. Las obligaciones positivas de los Estados con arreglo al artículo 8 del CEDH incluyen necesariamente una obligación de poner a disposición de los interesados copias de sus ficheros de datos. Era el Estado quien debía determinar las medidas para realizar las copias de los ficheros de datos personales o, en su caso, demostrar motivos fundados para su denegación. En el caso de las demandantes, los tribunales nacionales justificaron la prohibición de hacer copias de las historias clínicas, en especial, en 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 dicho abuso a través de medios distintos a la denegación de las copias de los expedientes, como limitar el grupo de personas autorizadas para acceder a los mismos. 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.

126 TEDH, *K.H. y otros contra Eslovaquia*, nº 32881/04, de 6 de noviembre 2009.

Respecto de los servicios de Internet, las características de los sistemas de tratamiento de datos deben posibilitar que los interesados puedan realmente entender lo que está ocurriendo con sus datos.

El tratamiento leal también implica que los responsables del tratamiento estén preparados para sobrepasar los requisitos mínimos legales obligatorios de servicio al interesado, si así lo exigen intereses legítimos del interesado.

3.5. El principio de rendición de cuentas

Puntos clave

- La rendición de cuentas exige la aplicación activa por parte de los responsables del tratamiento de medidas que promuevan y garanticen la protección de datos en sus actividades de tratamiento.
- Los responsables del tratamiento son responsables de que sus operaciones de tratamiento cumplan con la legislación en materia de protección de datos.
- Los responsables del tratamiento deben poder demostrar a los interesados, al público en general y a las autoridades de supervisión, en cualquier momento, que cumplen con las disposiciones en materia de protección de datos.

La Organización de Cooperación y Desarrollo Económicos (OCDE) adoptó directrices de privacidad en 2013, las cuales destacaban que los responsables del tratamiento tienen una función importante a la hora de aplicar la protección de datos en la práctica. Las directrices desarrollan el principio de rendición de cuentas en el sentido de que «a todo responsable del tratamiento se le deberían pedir responsabilidades por el cumplimiento de las medidas que permiten la aplicación de los principios [materiales] antes expuestos».[127]

Si bien el Convenio nº 108 no hace referencia a la rendición de cuentas de los responsables del tratamiento, dejando principalmente que sea la legislación nacional quien trate esta cuestión, el artículo 6, apartado 2, de la Directiva de protección de datos establece que el responsable del tratamiento deberá garantizar el cumplimiento de los principios relacionados con la calidad de los datos incluidos en el apartado 1.

127 OCDE (2013), *Directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales*, artículo 14.

Ejemplo: Un ejemplo legislativo que destaca el principio de rendición de cuentas es la modificación de 2009[128] de la Directiva 2002/58/CE sobre la privacidad en las comunicaciones electrónicas. De conformidad con el artículo 4 en su forma modificada, la Directiva impone una obligación de aplicar una política de seguridad, en concreto, «garantizarán 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 la Directiva, el legislador decidió que era necesario introducir un requisito expreso de contar con una política de seguridad y de aplicarla.

Según el dictamen del Grupo del artículo 29,[129] la esencia de la rendición de cuentas es la obligación del responsable del tratamiento de:

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

- tener disponible documentación que demuestre a los interesados y a las autoridades de supervisión qué medidas han sido adoptadas para lograr la observancia de las normas en materia de protección de datos.

El principio de rendición de cuentas exige, por tanto, que los responsables del tratamiento demuestren de forma activa que existe dicho cumplimiento y no sólo que esperen a que los interesados o las autoridades de supervisión señalen las posibles carencias.

128 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) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores, DO 2009 L 337, p. 11.

129 Grupo del artículo 29, *Dictamen 3/2010 sobre el principio de responsabilidad*, WP 173, Bruselas, de 13 de julio de 2010.

4

Las normas de la legislación europea en materia de protección de datos

UE	Materias cubiertas	CdE
Normas sobre el tratamiento lícito de datos no sensibles		
Directiva de protección de datos, artículo 7, letra a)	Consentimiento	Recomendación de perfilado, artículo 3.4, letra b), y artículo 3.6
Directiva de protección de datos, artículo 7, letra b)	Relación (pre-) contractual	Recomendación de perfilado, artículo 3.4, letra b)
Directiva de protección de datos, artículo 7, letra c)	Deberes legales del responsable del tratamiento	Recomendación de perfilado, artículo 3.4, letra a)
Directiva de protección de datos, artículo 7, letra d)	Intereses vitales del interesado	Recomendación de perfilado, artículo 3.4, letra b)
Directiva de protección de datos, artículo 7, letra e), y artículo 8, apartado 4 TJUE, asunto C-524/06, *Huber contra Bundesrepublik Deutschland*, de 16 de diciembre de 2008	Interés público y ejercicio del poder público	Recomendación de perfilado, artículo 3.4, letra b)
Directiva de protección de datos, artículo 7 letra f), artículo 8, apartados 2 y 3 TJUE, asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) contra Administración del Estado*, de 24 de noviembre de 2011	Intereses legítimos de terceros	Recomendación de perfilado, artículo 3.4, letra b)

Normas sobre el tratamiento lícito de datos sensibles		
Directiva de protección de datos, artículo 8, apartado 1	Prohibición general de tratamiento	Convenio nº 108, artículo 6
Directiva de protección de datos, artículo 8, apartados 2 a 4	Excepciones a la prohibición general	Convenio nº 108, artículo 6
Directiva de protección de datos, artículo 8, apartado 5	Tratamiento de datos sobre condenas (penales)	Convenio nº 108, artículo 6
Directiva de protección de datos, artículo 8, apartado 7	Tratamiento de los números de identificación	
Normas relativas al tratamiento seguro		
Directiva de protección de datos, artículo 17	Obligación de proporcionar un tratamiento seguro	Convenio nº 108, artículo 7 TEDH, *I. contra Finlandia*, nº 20511/03, de 17 de julio de 2008
Directiva sobre la privacidad en las comunicaciones electrónicas, artículo 4, apartado 2	Notificaciones de violación de datos personales	
Directiva de protección de datos, artículo 16	Obligación de confidencialidad	
Normas relativas a la transparencia del tratamiento		
	Transparencia en general	Convenio nº 108, artículo 8, letra a)
Directiva de protección de datos, artículos 10 y 11	Información	Convenio nº 108, artículo 8, letra a)
Directiva de protección de datos, artículos 10 y 11	Excepciones a la obligación de informar	Convenio nº 108, artículo 9
Directiva de protección de datos, artículos 18 y 19	Notificación	Recomendación de perfilado, artículo 9.2, letra a)
Normas relativas a la promoción del cumplimiento		
Directiva de protección de datos, artículo 20	Controles previos	
Directiva de protección de datos, artículo 18, apartado 2	Delegados de protección de datos personales	Recomendación de perfilado, artículo 8.3
Directiva de protección de datos, artículo 27	Códigos de conducta	

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**, quedará al arbitrio de las Partes del Convenio

nº 108 aclarar este margen de interpretación en sus legislaciones nacionales. La situación en el **Derecho de la Unión Europea** es distinta: para el establecimiento de la protección de los datos en el mercado interior, se consideró necesario contar con normas más detalladas a escala europea para armonizar el nivel de protección de los datos de las legislaciones nacionales de los Estados miembros. La Directiva de protección de datos establece, de conformidad con los principios establecidos en su artículo 6, un conjunto de normas detalladas que deben ser fielmente incorporadas a las legislaciones nacionales. Las siguientes observaciones sobre las normas detalladas en materia de protección de datos a escala europea versan principalmente, por lo tanto, sobre el Derecho de la UE.

4.1. Normas relativas al tratamiento lícito

Puntos clave

- Los datos personales podrán tratarse de forma lícita si:
  - el tratamiento se funda en el consentimiento del interesado;
  - los intereses vitales de los interesados exigen el tratamiento de sus datos; o
  - el motivo del tratamiento son los intereses legítimos de terceros, aunque solo mientras no prevalezcan los intereses de protección de los derechos fundamentales de los interesados.
- El tratamiento lícito de datos personales sensibles está sometido a un régimen especial más estricto.

La Directiva de protección de datos incluye dos conjuntos de normas distintos para el tratamiento lícito de los datos: uno para los datos no sensibles, en el artículo 7, y otro para los datos sensibles, en el artículo 8.

4.1.1. Tratamiento lícito de los datos no sensibles

El capítulo II de la Directiva 95/46, cuyo título es «Condiciones generales para la licitud del tratamiento de datos personales», establece que, con sujeción a las excepciones que se permiten en el artículo 13, todos los tratamientos de datos personales deben cumplir, en primer lugar, los principios relativos a la calidad de los datos, establecidos en el artículo 6 de la Directiva de protección de datos y, en segundo lugar, uno de los criterios relativos a la legitimación del tratamiento de datos, incluidos en

el artículo 7.[130] Esto explica los casos que legitiman el tratamiento de los datos personales no sensibles.

Consentimiento

En el Derecho del CdE no se menciona el consentimiento ni en el artículo 8 del CEDH ni en el Convenio nº 108. Sin embargo, la jurisprudencia del TEDH y diversas recomendaciones del Consejo de Europa sí aluden a dicho consentimiento. **De acuerdo con el Derecho de la UE**, el artículo 7, letra a), de la Directiva de protección de datos consagra el consentimiento como base para que el tratamiento de datos sea legítimo. Asimismo, también se menciona expresamente en el artículo 8 de la Carta.

Relación contractual

Otro fundamento del tratamiento legítimo de los datos personales **con arreglo al Derecho de la UE**, mencionado en el artículo 7, letra b), de la Directiva de protección de datos, es si es «necesario para la ejecución de un contrato en el que el interesado sea parte». Esta disposición también abarca a las relaciones precontractuales. Por ejemplo: una parte pretende celebrar un contrato pero todavía no lo ha hecho, posiblemente porque todavía faltan por hacer algunas comprobaciones. Si una parte requiere tratar datos a tales efectos, dicho tratamiento estará legitimado en la medida en que sea «para la aplicación de medidas precontractuales adoptadas a petición del interesado».

En cuanto al Derecho del CdE, «la protección de los derechos y las libertades de los demás» se menciona en el artículo 8, apartado 2, del CEDH, como motivo de injerencia legítima en el derecho a la protección de datos.

Deberes legales del responsable del tratamiento

El Derecho de la UE menciona expresamente otro criterio relativo a la legitimación del tratamiento de datos, en concreto, si éste «es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento» (artículo 7, letra c), de la Directiva de protección de datos). Esta disposición hace

130 TJUE, asuntos acumulados C-465/00, C-138/01 y C-139/01 *Österreichischer Rundfunk y otros*, de 20 de mayo de 2003, apdo. 65; TJUE, asunto C-524/06, *Heinz Huber contra Bundesrepublik Deutschland*, de 16 de diciembre de 2008, apdo. 48; TJUE, asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) contra Administración del Estado*, de 24 de noviembre de 2011, apdo. 26.

referencia a los responsables del tratamiento que actúan en el sector privado. Las obligaciones jurídicas de los responsables del tratamiento de datos del sector público quedan comprendidas en el artículo 7, letra e), de la Directiva. Existen muchos casos en que los responsables del tratamiento del sector privado están obligados por ley a tratar datos de otras personas; por ejemplo, los médicos y los hospitales tienen el deber jurídico de almacenar datos sobre el tratamiento de los pacientes durante varios años, los empresarios deben tratar datos sobre los empleados a los efectos de la seguridad social y tributación, así como las empresas deben tratar datos sobre sus clientes por motivos fiscales.

En el contexto de la transferencia obligatoria de los datos de los pasajeros por parte de las compañías aéreas a las autoridades extranjeras de control de inmigración, se plantea la cuestión de si las obligaciones jurídicas con arreglo a la legislación *extranjera* podría constituir o no un fundamento legítimo para el tratamiento de datos con arreglo al Derecho de la UE (esta cuestión se debatirá con más detalle en el apartado 6.2).

Las obligaciones jurídicas del responsable del tratamiento servirán de base para el tratamiento legítimo de los datos **con arreglo al Derecho del CdE.** Tal como se ha señalado anteriormente, las obligaciones jurídicas del responsable del tratamiento del sector privado constituyen únicamente un caso específico de los intereses legítimos de los demás, tal como menciona el artículo 8, apartado 2, del CEDH. El ejemplo anterior resulta, por tanto, relevante para el Derecho del CdE.

Interés vital del interesado

Según el Derecho de la UE, el artículo 7, letra d), de la Directiva de protección de datos establece que el tratamiento de datos personales es legítimo si «es necesario para proteger el interés vital del interesado». Dicho interes, que está estrechamente relacionado con la supervivencia del interesado, podría constituir el fundamento, por ejemplo, del uso legítimo de datos de salud o de datos sobre personas desaparecidas.

Según el Derecho del CdE, el interés vital del interesado no se menciona en el artículo 8 del CEDH como un motivo de injerencia legítima en el derecho a la protección de datos. En algunas de las recomendaciones del Consejo de Europa que complementan al Convenio nº 108 en ámbitos específicos, sin embargo, se menciona de forma expresa el interés vital del interesado como fundamento del tratamiento de

datos legítimo.[131] El interés vital del interesado debe, evidentemente, considerarse implícito en el conjunto de motivos que justifican el tratamiento de datos: la protección de los derechos fundamentales nunca debe poner en peligro el interés vital de la persona que se protege.

Interés público y ejercicio del poder público

Teniendo en cuenta las múltiples formas posibles que existen de organizar los asuntos públicos, el artículo 7, letra e), de la Directiva de protección de datos establece que los datos personales podrán ser tratados de forma lícita si «es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos [...]».[132]

Ejemplo: En el asunto *Huber contra Bundesrepublik Deutschland*,[133] 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, en el que se incluyen datos personales de nacionales de la UE no alemanes, residentes en Alemania durante un periodo de más de tres meses, es utilizado con fines estadísticos, así como por las autoridades policiales y judiciales al enjuiciar e investigar actividades delictivas o que pongan en peligro la seguridad pública. El órgano jurisdiccional que planteó la cuestión prejudicial solicitó un pronunciamiento sobre la compatibilidad con el Derecho comunitario del tratamiento de datos personales que lleva a cabo un registro central de extranjeros, a los cuales tienen acceso otras autoridades públicas, dado que no existe tal registro para los nacionales alemanes.

El TJUE sostuvo, en primer lugar, que de conformidad con el artículo 7, letra e), de la Directiva, el tratamiento de datos personales puede ser lícito únicamente si es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos.

Según el Tribunal, «habida cuenta del objetivo consistente en equiparar el nivel de protección en todos los Estados miembros, el concepto de necesidad, tal

131 Recomendación de creación de perfiles, artículo 3.4, letra b).

132 Véase asimismo la Directiva de protección de datos, considerando 32.

133 TJUE, asunto C-524/06, *Huber contra Bundesrepublik Deutschland*, de 16 de diciembre de 2008.

como resulta del artículo 7, letra e), de la Directiva 95/46 [...] no puede tener un contenido variable en función de los Estados miembros. Por lo tanto, 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».[134]

El Tribunal señala 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. Y si, en principio, es legítimo que un Estado miembro utilice un registro como el AZR como apoyo a las autoridades encargadas de aplicar la normativa en materia de derecho de residencia, dicho registro no podrá contener más información que la que resulte necesaria para tal fin. El Tribunal concluye 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 deberá verificar si estas condiciones se satisfacen en este litigio particular. Si no es así, no cabe considerar en ningún caso que la conservación y tratamiento de datos personales en el marco de un Registro como el AZR con fines estadísticos[135] sean necesarios, en el sentido del artículo 7, letra e), de la Directiva 95/46/CE.

Por último, en lo que atañe a la cuestión del uso de los datos incluidos en el registro para luchar contra la delincuencia, el Tribunal sostuvo 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 en cuestión no contiene datos personales relacionados con nacionales del Estado miembro de que se trate y esta diferencia de tratamiento constituye una discriminación prohibida por el artículo 18 del TFUE. Por consiguiente, esta disposición, tal como fue interpretada por el Tribunal, «se opone a que un Estado miembro establezca, 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».[136]

134 *Ibid.*, apdo. 52.

135 *Ibid.*, apdos. 54, 58, 59, 66 a 68.

136 *Ibid.*, apdos. 78 y 81.

El uso de los datos personales por parte de las autoridades que actúen en el ámbito público está sujeto también al artículo 8 del CEDH.

Interés legítimo perseguido por el responsable del tratamiento o por un tercero

El interesado no es la única persona con un interés legítimo. El artículo 7, letra f), de la Directiva de protección de datos establece que los datos personales pueden ser tratados de forma legítima si «es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comunique los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección [...]».

En la siguiente sentencia, el TJUE se pronunció de forma expresa sobre el artículo 7, letra f), de la Directiva:

Ejemplo: En el asunto *ASNEF y FECEMD*,[137] el TJUE aclaró que a la legislación nacional no se le permite añadir otras condiciones a aquellas mencionadas en el artículo 7, letra f), de la Directiva del tratamiento lícito de los datos. Dicho asunto hacía referencia a la situación de la legislación española de protección de datos, que contenía una disposición por la cual otras partes privadas podrían reivindicar un interés legítimo en el tratamiento de datos personales únicamente si estos ya figuraban en fuentes accesibles al público.

El Tribunal señaló en primer lugar que la Directiva 95/46 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 nacionales aplicables en este ámbito tampoco debe suponer una disminución de la protección que garantizan, sino que, en su lugar, debe asegurar un alto nivel de protección dentro de la UE.[138] Así pues, el Tribunal sostuvo que «se deduce el objetivo consistente en asegurar un nivel de protección equivalente en todos los Estados miembros que el artículo 7 de la Directiva 95/46 establece una lista exhaustiva y taxativa de los casos en que un tratamiento de datos personales

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

138 *Ibid.*, apdo. 28. Véase la Directiva de protección de datos, considerandos 8 y 10.

puede considerarse lícito». Además, «los Estados miembros no pueden ni añadir al artículo 7 de la Directiva 95/46 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».[139] El Tribunal 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».

Habida cuenta de estas consideraciones, el Tribunal concluyó que «el artículo 7, letra f), de la Directiva 95/46 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 este, 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».[140]

En las recomendaciones del CdE pueden encontrarse formulaciones similares. La Recomendación de perfilado reconoce como legítimo el tratamiento de datos personales a efectos de perfilado si es necesaria para los intereses legítimos de terceros «salvo cuando los derechos y libertades fundamentales de la persona interesada prevalezcan sobre dichos intereses».[141]

139 TJUE, asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) contra Administración del Estado*, de 24 de noviembre de 2011, apdos. 30 y 32.

140 *Ibid.*, apdos. 40, 44, 48 y 49.

141 Recomendación de creación de perfiles, artículo 3.4, letra b).

4.1.2. Tratamiento lícito de los datos sensibles

El Derecho del CdE remite al Derecho nacional para el establecimiento de la protección adecuada para el uso de los datos sensibles, mientras que **el Derecho de la UE,** en el artículo 8 de la Directiva de protección de datos, contiene un régimen pormenorizado del tratamiento de categorías de datos que revelen: el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como datos relativos a la salud o a la sexualidad. En principio, queda prohibido el tratamiento de datos sensibles.[142] Existe, sin embargo, una lista exhaustiva de excepciones a dicha prohibición, contempladas en el artículo 8, apartados 2 y 3, de la Directiva. Entre estas excepciones se incluyen el consentimiento explícito del interesado, el interés vital del interesado, el interés legítimo de terceros y el interés público.

Contrariamente a lo que ocurre en el caso del tratamiento de datos no sensibles, no se considera que una relación contractual con el interesado constituya una base general para el tratamiento legítimo de datos sensibles. Por tanto, si deben tratarse datos sensibles en el contexto de un contrato con el interesado, el uso de dichos datos exigirá la existencia de un consentimiento explícito autónomo del interesado, además del acuerdo de celebrar un contrato. Una petición expresa por parte del interesado de productos o servicios que revelarían necesariamente datos sensibles debería considerarse, sin embargo, equivalente a un consentimiento explícito.

Ejemplo: Si un pasajero de una compañía aérea, en el contexto de la reserva de un vuelo, solicita a dicha compañía que le proporcione una silla de ruedas y comida kosher, se permitirá a dicha compañía utilizar estos datos incluso si el pasajero no ha firmado una cláusula de consentimiento adicional en la que indique que está de acuerdo con el uso de los datos que le conciernen que revelan información sobre su salud y sus creencias religiosas.

Consentimiento explícito del interesado

La primera condición para que un tratamiento de datos sea legítimo, con independencia de si son o no datos sensibles, es el consentimiento del interesado. En el caso de los datos sensibles, dicho consentimiento debe ser explícito. El derecho nacional podrá establecer, sin embargo, que el consentimiento para el uso de datos sensibles

142 Directiva de protección de datos, artículo 8, apartado 1.

no es un fundamento jurídico suficiente para permitir el tratamiento de los mismos,[143] por ejemplo cuando, en casos excepcionales, el tratamiento conlleve riesgos poco habituales para el interesado.

En un caso especial, incluso el consentimiento implícito se reconoce como fundamento jurídico para el tratamiento de datos sensibles: el artículo 8, apartado 2, letra e), de la Directiva establece que el tratamiento no queda prohibido si se refiere a datos que el interesado haya hecho manifiestamente públicos. Esta disposición presume obviamente que la acción del interesado, al hacer públicos sus datos, debe interpretarse que implica el consentimiento por parte del interesado al uso de dichos datos.

Interés vital del interesado

Como ocurre en el caso de los datos no sensibles, los datos sensibles podrán ser tratados para salvaguardar del interés vital del interesado.[144]

Para que el tratamiento de datos sensibles sea legítimo sobre esta base, es necesario que resulte imposible preguntar al interesado su decisión al respecto, por ejemplo, porque el interesado no fuera consciente o estuviera ausente y no pudiera ser localizado.

Intereses legítimos de terceros

Tal como ocurre en el caso de los datos no sensibles, los intereses legítimos de otros podrán servir como base del tratamiento de datos sensibles. En el caso de los datos sensibles, de conformidad con lo dispuesto en el artículo 8, apartado 2, de la Directiva de protección de datos, sin embargo, esto es aplicable únicamente a los siguientes casos:

- cuando el tratamiento sea necesario para salvaguardar el interés vital de otra persona[145] en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

143 *Ibid.,* artículo 8, apartado 2, letra a).

144 *Ibid.,* artículo 8, apartado 2, letra c).

145 *Ibid.*

- cuando los datos sensibles sean relevantes en materia de Derecho laboral, como los datos relativos a la salud, por ejemplo en el contexto de un lugar de trabajo especialmente peligroso, o datos sobre sus creencias religiosas, por ejemplo en el contexto de vacaciones;[146]

- cuando las fundaciones, asociaciones o cualquier otro organismo sin fin de lucro cuya finalidad sea política, filosófica, religiosa o sindical, trate datos sobre sus miembros o patrocinadores u otras partes interesadas (dichos datos son sensibles porque pueden revelar las creencias religiosas o políticas de las personas físicas a que hagan referencia);[147]

- cuando los datos sensibles se utilizan en el contexto de un procedimiento judicial ante una autoridad jurisdiccional o administrativa para el reconocimiento, ejercicio o defensa de un derecho.[148]

- Además, de conformidad con el artículo 8, apartado 3, de la Directiva de protección de datos, cuando los datos de salud se utilicen para exámenes y tratamientos médicos realizados por profesionales sanitarios, la gestión de estos servicios está incluida en esta excepción. Como garantía especial, las personas serán reconocidas como «prestadores de asistencia sanitaria» únicamente si están sujetos a obligaciones profesionales específicas de confidencialidad.

Interés público

De forma adicional, de conformidad con el artículo 8, apartado 4, de la Directiva de protección de datos, los Estados miembros podrán introducir más fines para los que pueden tratarse los datos sensibles, siempre que:

- el tratamiento de los datos sea por motivos de interés público importante;

- esté establecido por la legislación nacional o por decisión de la autoridad de supervisión; y

146 *Ibid.,* artículo 8, apartado 2, letra b).

147 *Ibid.,* artículo 8, apartado 2, letra d).

148 *Ibid.,* artículo 8, apartado 2, letra e).

- la legislación nacional o la decisión de la autoridad de supervisión incluya las garantías necesarias para salvaguardar de forma eficaz los intereses de los interesados.[149]

Un ejemplo destacado son los sistemas de expedientes de salud electrónicos, que muchos Estados miembros están a punto de establecer. Dichos sistemas permitirán que los datos de salud, obtenidos por los prestadores de servicios sanitarios mientras tratan a los pacientes, estén disponibles para otros prestadores de servicios sanitarios que atiendan a estos pacientes en ámbitos más amplios, normalmente a escala nacional.

El Grupo del artículo 29 concluyó que el establecimiento de dichos sistemas no puede tener lugar con arreglo a las normas legales existentes relativas al tratamiento de datos de los pacientes sobre la base del artículo 8, apartado 3, de la Directiva de protección de datos. Asumir que la existencia de dichos sistemas de expedientes de salud electrónicos constituye un motivo de interés público, podría basarse, sin embargo, en el artículo 8, apartado 4, de la Directiva, el cual exige una base jurídica explícita para su establecimiento que incluya también las garantías necesarias que garanticen que el sistema funcione de forma segura.[150]

4.2. Normas relativas a la seguridad del tratamiento

Puntos clave

- Las normas relativas a la seguridad del tratamiento implican una obligación por parte del responsable del tratamiento y del encargado del tratamiento de aplicar las medidas técnicas y organizativas oportunas para evitar cualquier injerencia no autorizada en las operaciones de tratamiento de datos.
- El nivel necesario de la seguridad de datos queda determinado por:
  - las opciones de seguridad disponibles en el mercado para cualquier tipo particular de tratamiento;
  - los costes, y

149 *Ibid.,* artículo 8, apartado 4.

150 Grupo 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, de 15 de febrero de 2007.

- la sensibilidad de los datos tratados.

- El tratamiento de datos seguro quedará, además, garantizado por el deber general de todas las personas, responsables o encargados del tratamiento, de garantizar que los datos siguen siendo confidenciales.

La obligación de los responsables del tratamiento y de los encargados del tratamiento de adoptar medidas apropiadas para garantizar la seguridad de los datos queda establecida, por tanto, en la **legislación en materia de protección de datos del CdE** así como en la **legislación europea en materia de protección de datos**.

4.2.1. Elementos de la seguridad de datos

De conformidad con las disposiciones relevantes en el **Derecho de la UE**:

> *«Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales».*[151]

En el **Derecho del CdE** existe una disposición similar:

> *«Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados de datos contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.»*[152]

Con frecuencia, también existen normas industriales, nacionales e internacionales que han sido desarrolladas para un tratamiento de datos seguro. El sello europeo de privacidad (EuroPriSe), por ejemplo, es un proyecto eTEN (Redes transeuropeas de telecomunicación) de la UE que ha explorado las posibilidades de la certificación de productos, en especial de programas informáticos, como conformes con 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

151 Directiva de protección de datos, artículo 17, apartado 1.

152 Convenio nº 108, artículo 7.

Unión Europea, de los Estados miembros y de la comunidad empresarial para prevenir, tratar y dar respuesta a los problemas de seguridad de las redes y de la información.[153] ENISA publica de manera periódica análisis de las actuales amenazas a la seguridad, así como asesoramiento sobre cómo tratarlas.

La seguridad de los datos no se logra únicamente disponiendo del equipo adecuado (hardware y programas informáticos), sino que también exige la existencia de normas de organización internas adecuadas. Lo ideal sería que dichas normas internas comprendieran las siguientes cuestiones:

- suministro de información periódico 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;

- clara distribución de las responsabilidades y un esquema claro de las competencias en cuestiones de tratamiento de datos, en especial en lo que respecta a las decisiones de tratar datos personales y transmitir datos a terceros;

- uso de los datos personales únicamente con arreglo a las instrucciones de la persona competente o de conformidad con las normas generales establecidas;

- protección del acceso a las ubicaciones y al hardware y programas informáticos del responsable del tratamiento o del encargado del tratamiento, incluidos los controles sobre las autorizaciones de acceso;

- garantizar que las autorizaciones para acceder a los datos personales han sido atribuidas por la persona competente y exigen documentación adecuada;

- protocolos automatizados sobre el acceso a los datos personales por vía electrónica y controles periódicos de dichos protocolos por parte de una oficina de supervisión interna;

- documentación cuidadosa sobre otras formas de comunicación distintas al acceso automatizado de los datos para poder demostrar que no se han producido transmisiones de datos ilegales.

153 Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, DO 2004 L 77.

Ofrecer a los miembros del personal formación y educación adecuadas sobre la seguridad de los datos también es un elemento importante de las medidas 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 de los empleados, las auditorías periódicas, los ensayos de penetración y los sellos de calidad.

Ejemplo: En el asunto *I. contra Finlandia*,[154] la demandante no pudo demostrar que otros empleados del hospital donde trabajaba habían accedido de forma ilegítima a su historia clínica, por lo que los tribunales nacionales rechazaron su denuncia de violación de su derecho a la protección de datos. 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». Para el Tribunal resultó decisivo que el sistema de expedientes disponible en el hospital estuviera claramente en discordancia con los requisitos legales incluidos en la legislación nacional, un hecho que no fue ponderado de forma adecuada por los tribunales nacionales.

Notificación de violación de datos personales

En la legislación en materia de protección de datos de varios países europeos se ha introducido un nuevo instrumento que aborda las violaciones de la seguridad de los datos: la obligación de los prestadores de servicios de comunicaciones electrónicas de notificar las violaciones de datos personales tanto a las posibles víctimas como a las autoridades de supervisión. En el caso de los prestadores de telecomunicaciones,

154 TEDH, *I. contra Finlandia*, nº 20511/03, de 17 de julio de 2008.

esto resulta obligatorio en virtud del Derecho de la UE.[155] La finalidad de la notificación de violación de datos personales a los interesados es evitar daños, la notificación de violaciones de datos personales y sus posibles consecuencias reduce el riesgo de efectos negativos para los interesados. En los casos de negligencia grave, los prestadores podrán ser multados.

Será necesario establecer de antemano procedimientos internos para la gestión y la notificación efectiva de violaciones de seguridad, dado que el plazo para la obligación de informar a los interesados y/o a la autoridad de supervisión, con arreglo a la legislación nacional, es normalmente bastante corto.

4.2.2. Confidencialidad

De conformidad con el Derecho de la UE, el tratamiento de datos seguro quedará además garantizado por la obligación general de todas las personas, responsables del tratamiento o encargados del tratamiento, de garantizar que los datos siguen siendo confidenciales.

> 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, el cual 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. Esto puede llevarse a cabo, por ejemplo, ofreciendo devolver la llamada al número de teléfono que figura en la ficha del cliente.

El artículo 16 de la Directiva de protección de datos afecta únicamente a la confidencialidad en la relación entre el responsable del tratamiento y el encargado del tratamiento. La cuestión de si los responsables del tratamiento deben mantener o no la

155 Véase la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, (*Directiva sobre la privacidad y las comunicaciones electrónicas*), DO 2002 L 201, artículo 4, apartado 3, 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; véase, asimismo, 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) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores, DO 2009 L 337.

confidencialidad de los datos, en el sentido de que no pueden revelarlos a terceros, se aborda en los artículos 7 y 8 de la Directiva.

El deber de confidencialidad no se amplía a las situaciones en que los datos proceden del conocimiento de una persona en su calidad de particular y no como empleado de un responsable del tratamiento o de un encargado del tratamiento. En este caso, el artículo 16 de la Directiva de protección de datos no es aplicable, ya que, de hecho, el uso de datos personales por parte de los particulares queda totalmente exceptuado de la remisión que realiza la Directiva cuando dicho uso entra dentro de los límites de la denominada excepción doméstica.[156] La excepción doméstica es el uso de datos personales «efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas».[157] Teniendo en cuenta la resolución del TJUE en el asunto *Bodil Lindqvist*,[158] esta excepción deberá, sin embargo, interpretarse de forma limitada, en especial respecto de la difusión de los datos. En particular, la excepción doméstica no alcanzará a la publicación de los datos personales a un número ilimitado de destinatarios en Internet (para más detalles sobre el asunto, véanse los apartados 2.1.2, 2.2, 2.3.1 y 6.1).

De acuerdo con el Derecho del CdE, la obligación de confidencialidad está implícita en el concepto de seguridad de los datos en el artículo 7 del Convenio nº 108, que trata sobre la seguridad de los datos.

En el caso de los encargados del tratamiento, la confidencialidad implica que podrán utilizar los datos personales que le hayan sido atribuidos por el responsable del tratamiento únicamente de conformidad con las instrucciones que dicho responsable haya facilitado. En el caso de los empleados de un responsable del tratamiento o de un 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 del tratamiento y sus encargados del tratamiento. Además, los responsables del tratamiento y los encargados del tratamiento adoptarán medidas específicas para establecer un deber legal de confidencialidad para sus empleados, normalmente mediante la inclusión de cláusulas de confidencialidad en el contrato de trabajo del empleado.

156 Directiva de protección de datos, artículo 3, apartado 2, guión segundo.

157 *Ibid*.

158 TJUE, asunto C-101/01, *Bodil Lindqvist*, de 6 de noviembre de 2003.

La infracción de los deberes profesionales de confidencialidad está sancionada de conformidad con el Derecho penal en muchos Estados miembros de la UE y Partes del Convenio nº 108.

4.3. Normas relativas a la transparencia del tratamiento

Puntos clave

- Antes de comenzar a tratar datos personales, el responsable del tratamiento deberá, como mínimo, informar, a los interesados sobre su identidad y sobre la finalidad del tratamiento de datos, salvo en el caso en que el interesado ya disponga de esta información.
- En los casos en que los datos sean obtenidos de terceros, la obligación de facilitar información no será aplicable si:
  - el tratamiento de datos está previsto por la ley; o
  - se ha demostrado que la comunicación de la información es imposible o exigiría esfuerzos desproporcionados.
- Antes de comenzar a tratar datos personales, el responsable del tratamiento deberá, además:
  - notificar a la autoridad de supervisión las operaciones de tratamiento previstas; o
  - documentar internamente el tratamiento por parte de un delegado de protección de datos personales independiente, si la legislación nacional establece dicho procedimiento.

El principio de tratamiento leal requiere que el tratamiento sea transparente. **El Derecho del CdE** establece, para este fin, que cualquier persona puede confirmar la existencia de ficheros de tratamiento de datos, su finalidad y el responsable del tratamiento de los mismos.[159] Será el Derecho nacional quien determine el modo en que esto debe llevarse a cabo. **El Derecho de la UE** es más específico, asegurando la transparencia respecto del interesado mediante la existencia de la obligación por parte del responsable del tratamiento de informar al interesado, y respecto del público en general mediante notificación.

159 Convenio nº 108, artículo 8, letra a).

En ambos sistemas jurídicos, podrán existir excepciones y limitaciones a las obligaciones de transparencia del responsable del tratamiento en la legislación nacional cuando dicha limitación constituye una medida necesaria para salvaguardar determinados intereses públicos o la protección del interesado o de los derechos y libertades de otras personas, siempre que sean necesarias en una sociedad democrática.[160] Dichas excepciones podrán ser necesarias, por ejemplo, en el contexto de la investigación de un delito, aunque también podrán estar justificadas en otras circunstancias.

4.3.1. Información

De conformidad tanto con el Derecho del CdE como con el Derecho de la UE, el responsable del tratamiento de datos está obligado a informar al interesado con antelación sobre el tratamiento previsto.[161] Esta obligación no depende de que exista o no 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 se muestra o no interesado en la información.

Contenido de la información

La información deberá incluir la finalidad del tratamiento, así como la identidad y los datos de contacto del responsable del tratamiento.[162] La Directiva de protección de datos exige que se facilite otra información adicional cuando « habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado». Los artículos 10 y 11 de la Directiva destacan, entre otras cosas, las categorías de datos tratados y los destinatarios de dichos datos, así como la existencia del derecho de acceso y el derecho de rectificación de los datos. En los casos en que los datos se recaban del propio interesado, la información deberá aclarar el carácter obligatorio o voluntario de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder.[163]

160 *Ibid.*, artículo 9, apartado 2, y Directiva de protección de datos, artículo 13, apartado 1.

161 Convenio nº 108, artículo 8, letra a); y Directiva de protección de datos, artículos 10 y 11.

162 Convenio nº 108, artículo 8, letra a); y Directiva de protección de datos, artículos 10, letras a) y b).

163 Directiva de protección de datos, artículo 10, letra c).

Desde el punto de vista del **Derecho del CdE**, la información al interesado podrá ser considerada una buena práctica con arreglo al principio de tratamiento leal de los datos y, en este sentido, también forma parte de dicho Derecho.

El principio de tratamiento leal exige que la información sea fácilmente comprensible por parte de los interesados. El lenguaje que debe utilizarse será el que resulte adecuado para los destinatarios. Será necesario que tanto el nivel como el tipo de lenguaje sean distintos en función de si el público destinatario es, por ejemplo, adulto o infantil, el público en general o expertos académicos.

Algunos interesados desearán ser informados únicamente de forma resumida sobre el modo y el motivo por el que los datos serán tratados, mientras que otros exigirán una explicación detallada. El modo en que debe ponderarse este aspecto de la información leal fue considerado en un dictamen del Grupo del artículo 29, en el cual se promueve la idea de los denominados avisos por capas,[164] que permiten al interesado decidir qué nivel de detalle prefiere.

Momento de suministro de la información

La Directiva de protección de datos incluye disposiciones ligeramente distintas relacionadas con el momento en que debe suministrarse la información, dependiendo de si los datos son recabados del propio interesado (artículo 10) o de un tercero (artículo 11). En los casos en que los datos son recabados del propio interesado, la información deberá suministrarse, a más tardar, cuando tiene lugar la recogida. Cuando los datos son recabados de terceros, la información deberá suministrarse, a más tardar, cuando el responsable del tratamiento registra los datos o antes de que los datos se comuniquen por primera vez a un tercero.

Excepciones a la obligación de informar

De conformidad con el Derecho de la UE, existe una excepción general a la obligación de informar al interesado para los casos en que este ya haya sido informado.[165] Esta excepción hace referencia a las situaciones en que el interesado, según las circunstancias del caso, ya conozca que un determinado responsable del tratamiento tratará sus datos para una determinada finalidad.

164 Grupo del artículo 29 (2004), *Dictamen 10/2004 sobre una mayor armonización de las disposiciones relativas a la información*, WP 100, Bruselas, de 25 de noviembre de 2004.

165 Directiva de protección de datos, artículo 10 y artículo 11, apartado 1.

El artículo 11 de la Directiva, que hace referencia a la obligación de informar al interesado cuando los datos no hayan sido recabados del interesado, también indica que no existirá dicha obligación, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando:

- la información al interesado resulte imposible,
- exija esfuerzos desproporcionados,
- el registro o la comunicación de los datos estén expresamente prescritos por ley.[166]

Únicamente el artículo 11, apartado 2, de la Directiva de protección de datos establece que no es necesario informar a los interesados sobre las operaciones de tratamiento que estén prescritas por ley. Habida cuenta de la presunción jurídica general de conocimiento de la ley por parte de aquellos a quienes resulta aplicable, podría argumentarse que, en los casos en que los datos son recabados del propio interesado, con arreglo al artículo 10 de la Directiva, el interesado está informado. Pero, teniendo en cuenta que el conocimiento de la ley es únicamente una presunción, el principio de tratamiento leal exigiría, con arreglo al artículo 10, que se informe al interesado incluso si el tratamiento está prescrito por la ley, particularmente cuando informar al interesado no supone una carga especialmente pesada cuando los datos son recabados directamente del propio interesado.

En lo que atañe al Derecho del CdE, el Convenio nº 108 establece expresamente excepciones a su propio artículo 8. De nuevo, las excepciones establecidas en los artículos 10 y 11 de la Directiva de protección de datos pueden ser considerados ejemplos de buenas prácticas para las excepciones establecidas en el artículo 9 del Convenio nº 108.

Distintos modos de información

La forma ideal de información sería dirigirse individualmente a cada uno de los interesados, de forma oral o por escrito. Si los datos son recabados del propio interesado, la comunicación de la información debería realizarse a la par que la recogida. Sin embargo, en especial cuando los datos son recabados de terceros y, habida cuenta de las dificultades prácticas obvias para ponerse en contacto personalmente

166 *Ibid.*, considerando 40 y artículo 11, apartado 2.

con los interesados, la información también podrá proporcionarse mediante la publicación adecuada.

Uno de los modos más eficaces de información será que la página de inicio del responsable del tratamiento incluya las cláusulas de información oportunas, como una política de privacidad del sitio web. Existe, sin embargo, una parte significativa de la población que no utiliza Internet, por lo que la política de información de una empresa o de una autoridad pública deberá tener esto en cuenta.

4.3.2. Notificación

El Derecho nacional puede obligar a los responsables del tratamiento a que notifiquen a la autoridad de supervisión competente sus operaciones de tratamiento de forma que estas puedan ser publicadas. De forma alternativa, la legislación nacional podrá establecer que los responsables del tratamiento puedan utilizar un delegado de protección de datos personales, que sea responsable en particular de llevar un registro de los tratamientos efectuados por el responsable del tratamiento.[167] Este registro interno deberá estar disponible, previa petición, para el público interesado.

> Ejemplo: La notificación, así como la documentación del delegado de protección de datos personales interno, deberá describir las principales características del tratamiento de datos de que se trate. Esto incluirá información sobre el responsable del tratamiento, la finalidad del tratamiento, la base jurídica del tratamiento, las categorías de los datos tratados, los posibles terceros destinatarios y si están previstos los transfronterizos de flujos transfronterizos de datos y, en su caso, cuáles serían.

La publicación de notificaciones por parte de la autoridad de supervisión deberá revestir la forma de un registro especial. Para cumplir su objetivo, el acceso a dicho registro debe ser sencillo y gratuito. Esto mismo es aplicable a la documentación que conserva el delegado de protección de datos personales del responsable del tratamiento.

El Derecho nacional podrá establecer las excepciones a los deberes de notificar a la autoridad de supervisión competente o de contratar a un delegado de protección de datos personales interno que se enumeran en el artículo 18, apartado 2, de la

167 *Ibid.,* artículo 18, apartado 2, inciso segundo.

Directiva de protección de datos[168] para las operaciones de tratamiento que no suelen plantear un riesgo específico a los interesados.

4.4. Normas para promover el cumplimiento

Puntos clave

- Al desarrollar el principio de rendición de cuentas, la Directiva de protección de datos menciona diversos instrumentos para promover su cumplimiento:
  - el control previo por parte de la autoridad de supervisión nacional de las operaciones de tratamiento previstas;
  - delegados responsables de protección de datos personales que proporcionarán al responsable del tratamiento conocimientos específicos en el ámbito de la protección de datos;
  - códigos de conducta que especifican las normas de protección de datos existentes para su aplicación en sectores específicos, especialmente en los negocios.
- El Derecho del CdE propone instrumentos similares para promover el cumplimiento en su Recomendación sobre la elaboración de perfiles.

4.4.1. Controles previos

De conformidad con el artículo 20 de la Directiva de protección de datos, la autoridad de supervisión deberá verificar las operaciones de tratamiento que puedan suponer riesgos específicos para los derechos y libertades de los interesados, tanto por su finalidad como por las circunstancias del tratamiento, antes de que este último comience. El Derecho nacional deberá determinar qué operaciones de tratamiento deben ser objeto de control previo. Dicho control podrá tener como consecuencia la prohibición de las operaciones de tratamiento o una orden para modificar las características del diseño de las operaciones de tratamiento. El artículo 20 de la Directiva pretende garantizar que el tratamiento que suponga un riesgo innecesario ni siquiera comience ni tan se inicie, ya que la autoridad de supervisión tendrá competencia para prohibir dichas operaciones. El requisito previo para que este mecanismo sea eficaz es que la autoridad de supervisión sea verdaderamente notificada. Para garantizar que los responsables del tratamiento cumplen con su obligación de

168 *Ibid.*, artículo 18, apartado 2, inciso primero.

notificación, las autoridades de supervisión precisan disponer de poderes coercitivos, como la posibilidad de imponer multas a los responsables del tratamiento.

Ejemplo: Si una empresa realiza operaciones de tratamiento que, de conformidad con el Derecho nacional, están sujetas a control previo, dicha empresa deberá presentar a la autoridad de supervisión la documentación relativa a dichas operaciones. La empresa no estará autorizada a comenzar las operaciones de tratamiento sin antes recibir una respuesta positiva por parte de la autoridad de supervisión.

En algunos Estados miembros, el Derecho nacional establece como alternativa que las operaciones de tratamiento puedan comenzar si no hay reacción de la autoridad de supervisión en un plazo predeterminado, por ejemplo, en tres meses.

4.4.2. Delegados de protección de datos personales

La Directiva de protección de datos prevé la posibilidad de que el Derecho nacional establezca que los responsables del tratamiento puedan designar a un empleado para que actúe como delegado de protección de datos personales.[169] La misión de dicho empleado será garantizar que el tratamiento de datos no se realice en perjuicio de los derechos y libertades de los interesados.[170]

Ejemplo: En Alemania, con arreglo al artículo 4 *septies*, apartado 1, de la Ley Federal Alemana de protección de datos (*Bundesdatenschutzgesetz*), las empresas de titularidad privada deben designar a un delegado de protección de datos personales interno si emplean de forma permanente a diez o más personas en el tratamiento automatizado de datos personales.

La posibilidad de lograr dicho objetivo requiere que el puesto de delegado de protección de datos disponga de un cierto grado de independencia dentro de la organización del responsable del tratamiento, tal como señala expresamente la Directiva. También resultarán necesarios unos derechos laborales sólidos, que actúen de salvaguarda contra eventualidades como un despido improcedente, de forma apoyar el funcionamiento eficaz de su labor.

169 *Ibid.,* artículo 18, apartado 2, inciso segundo.

170 *Ibid.*

Con el fin de promover el cumplimiento de la legislación nacional en materia de protección de datos, también se ha adoptado el concepto de delegados responsable de protección de datos personales interno en algunas de las recomendaciones del CdE.[171]

4.4.3. Códigos de conducta

Las empresas y entidades de otros sectores pueden elaborar normas detalladas en relación con sus actividades de tratamiento típicas, codificando en ellas las mejores prácticas. Los conocimientos especializados de los miembros del sector favorecerán que se encuentren soluciones que sean prácticas y, por lo tanto, faciliten que sean seguidas. En consecuencia, se anima a los Estados miembros – así como a la Comisión Europea – a que promuevan la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la Directiva.[172]

Para garantizar que estos códigos de conducta son conformes con las disposiciones nacionales adoptadas con arreglo a la Directiva de protección de datos, los Estados miembros deberán establecer un procedimiento para evaluar los códigos. Este procedimiento normalmente necesitará la participación de la autoridad nacional, las asociaciones profesionales y otras organizaciones representantes de otras categorías de responsables de tratamientos.[173]

Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios ya existentes, podrán ser sometidos a examen del Grupo de Trabajo del Artículo 29. Una vez recibido el dictamen favorable del Grupo de Trabajo, la Comisión Europea podrá efectuar una publicidad adecuada de dichos códigos.[174]

Ejemplo: La Federación Europea de Marketing Directo e Interactivo (FEDMA) desarrolló un código europeo de buenas prácticas para el uso de datos personales en el sector del marketing directo. El código fue , con resultado satisfactorio,

171 Véase, por ejemplo, la Recomendación de creación de perfiles, artículo 8, apartado 3.

172 Véase la Directiva de protección de datos, artículo 27, apartado 1.

173 *Ibid.,* artículo 27, apartado 2.

174 *Ibid.,* artículo 27, apartado 3.

aprobado por el Grupo del Artículo 29. En 2010, se añadió un anexo relativo a las comunicaciones comerciales electrónicas.[175]

175 Grupo del artículo 29 (2010), *Dictamen 4/2010 relativo al «Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización directa»*, WP 174, Bruselas, de 13 de julio de 2010.

5

Los derechos del interesado y su aplicación

UE	Materias cubiertas	CdE
Derecho de acceso		
Directiva de protección de datos, artículo 12 TJUE, asunto C-553/07, *College van burgemeester en wethouders van Rotterdam contra M.E.E. Rijkeboer*, de 7 de mayo de 2009	**Derecho de acceso a los propios datos**	Convenio nº 108, artículo 8, letra b)
	Derecho de rectificación, supresión (cancelación) o bloqueo	Convenio nº 108, artículo 8, letra c) TEDH, *Cemalettin Canli contra Turquía*, nº 22427/04, de 18 de noviembre de 2008 TEDH, *Segerstedt-Wiberg y otros contra Suecia*, nº 62332/00, de 6 de junio de 2006 TEDH, *Ciubotaru contra Moldavia*, nº 27138/04, de 27 de abril de 2010
Derecho de oposición		
Directiva de protección de datos, artículo 14, apartado 1, letra a)	**Derecho de oposición debido a la situación particular del interesado**	Recomendación sobre perfilado, artículo 5.3

Directiva de protección de datos, artículo 14, apartado 1, letra b)	**Derecho de oposición a un uso posterior de los datos con fines de prospección comercial**	Recomendación sobre marketing directo, artículo 4.1
Directiva de protección de datos, artículo 15	**Derecho de oposición a las decisiones automatizadas**	Recomendación sobre perfilado, artículo 5.5
Supervisión independiente		
Carta, artículo 8, apartado 3 Directiva de protección de datos, artículo 28 Reglamento de protección de datos, de las instituciones de la UE, capítulo V TJUE, asunto C-518/07, *Comisión Europea contra la República Federal de Alemania*, de 9 de marzo de 2010 TJUE, asunto C-614/10, *Comisión Europea contra República de Austria*, de 16 de octubre de 2012 TJUE, asunto C-288/12, *Comisión Europea contra Hungría*, de 8 de abril de 2014	**Autoridades nacionales de supervisión**	Convenio nº 108, Protocolo adicional, artículo 1
Recursos y sanciones		
Directiva de protección de datos, artículo 12	**Solicitud al responsable del tratamiento**	Convenio nº 108, artículo 8, letra b)
Directiva de protección de datos, artículo 28, apartado 4 Reglamento de protección de datos de las instituciones de la UE, artículo 32, apartado 2	**Reclamaciones ante una autoridad de supervisión**	Convenio nº 108, Protocolo adicional, artículo 1, apartado 2, letra b)
Carta, artículo 47	**Tribunales (en general)**	CEDH, artículo 13
Directiva de protección de datos, artículo 28, apartado 3	**Tribunales nacionales**	Convenio nº 108, Protocolo adicional, artículo 1, apartado 4
TFUE, artículo 263, apartado 4 Reglamento de protección de datos de las instituciones de la UE, artículo 32, apartado 1 TFUE, artículo 267	**TJUE**	
	TEDH	TEDH, artículo 34

Recursos y sanciones		
Carta, artículo 47 Directiva de protección de datos, artículos 22 y 23 TJUE, asunto C-14/83, *Sabine von Colson y Elisabeth Kamann contra Land Nordrhein-Westfalen*, de 10 de abril de 1984 TJUE, asunto C-152/84, *M.H. Marshall contra Southampton and South-West Hampshire Area Health Authority*, de 26 de febrero de 1986	**En relación con los incumplimientos de la legislación nacional sobre protección de datos**	CEDH, artículo 13 (solo para los Estados miembros del CdE) Convenio nº 108, artículo 10 TEDH, *K.U. contra Finlandia*, nº 2872/02, de 2 de marzo de 2008 TEDH, *Biriuk contra Lituania*, nº 23373/03, de 25 de noviembre de 2008
Reglamento de protección de datos de las instituciones de la UE, artículos 34 y 49 TJUE, asunto C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd*, de 29 de junio de 2010	**En relación con los incumplimientos 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 mecanismos adecuados para su correcta aplicación. En la legislación europea en materia de protección de datos, el interesado debe estar facultado por la legislación nacional para proteger sus datos. El Derecho nacional también debe establecer autoridades de supervisión independientes para ayudar a que los interesados ejerzan sus derechos y supervisar el tratamiento de datos personales. De forma adicional, el derecho a un recurso efectivo, tal como garantiza el CEDH y la Carta, exige que estén disponibles recursos judiciales para las personas que así lo requieran.

5.1. Los derechos de los interesados

Puntos clave

- Toda persona tiene derecho con arreglo al Derecho nacional a solicitar información a los responsables del tratamiento sobre si están tratando datos que le conciernen.
- Con arreglo al Derecho nacional, los interesados tendrán derecho a:
  - el acceso a sus propios datos frente a cualquier responsable del tratamiento que trate dichos datos;

  - hacer que el responsable del tratamiento de sus datos los rectifique (o bloquee, según el caso), si los datos son inexactos;
  - hacer que sus datos sean suprimidos o bloqueados, según el caso, por el responsable del tratamiento si dicho responsable está tratando sus datos de forma ilegal.
- De forma adicional, los interesados tendrán derecho a oponerse frente a los responsables respecto de:
  - las decisiones automatizadas (adoptadas mediante el uso de datos personales tratados únicamente mediante procedimientos automatizados);
  - el tratamiento de sus datos si conduce a resultados desproporcionados;
  - el uso de sus datos para fines de marketing directo.

5.1.1. Derecho de acceso

Conforme al Derecho de la UE, el artículo 12 de la Directiva de protección de datos incluye los elementos del derecho de acceso del interesado a los datos, incluido el derecho a obtener del responsable del tratamiento «la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos», así como «la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos».

En el Derecho del CdE, existen estos mismos derechos y deben quedar establecidos por la legislación nacional (artículo 8 del Convenio nº 108). En diversas recomendaciones del CdE, se utiliza el término «acceso» y se describen los distintos aspectos del derecho de acceso, cuya aplicación en la legislación nacional debe proponerse del mismo modo que se ha descrito en el párrafo anterior.

De conformidad con el artículo 9 del Convenio nº 108 y el artículo 13 de la Directiva de protección de datos, la obligación de los responsables del tratamiento de responder a las peticiones de acceso del interesado podrá quedar limitada como consecuencia de los intereses legítimos prevalentes de otros. Por intereses legítimos prevalentes se entienden los intereses públicos como la seguridad nacional, la seguridad pública y la represión de infracciones penales, así como los intereses privados más fundados que los meros intereses de protección de los datos. Toda excepción o limitación deberá ser necesaria en una sociedad democrática y proporcionada

para el fin que persigue. 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 las posibles limitaciones en el derecho de acceso de todo interesado.

Cuando los datos se traten exclusivamente con fines de investigación científica o con fines estadísticos, la Directiva de protección de datos permite que el derecho nacional limite el derecho de acceso. Sin embargo, en estos casos, deberán aplicarse las garantías legales apropiadas. En particular, debe garantizarse que no se adoptan medidas o decisiones relativas a personas concretas en el contexto de dicho tratamiento de datos y que «no exista ningún riesgo de atentado contra la privacidad del interesado».[176] El artículo 9, apartado 3, del Convenio nº 108 contiene disposiciones similares.

El derecho de acceso a los propios datos

Según el Derecho del CdE, el derecho de acceso a los propios datos está reconocido por el artículo 8 del Convenio nº 108. El TEDH ha declarado en repetidas ocasiones que existe un derecho de acceso a la información sobre los propios datos personales que otras personas conservan o utilizan, y que dicho derecho deriva de la necesidad del respeto a la vida privada.[177] En el asunto *Leander*,[178] el TEDH concluyó que el derecho de acceso a los datos personales almacenados por las autoridades públicas podría ser objeto, sin embargo, de limitaciones en determinadas circunstancias.

Según el Derecho de la UE, el derecho de los individuos al acceso a los datos que le conciernen se reconoce expresamente en el artículo 12 de la Directiva de protección de datos y, como derecho fundamental, en el artículo 8, apartado 2, de la Carta.

El artículo 12, letra a), de la Directiva establece que los Estados miembros deben garantizar a todos los interesados el derecho a acceder a sus datos personales. En particular, todos los interesados tienen derecho a obtener del responsable del tratamiento la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como la información por lo menos de lo siguiente:

176 Directiva de protección de datos, artículo 13, apartado 2.

177 TEDH, *Gaskin contra el Reino Unido*, nº 10454/83, de 7 de julio de 1989; TEDH, *Odièvre contra Francia* [GS], nº 42326/98, de 13 de febrero de 2003; TEDH, *K.H. y otros contra Eslovaquia*, nº 32881/04, de 28 de abril de 2009; TEDH, *Godelli contra Italia*, nº 33783/09, de 25 de septiembre de 2012.

178 TEDH, *Leander contra Suecia*, nº 9248/81, de 11 de julio de 1985.

- los fines de dichos tratamientos,
- las categorías de datos a que se refieren,
- los datos objeto de los tratamientos,
- los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos,
- toda la información disponible sobre el origen de los datos objeto de los tratamientos,
- en los casos de decisiones automatizadas, la lógica que subyace al tratamiento automatizado de los datos.

La legislación nacional podrá añadir otros datos que el responsable del tratamiento podrá proporcionar, por ejemplo, indicar la base jurídica que autoriza el tratamiento de datos.

Ejemplo: Al acceder a los propios datos personales, las personas pueden establecer si los datos son o no exactos, por lo que resulta indispensable que se informe al interesado sobre las categorías de datos tratados, así como sobre el contenido de los datos. Por lo tanto, no es suficiente que el responsable del tratamiento comunique simplemente al interesado que está tratando su nombre, dirección, fecha de nacimiento y ámbito de interés. El responsable del tratamiento también podrá revelar al interesado que está tratando «el nombre: N.N.; una dirección: 1040 Viena, Schwarzenbergplatz 11, Austria; la fecha de nacimiento: 10.10.1974; el ámbito de interés (de conformidad con la declaración del interesado): música clásica». El último elemento incluye, además, información sobre el origen de los datos.

La comunicación al interesado sobre los datos que son objeto del tratamiento y toda la información disponible, en lo que atañe a su fuente, deberá realizarse de forma inteligible, lo cual significa que el responsable de los datos deberá explicar al interesado de forma detallada los datos que está tratando. Por ejemplo, indicar únicamente las abreviaturas técnicas o los términos médicos como respuesta a una solicitud de acceso no será suficiente, incluso si solo se almacenan las abreviaturas o los términos.

Deberá proporcionarse información sobre el origen de los datos que el responsable del tratamiento está tratando, como respuesta a una petición de acceso, siempre que la información esté disponible. Esta disposición ha de interpretarse a la luz de los principios de lealtad y rendición de cuentas. Los responsables del tratamiento no podrán destruir información sobre el origen de los datos para quedar exentos de la obligación de revelarlo, ni podrán ignorar el nivel habitual y las necesidades reconocidas para la documentación en el ejercicio de sus actividades. La no conservación de los documentos sobre el origen de los datos tratados por lo general no satisface las obligaciones del responsable del tratamiento que derivan del derecho de acceso.

Cuando se llevan a cabo evaluaciones automatizadas, será necesario explicar la lógica general de la evaluación, incluidos los criterios especiales que se han considerado al evaluar al interesado.

La Directiva no deja claro si el derecho de acceso a la información concierne al pasado y, en su caso, a qué periodo del pasado. En ese sentido, tal como ha subrayado la jurisprudencia del TJUE, el derecho de acceso a los propios datos no puede quedar limitado de forma indebida por limitaciones temporales. También debe proporcionarse a los interesados una oportunidad razonable de obtener información sobre las operaciones de tratamiento pasadas.

Ejemplo: En el asunto *Rijkeboer*,[179] se pidió al TJUE que determinara si, según el artículo 12, letra a), de la Directiva, el derecho de acceso del interesado a la información sobre los destinatarios o las categorías de destinatarios a quienes se comunican los datos puede circunscribirse al periodo de un año anterior a la solicitud de acceso.

Para determinar si el artículo 12, letra a), de la Directiva autoriza dicha limitación en el tiempo, el tribunal decidió interpretar dicho artículo a la luz de los objetivos de la misma. El Tribunal declaró en primer lugar que el derecho de acceso es indispensable para que el interesado ejerza el derecho de obtener del responsable del tratamiento de datos, la rectificación, la supresión o el bloqueo de los datos (artículo 12, letra b)) o que proceda a notificar a los terceros a quienes se hayan comunicado los datos, toda rectificación, supresión o bloqueo efectuado (artículo 12, letra c)). El derecho de acceso es, igualmente, condición necesaria para el ejercicio por el interesado del derecho de oposición al tratamiento de

179 TJUE, asunto C-553/07, *College van burgemeester en wethouders van Rotterdam contra M.E.E. Rijkeboer*, de 7 de mayo de 2009.

sus datos personales (artículo 14) como lo es para el derecho a recurrir por los daños sufridos (artículos 22 y 23).

Para garantizar el efecto útil de las disposiciones citadas anteriormente, el Tribunal sostuvo 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».

El derecho de rectificación, supresión y bloqueo de los datos

«Cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento».[180] En línea con estos principios, los interesados deben tener derecho de acuerdo a la legislación nacional a obtener del responsable del tratamiento la rectificación, la supresión o el bloqueo de los datos si consideran que su tratamiento no se ajusta a las disposiciones de la Directiva, en particular a causa del carácter incompleto o inexacto de los datos.[181]

Ejemplo: En el asunto *Cemalettin Canli contra Turquía*,[182] el TEDH consideró que constituía una violación del artículo 8 del CEDH una política de información incorrecta en procedimientos penales.

El demandante había estado dos veces implicado en procedimientos penales debido a su supuesta pertenencia a organizaciones ilícitas pero nunca había sido condenado. Cuando el demandante fue detenido de nuevo y se le acusó de otro delito, la policía envió al órgano jurisdiccional penal un informe titulado «*formulario de información sobre otros delitos*», en el cual aparecía que el demandante había sido miembro de dos organizaciones ilícitas. La petición del demandante de obtener el informe y de modificación de los antecedentes policiales no tuvo éxito. El TEDH sostuvo que la información del informe policial estaba incluida en el ámbito de aplicación del artículo 8 del CEDH, ya que la información pública también puede quedar dentro del ámbito de la «vida privada» cuando ha sido

180 Directiva de protección de datos, considerando 41.

181 *Ibid.,* artículo 12, letra b).

182 TEDH, *Cemalettin Canli contra Turquía*, nº 22427/04, de 18 de noviembre de 2008, apdos. 33, 42 y 43; TEDH, *Dalea contra Francia,* nº 964/07, de 2 de febrero de 2010.

recopilada y almacenada sistemáticamente en ficheros que las autoridades conservan. Además, el informe policial no era correcto y su elaboración y envío al órgano jurisdiccional penal no había sido realizado de conformidad con la ley. El Tribunal concluyó que había existido una violación del artículo 8.

Ejemplo: En el asunto *Segerstedt-Wiberg y otros contra Suecia*,[183] 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. El TEDH consideró satisfactorio que el almacenamiento de los datos en cuestión dispusiera de fundamento jurídico y persiguiera un fin legítimo. Respecto de algunos de los demandantes, el TEDH consideró que la conservación de datos continua suponía una injerencia desproporcionada en sus vidas privadas. Por ejemplo, en el caso del Sr. Schmid, 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 perseguía ningún interés para la seguridad nacional relevante, en especial debido a su carácter histórico. El TEDH concluyó que había existido una violación del artículo 8 del CEDH respecto de cuatro de los cinco demandantes.

En algunos casos, bastará que el interesado simplemente pida la rectificación, por ejemplo, de la forma en que se deletrea un nombre, cambiar la dirección o un número de teléfono. Si dichas peticiones están vinculadas, sin embargo, a cuestiones jurídicas, como la identidad jurídica del interesado o a corregir el lugar de residencia de entrega de documentos jurídicos, las solicitudes de rectificación no serán suficientes y el responsable del tratamiento estará facultado a solicitar pruebas de la supuesta inexactitud. Dichas peticiones no deben suponer una carga de la prueba no razonable sobre el interesado ni, por lo tanto, evitar que los interesados puedan exigir 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.[184]

Ejemplo: En el asunto *Ciubotaru contra Moldavia*,[185] el demandante no pudo modificar el registro de su origen étnico de moldavo a rumano en los expedien-

183 TEDH, *Segerstedt-Wiberg y otros contra Suecia*, nº 62332/00, de 6 de junio de 2006, apdos. 89 y 90; véase, asimismo, por ejemplo, TEDH, *M.K. contra Francia*, nº 19522/09, de 18 de abril de 2013.

184 TEDH, *Rotaru contra Rumanía*, nº 28341/95, de 4 de mayo de 2000.

185 TEDH, *Ciubotaru contra Moldavia*, nº 27138/04, de 27 de abril de 2010, apdos. 51 y 59.

tes oficiales, supuestamente debido al hecho de que no había logrado fundar su petición. El TEDH consideró aceptable que los Estados exigieran pruebas objetivas cuando registran la identidad étnica de una persona física. Cuando dicha petición estuviera basada en motivos meramente objetivos e infundados, las autoridades podían 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 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 emplearon las autoridades soviéticas para registrar a sus padres. Al evitar que se examinase la reclamación del demandante a la luz de pruebas objetivamente verificables, el Estado no cumplió con su obligación positiva de garantizarle al demandante el respeto efectivo a su vida privada. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

Durante el litigio o procedimiento civil ante una autoridad pública para decidir si los datos son o no correctos, los interesados podrán solicitar que se realice una inscripción o una anotación en el fichero de datos, destacando que se ha impugnado la exactitud de los mismos y que está pendiente una resolución oficial. Durante ese periodo, el responsable del tratamiento no deberá presentar los datos como ciertos o definitivos, en especial ante terceros.

La petición del interesado para que se supriman o eliminen sus datos está basada con frecuencia en la reivindicación de que el tratamiento no tiene una base legítima. Dichas reclamaciones se suelen plantear cuando el consentimiento ha sido revocado o cuando ya no son necesarios determinados datos para cumplir con la finalidad de la recogida de los datos. 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 legitimidad del mismo. De conformidad con el principio de rendición de cuentas, el responsable del tratamiento deberá ser capaz de demostrar en cualquier momento que existe una base jurídica sólida para sus tratamientos de datos, de lo contrario deberán detenerse.

Si se impugna el tratamiento de los datos porque los datos son supuestamente incorrectos o se tratan de forma ilícita, el interesado podrá solicitar, conforme al principio de tratamiento leal, que se bloqueen los datos en cuestión, lo cual significa que los

datos no serán suprimidos sino que el responsable del tratamiento deberá abstenerse de utilizarlos durante el periodo de bloqueo. Esto sería especialmente necesario si el uso continuado de los datos conservados inexactos o ilegítimos pudiera perjudicar al interesado. El derecho nacional deberá establecer más detalles sobre cuándo podrá plantearse la obligación de bloqueo del uso de los datos y el modo de ejercitar dicho bloqueo.

Los interesados, además, tienen derecho a obtener del responsable del tratamiento la notificación a terceros de cualquier bloqueo, rectificación o supresión, si éstos han recibido datos con anterioridad a dichas operaciones de tratamiento. Dado que el responsable del tratamiento ha de documentar la divulgación de datos a terceros, debería ser posible identificar a los destinatarios y la solicitud de supresión. Sin embargo, si mientras tanto se publican los datos en Internet, por ejemplo, puede que sea imposible suprimir los datos en todos los casos, ya que los destinatarios de los datos no pueden ser encontrados. De conformidad con la Directiva de protección de datos, será obligatorio contactar con los destinatarios de los datos para su rectificación, supresión o bloqueo de los datos, «si no resulta imposible o supone un esfuerzo desproporcionado».[186]

5.1.2. Derecho de oposición

El derecho de oposición incluye el derecho de oponerse a las decisiones individuales automatizadas, el derecho de oposición debido a la situación específica del interesado y el derecho de oposición al uso posterior de los datos para fines de marketing directo.

El derecho de oposición a las decisiones individuales automatizadas

Las decisiones automatizadas son decisiones adoptadas mediante el uso de datos personales tratados únicamente mediante procedimientos automatizados. Si es posible que dichas decisiones tengan un impacto considerable en las vidas de las personas físicas a las que conciernen puesto que, por ejemplo, hacen referencia a la solvencia, el rendimiento laboral, la conducta o la fiabilidad, será necesaria establecer una protección especial para evitar consecuencias inadecuadas. La Directiva de protección de datos establece que las decisiones automatizadas no deben

186 Directiva de protección de datos, artículo 12, letra c), en la parte segunda de la última frase.

determinar cuestiones que son importantes para las personas físicas, requiriendo que la persona física tenga derecho a revisar la decisión automatizada.[187]

Ejemplo: Un importante ejemplo práctico de toma de decisiones automatizadas es la calificación crediticia. Para decidir rápidamente sobre la solvencia de un futuro cliente, se recogen determinados datos como la profesión y la situación familiar del cliente y se combinan con datos sobre el interesado, que estén disponibles en otras fuentes, como los sistemas de informaciones de crédito. Dichos datos son incorporan automáticamente en un algoritmo de calificación, que calcula el valor total que representa la solvencia del cliente potencial. Por lo tanto, el empleado de la empresa puede decidir en cuestión de segundos si admite o no al interesado como cliente.

Sin embargo, según la Directiva, los Estados miembros permitirán que una persona pueda verse sometida a una decisión individual automatizada cuando los intereses del interesado no están en juego, porque la decisión favorece al interesado, o cuando los defiende por otros medios adecuados.[188] En el **Derecho del CdE** también existe un derecho de oposición inherente a las decisiones automatizadas, tal como puede verse en la Recomendación de perfilado.[189]

El derecho de oposición debido a la situación concreta del interesado

No existe un derecho general de oposición de los interesados al tratamiento de sus datos.[190] El artículo 14, letra a), de la Directiva de protección de datos, sin embargo, faculta al interesado a plantear una oposición por razones legítimas propias de su situación particular. En la Recomendación de perfilado del CdE se ha reconocido un derecho similar.[191] Dichas disposiciones tienen por objeto encontrar el equilibrio adecuado entre los derechos de protección de los datos del interesado y los derechos legítimos de los demás al tratar datos del interesado.

187 *Ibid.,* artículo 15, apartado 1.

188 *Ibid.,* artículo 15, apartado 2.

189 Recomendación de perfilado, artículo 5, apartado 5.

190 Véase, asimismo, TEDH, *M.S. contra Suecia*, nº 20837/92, de 27 de agosto de 1997, en la que se comunicaron datos médicos sin consentimiento ni la posibilidad de oposición; TEDH, *Leander contra Suecia*, nº 9248/81, de 26 de marzo de 1987; o TEDH, *Mosley contra el Reino Unido*, nº 48009/08, de 10 de mayo de 2011.

191 Recomendación de perfilado, artículo 5, apartado 3.

Ejemplo: Un banco almacena durante siete años datos sobre los clientes que han incumplido los pagos de préstamos. Un cliente cuyos datos están almacenados en esta base de datos solicita un nuevo préstamo. Se consulta la base de datos, se emite una evaluación de la situación financiera y se deniega el préstamo al cliente. El cliente puede, sin embargo, oponerse a que sus datos personales estén registrados en la base de datos y solicitar la supresión de los datos si puede demostrar que la falta de pago se debió exclusivamente a un error que corrigió inmediatamente después de tener conocimiento del mismo.

El efecto de una oposición que tiene éxito es que los datos en cuestión ya no podrán ser tratados por el responsable del tratamiento. Sin embargo, las operaciones de tratamiento efectuadas con los datos del interesado antes de la oposición seguirán siendo legítimas.

El derecho de oposición a un uso posterior de los datos para fines de marketing directo

El artículo 14, letra b), de la Directiva de protección de datos establece un derecho específico de oposición al uso de sus datos con fines de marketing directo. Dicho derecho también ha sido establecido en la Recomendación de marketing directo del CdE.[192] Este tipo de oposición está previsto que se plantee cuando los datos se pongan a disposición de terceros con fines de marketing directo. Deberá proporcionarse al interesado, por tanto, la posibilidad de oponerse antes de que se transfieran los datos.

5.2. Supervisión independiente

Puntos clave

- Para garantizar una protección de datos efectiva, deben establecerse autoridades de supervisión independientes de acuerdo al derecho nacional.
- Las autoridades nacionales de supervisión deberán actuar con total independencia, la cual deberá quedar garantizada en una ley fundamental y reflejada en la estructura organizativa específica de la autoridad de supervisión.

192 Consejo de Europa, Comité de Ministros (1985), Recomendación Rec(85)20 a los Estados miembros sobre la protección de los datos personales utilizados con fines de marketing directo, de 25 de octubre de 1985, artículo 4, apartado 1.

- Las autoridades de supervisión tienen tareas específicas, entre otras:
  - 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 del tratamiento y a los encargados del tratamiento;
  - intervenir, en caso necesario
    - avisando, amonestando o incluso multando a los responsables del tratamiento y los encargados del tratamiento,
    - ordenando que se rectifiquen, bloqueen o supriman los datos,
    - imponiendo una prohibición sobre el tratamiento;
  - someter los asuntos a los órganos jurisdiccionales.

La Directiva de protección de datos exige un control independiente como medio importante para garantizar una protección de datos efectiva. La Directiva introdujo un instrumento para la aplicación de la protección de datos que no aparecía ni en el Convenio nº 108 ni en las Directrices de la OCDE relativas a la privacidad.

Teniendo en cuenta que se ha demostrado que el control independiente es indispensable para el desarrollo de una protección de datos efectiva, una nueva disposición de las Directrices de la OCDE relativas a la privacidad revisadas 2013, pide a los países miembros que «establezcan y mantengan autoridades de aplicación de la protección de la privacidad con la dirección, los recursos y la experiencia técnica necesarios para ejercer sus competencias de forma eficaz y adoptar decisiones de forma objetiva, imparcial y coherente».[193]

Conforme al Derecho del CdE, el Protocolo adicional del Convenio nº 108 convirtió en obligatoria la creación de autoridades de supervisión. Este instrumento contiene en el artículo 1 el marco jurídico de las autoridades de supervisión independientes que las Partes Contratantes deben aplicar en sus derechos nacionales. Utiliza formulaciones similares a las empleadas en la Directiva de protección de datos para describir

193 OCDE (2013), Directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, apartado 19, letra c).

las tareas y competencias de dichas autoridades. En principio, las autoridades de supervisión deberían funcionar, por tanto, de la misma forma tanto en el Derecho de la UE como del CdE.

Conforme al Derecho de la UE, las competencias y la estructura organizativa de las autoridades de supervisión fueron fijadas en el artículo 28, apartado 1, de la Directiva de protección de datos. El Reglamento de protección de datos de las instituciones de la UE[194] establece al SEPD como autoridad de supervisión del tratamiento de datos por parte de los organismos e instituciones de la UE. Al destacar las funciones y responsabilidades de la autoridad de supervisión, dicho Reglamento está inspirado en la experiencia obtenida desde la promulgación de la Directiva de protección de datos.

La independencia de las autoridades de protección de datos queda garantizada en el artículo 16, apartado 2, del TFUE y el artículo 8, apartado 3, de la Carta. Esta última disposición contempla específicamente el control por parte de una autoridad independiente como un elemento esencial del derecho fundamental a la protección de los datos. Además, la Directiva de protección de datos exige a los Estados miembros que establezcan autoridades de control para supervisar la aplicación de la Directiva, que actuarán con total independencia.[195] La legislación que fundamenta la creación de un órgano de control no sólo debe incluir disposiciones que garanticen de forma específica la independencia sino que la estructura organizativa específica de la autoridad también debe demostrar independencia.

En 2010, el TJUE abordó por primera vez la cuestión del alcance del requisito de independencia de las autoridades de control en materia de protección de datos.[196] Los siguientes ejemplos ilustran su postura.

194 Reglamento (CE) nº 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, artículos 41 a 48.

195 Directiva de protección de datos, artículo 28, apartado 1, última frase; Convenio nº 108, Protocolo Adicional, artículo 1, apartado 3.

196 Véase FRA (2010), «*Fundamental rights: challenges and achievements in 20*10» (Derechos fundamentales: desafíos y logros para el año 2010), Informe anual de 2010, p. 59. La Agencia de los Derechos Fundamentales de la Unión Europea trató esta cuestión con mayor detalle en su informe «*Data protection in the European Union: the role of National Data Protection Authorities* (La protección de datos en la Unión Europea: el papel de las autoridades nacionales de protección de datos), que se publicó en mayo de 2010.

Ejemplo: En el asunto *Comisión contra República Federal de Alemania,*[197] la Comisión Europea había solicitado al TJUE que declarase que Alemania había adaptado de forma incorrecta el requisito de «total independencia» de las autoridades de supervisión responsables de garantizar la protección de los datos y, por tanto, incumplió las obligaciones que le incumben en virtud del artículo 28, apartado 1, de la Directiva de protección de datos. En opinión de la Comisión, el problema era que Alemania había sometido a la tutela del Estado a las autoridades de supervisión competentes para vigilar el tratamiento de datos personales en el sector no público en los diferentes Estados federales (*Länder*).

La apreciación del fundamento del recurso dependía, según el Tribunal, del alcance de la exigencia de independencia que establecía dicha disposición y, por lo tanto, de la interpretación del mismo.

El Tribunal subrayó que las palabras «con total independencia» del artículo 28, apartado 1, de la Directiva debe interpretarse según el tenor real de dicha disposición y con los objetivos y el sistema de la Directiva de protección de datos.[198] El Tribunal resaltó que las autoridades de supervisión son «las guardianas» de los derechos relacionados con el tratamiento de datos personales consagrados en la Directiva y su establecimiento en los Estados miembros se considera, por tanto, «un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales».[199] El Tribunal 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 el Estado o por los *Länder*, y no solamente de la de los organismos sujetos a control».[200]

El TJUE consideró asimismo 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. Tal como subrayó el tribunal, el artículo 44, apartado 2, precisa el concepto de independencia al añadir que, «en el ejercicio de sus funciones, el SEPD no solicitará ni

197 TJUE, asunto C-518/07, *Comisión Europea contra la República Federal de Alemania*, de 9 de marzo de 2010, apdo. 27.

198 *Ibid.*, apdos. 17 y 29.

199 *Ibid.*, apdo. 23.

200 *Ibid.*, apdo. 25.

admitirá instrucciones de nadie». Lo anterior descarta la supervisión estatal de una autoridad de control de protección de datos independiente.[201]

En consecuencia, el TJUE sostuvo que las instituciones alemanas de protección de datos a escala federal responsables de vigilar el tratamiento de datos personales en el sector no público no eran lo suficientemente independientes debido a que estaban sometidas a la tutela del Estado.

Ejemplo: En el asunto *Comisión contra Austria*,[202] el TJUE destacó problemas similares relacionados con la posición 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 Tribunal concluyó en este asunto que la legislación austriaca impedía a la autoridad austriaca de protección de datos ejercer sus funciones con total independencia en el sentido de la Directiva de protección de datos. La independencia de la autoridad austriaca de protección de datos no estaba lo suficientemente garantizada porque la Cancillería federal proporcionaba personal a la DSK, la supervisaba y tenía el derecho a estar informada en todo momento sobre su trabajo.

Ejemplo: En el asunto *Comisión Europea contra Hungría*,[203] el TJUE señaló que "la exigencia (...) según la cual debe garantizarse que cada 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 Tribunal también sostuvo que "Hungría ha incumplido las obligaciones que le incumben en virtud de 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, al poner fin antes de tiempo al mandato de la autoridad de control de la protección de datos personales".

Las autoridades de supervisión disponen de competencias y capacidades con arreglo al Derecho nacional para, entre otras:[204]

201 *Ibid.*, apdo. 27.

202 TJUE, asunto C-614/10, *Comisión Europea contra República de Austria*, de 16 de octubre de 2012, apdos. 59 y 63.

203 TJUE, asunto C-288/12, *Comisión Europea contra Hungría,* de 8 de abril de 2014, apdos. 50 y 67.

204 Directiva de protección de datos, artículo 28; véase asimismo el Convenio nº 108, Protocolo Adicional, artículo 1.

- asesorar a los responsables del tratamiento y a los interesados en relación con todas las cuestiones relativas a la protección de datos;
- investigar las operaciones de tratamiento e intervenir, en caso necesario;
- advertir o amonestar a los responsables del tratamiento;
- ordenar la rectificación, el bloqueo, la supresión o la destrucción de los datos;
- imponer una prohibición temporal o definitiva sobre el tratamiento;
- someter asuntos a los órganos jurisdiccionales competentes.

Para poder ejercer sus funciones, la autoridad de supervisión deberá tener acceso a todos los datos personales y a la información que resulte necesaria para su investigación, así como acceso a todos los locales en los que un responsable del tratamiento conserve la información relevante.

Existen diferencias considerables entre las jurisdicciones nacionales en relación con los procedimientos y los efectos jurídicos de las conclusiones de la autoridad de supervisión. Pueden variar desde recomendaciones parecidas a las del defensor de pueblo hasta resoluciones de ejecución inmediata. Por lo tanto, al analizar la eficacia de los recursos disponibles en una jurisdicción, dichos instrumentos deberán interpretarse en su contexto.

5.3. Recursos y sanciones

Puntos clave

- De conformidad con el Convenio nº 108, así como con la Directiva de protección de datos, el derecho nacional deberá establecer los recursos y sanciones adecuadas contra los incumplimientos del derecho de protección de datos.
  - El derecho a un recurso efectivo exige, con arreglo tanto al Derecho de la UE como al Derecho nacional, que se establezcan el derecho a recurso judicial contra los incumplimientos de los derechos de protección de datos, con independencia de la posibilidad de dirigirse a una autoridad de supervisión.
  - La legislación nacional deberá establecer sanciones que sean efectivas, equivalentes, proporcionadas y que tengan un efecto disuasorio.

- Antes de dirigirse a los órganos judiciales, se deberá contactar con un responsable del tratamiento. Si es obligatorio o no dirigirse a una autoridad de supervisión antes de recurrir a un tribunal, es una cuestión que debe determinar la legislación nacional.
- 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.
- Además, los interesados podrán dirigirse al TJUE, aunque solo en una medida muy limitada.

Los derechos con arreglo a la legislación en materia de protección de datos podrán ser ejercidos únicamente por las personas cuyos derechos estén en juego, las cuales son aquellas que son o, al menos, dicen ser los interesados. Dichas personas podrán ser representadas en el ejercicio de sus derechos por otras personas que, con arreglo a la legislación nacional, cumplan los requisitos necesarios. Los menores deberán estar representados por sus padres o tutores legales. Ante las autoridades de supervisión, una persona también podrá estar representada por asociaciones cuyo fin legítimo sea promover los derechos de protección de datos.

5.3.1. Peticiones al responsable del tratamiento

Los derechos mencionados en el apartado 3.2 deberán ser ejercidos ante el responsable del tratamiento. Dirigirse directamente a la autoridad nacional de supervisión o a un tribunal no ayudaría, puesto que la autoridad únicamente podría recomendar que primero se contacte con el responsable del tratamiento, y el tribunal consideraría que la solicitud no es admisible. Los requisitos formales de una petición jurídicamente relevante ante un responsable del tratamiento, especialmente si no se trata de una petición por escrito, deberán ser regulados por la legislación nacional.

La entidad con la que se ha contactado en calidad de responsable del tratamiento deberá reaccionar a la petición, incluso si no es el responsable del tratamiento. En todo caso, deberá emitirse una respuesta al interesado en el plazo establecido por la legislación nacional, incluso si es solo para decir que no se están tratando datos del solicitante. En el cumplimiento de las disposiciones del artículo 12, letra a), de la Directiva de protección de datos y el artículo 8, letra b), del Convenio nº 108, dicha solicitud deberá ser tratada «sin retrasos [...] excesivos». La legislación nacional debería, por tanto, disponer un plazo de respuesta que sea lo suficientemente corto que permita, sin embargo, que el responsable del tratamiento trate la solicitud de forma adecuada.

Antes de responder a la solicitud, la entidad con la que se ha contactado en calidad de responsable del tratamiento deberá establecer la identidad del solicitante para determinar si es, de hecho, la persona que dice ser y evitar de este modo un incumplimiento grave de la confidencialidad. Cuando los requisitos para establecer la identidad no quedan específicamente regulados por la legislación nacional, estos deberán ser decididos por el responsable del tratamiento. El principio de tratamiento leal exigiría, sin embargo, que los responsables del tratamiento no establezcan condiciones excesivamente gravosas para reconocer la identificación (y la autenticidad de la solicitud, tal como se ha indicado en el apartado 2.1.1).

La legislación nacional también deberá tratar la cuestión de si los responsables del tratamiento pueden exigir, antes de responder a las solicitudes, el pago de una tasa por parte del solicitante: El artículo 12, letra a), de la Directiva y el artículo 8, letra b), del Convenio nº 108 establecen que la respuesta a las solicitudes de acceso deberán proporcionarse «sin [...] gastos excesivos». La legislación nacional de muchos países europeos establece que las solicitudes con arreglo a la legislación en materia de protección de datos deberán ser gratuitas, siempre que el hecho de emitir una respuesta no suponga un esfuerzo excesivo o poco habitual. A su vez, los responsables del tratamiento están normalmente protegidos por la legislación nacional contra los abusos del derecho a obtener una respuesta a las solicitudes.

Si la persona, institución u organismo, contactado por el responsable del tratamiento, no niega ser el responsable del tratamiento, dicha entidad, dentro del plazo establecido por la legislación nacional, deberá:

- acceder a la solicitud y notificar a la persona solicitante sobre cómo se ha cumplido la solicitud; o

- informar al solicitante sobre el motivo por el que no se ha cumplido la solicitud.

5.3.2. Reclamaciones ante una autoridad de supervisión

Cuando una persona, que ha realizado una solicitud de acceso o ha interpuesto una oposición ante el responsable del tratamiento, no recibe una respuesta oportuna y satisfactoria, podrá ponerse en contacto con la autoridad nacional de supervisión de la protección de datos para reclamar su asistencia. Durante el procedimiento ante la autoridad de supervisión, debería aclararse si la persona, institución u organismo

al que se ha dirigido el solicitante estaba obligado a reaccionar a la solicitud y si la reacción fue correcta y suficiente. La persona será informada por la autoridad de supervisión del curso del procedimiento que trata su solicitud.[205] Los efectos jurídicos de los resultados del procedimiento ante las autoridades nacionales de supervisión dependerán de lo establecido en la legislación nacional: si las decisiones de la autoridad pueden ejecutarse legalmente, lo cual significa que son aplicables por la autoridad pública, o si es necesario interponer un recurso ante un tribunal si el responsable del tratamiento no sigue lo dispuesto en las resoluciones (dictamen, amonestación, etc.) de la autoridad de supervisión.

En el caso de que sean las instituciones u organismos de la UE quienes supuestamente hayan vulnerado los derechos de protección de datos contemplados en el artículo 16 del TFUE, el interesado podrá presentar una reclamación ante el SEPD,[206] la autoridad de supervisión independiente de protección de datos de las instituciones europeas, con arreglo al Reglamento de protección de datos de las instituciones de la UE, el cual establece las obligaciones y competencias del SEPD. Si en el plazo de seis meses, el SEPD no diera una respuesta, se entenderá desestimada la reclamación.

Las decisiones de la autoridad nacional de supervisión podrán recurrirse ante los tribunales. Esto resulta aplicable tanto para los interesados como para los responsables del tratamiento, que hayan participado en el procedimiento ante una autoridad de supervisión.

Ejemplo: El Comisario de Información del Reino Unido emitió una resolución el 24 de julio de 2013, por la que solicitaba a la policía de Hertfordshire que dejase de utilizar un sistema de seguimiento de placas de matrículas que consideró ilícito. Los datos recopilados por las cámaras eran almacenados tanto en las bases de datos de la policía local como en una base de datos centralizada. Las fotografías de las placas de matrícula se almacenaban durante dos años y las fotografías de los automóviles durante noventa días. Se consideró que dicho uso amplio de las cámaras y de otras formas de vigilancia no era proporcionado al problema que se estaba intentando solucionar.

205 Directiva de protección de datos, artículo 28, apartado 4.

206 Visto el Reglamento (CE) nº 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.

5.3.3. Interposición de una reclamación ante un tribunal

De conformidad con la Directiva de protección de datos, si a la persona que ha hecho una solicitud a un responsable del tratamiento con arreglo a la legislación en materia de protección de datos, no le ha satisfecho la respuesta del responsable del tratamiento, dicha persona estará facultada para interponer una reclamación ante un tribunal nacional.[207]

Si es obligatorio o no dirigirse a una autoridad de supervisión antes de recurrir a un tribunal, es una cuestión que deberá determinar la legislación nacional. En la mayoría de casos, sin embargo, será beneficioso para las personas que ejercen sus derechos de protección de datos recurrir primero a la autoridad de supervisión, puesto que los procedimientos para solicitar su asistencia deben ser gratuitos y poco burocráticos. Los conocimientos especializados que se documentan en la resolución de la autoridad de supervisión (dictamen, amonestación, etc.) también podrán servir de ayuda al interesado para ejercer sus derechos ante los tribunales.

De conformidad con el Derecho del CdE, las violaciones de los derechos de protección de datos, llevadas supuestamente a cabo a escala nacional de una Parte Contratante del CEDH y que constituyan, al mismo tiempo, una violación del artículo 8 del CEDH, podrán, además, ser objeto de recurso ante el TEDH, una vez agotadas todas las vías de recurso internas. La alegación de la violación del artículo 8 del CEDH ante el TEDH también debe cumplir otros criterios de admisibilidad (artículos 34 a 37 del CEDH).[208]

Aunque las demandas al TEDH pueden ir dirigidas únicamente contra las Partes Contratantes, también pueden dirigirse indirectamente contra acciones u omisiones de las partes privadas, 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 los incumplimientos de los derechos de protección de datos contemplados en su Derecho nacional.

207 Directiva de protección de datos, artículo 22.

208 CEDH, artículos 34 a 37, disponible en: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

Ejemplo: En el asunto *K.U. contra Finlandia,*[209] el demandante, un menor de edad, reclamó que se había publicado un anuncio de carácter sexual sobre su persona en un sitio de citas por Internet. El prestador de servicios no reveló la identidad de la persona que había publicado la información debido a las obligaciones de confidencialidad existentes en la legislación finlandesa. El demandante adujo que la legislación finlandesa no establecía una protección suficiente contra las actuaciones del particular que publicó datos incriminatorios en Internet sobre su persona. El TEDH resolvió que los Estados no solo estaban obligados a abstenerse de realizar injerencias arbitrarias en las vidas privadas de las personas físicas sino que, también, pueden quedar sometidos a obligaciones positivas que impliquen «la adopción de medidas destinadas a garantizar el respeto a la vida privada, incluso en el ámbito de las relaciones entre las personas físicas.». 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 proporcionaba dicha protección y el Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

Ejemplo: En el asunto *Köpke contra Alemania,*[210] la demandante había sido sospechosa de hurto en su lugar de trabajo, por lo que había sido objeto de videovigilancia encubierta. El TEDH concluyó que «nada indicaba que las autoridades internas no lograron un equilibrio justo, dentro de su margen de apreciación, entre el derecho al respeto a la vida privada del demandante con arreglo al artículo 8 y el interés del empresario en proteger tanto sus derechos de propiedad y el interés público de obtener una buena administración de la justicia». La demanda, por tanto, fue declarada inadmisible.

Si el TEDH considera que un Estado parte ha violado alguno de los derechos protegidos por el CEDH, dicho Estado parte estará obligado a ejecutar la sentencia de dicho Tribunal. 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 medidas generales que eviten violaciones similares a las que ha detectado el tribunal, ya sea mediante cambios en la legislación, la jurisprudencia o a través de otras medidas.

209 TEDH, *K.U. contra Finlandia*, nº 2872/02, de 2 de marzo de 2009.

210 TEDH, *Köpke contra Alemania* (dec.), nº 420/07, de 5 de octubre de 2010.

Cuando el TEDH considera que ha existido una violación del CEDH, el artículo 41 del CEDH establece que podrá conceder al demandante una satisfacción equitativa a expensas del Estado Parte.

De conformidad con el Derecho de la UE,[211] las víctimas de los incumplimientos de la legislación nacional en materia de protección de datos, que aplica la legislación europea en materia de protección de datos, podrán, en algunos casos, someter sus asuntos al TJUE. Existen dos posibles situaciones en las que una reclamación de incumplimiento de sus derechos de protección de datos por parte del interesado puede desembocar en un procedimiento ante el TJUE.

En el primer caso, el interesado tendría que ser una víctima directa de un acto administrativo o reglamentario de la UE que viole el derecho a la protección de datos de la persona física. De conformidad con el artículo 263, apartado 4, del TFUE:

> *«toda persona física o jurídica podrá interponer recurso [...] contra los actos de los que sea destinataria o que la afecten directa e individualmente y contra los actos reglamentarios que la afecten directamente y que no incluyan medidas de ejecución».*

Por tanto, las víctimas del tratamiento ilícito de sus datos por un órgano de la UE podrán recurrir directamente ante el Tribunal General del TJUE, que es el órgano que tiene competencia para dictar sentencia en asuntos relacionados con el Reglamento de protección de datos de las instituciones de la UE. La posibilidad de interponer una demanda directamente ante el TJUE también existe si una disposición jurídica de la UE afecta directamente a la situación jurídica de una persona.

La segunda situación hace referencia a la competencia del TJUE (Tribunal de Justicia) para pronunciar decisiones preliminares, con arreglo a lo dispuesto en el artículo 267 del TFUE.

Los interesados podrán, en el transcurso un procedimiento nacional, pedir al tribunal nacional que solicite una aclaración por parte del Tribunal de Justicia sobre la interpretación de los Tratados de la UE y sobre la interpretación y la validez de los actos de las instituciones, órganos u organismos de la UE. Dichas aclaraciones se

211 UE (2007), Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, firmado en Lisboa el 13 de diciembre de 2007, DO 2007 C 306. Véanse asimismo las versiones consolidadas del Tratado de la Unión Europea, DO 2012 C 326 y del TFUE, DO 2012 C 326.

denominan decisiones preliminares. Estas decisiones no son un recurso directo para el demandante sino que permiten a los tribunales nacionales garantizar una correcta interpretación del Derecho de la UE.

Si una parte del procedimiento ante los tribunales nacionales solicita que se remita una cuestión al TJUE, únicamente estarán obligados a cumplir dicha solicitud los tribunales nacionales que actúan como última instancia, contra cuya resolución no cabe recurso.

Ejemplo: En el asunto *Kärntner Landesregierung y otros*,[212] el Tribunal Constitución austriaco planteó preguntas al TJUE relativas a la validez de los artículos 3 a 9 de la Directiva 2006/24/CE (*Directiva sobre la conservación de datos*) a la luz de los artículos 7, 9 y 11 de la Carta, así como si determinadas disposiciones de la Ley federal austriaca de telecomunicaciones que transpone la Directiva sobre la conservación de datos eran incompatibles con aspectos de la Directiva de protección de datos y con el Reglamento de protección de datos de las instituciones de la UE.

El sr. Seitlinger, uno de los demandantes en el procedimiento ante el Tribunal Constitucional, sostuvo que utilizaba el teléfono, Internet y el correo electrónico tanto para su vida privada como con fines laborales. Por consiguiente, la información que envía y recibe pasa a través de las redes de telecomunicaciones públicas. Con arreglo a lo dispuesto en la Ley austriaca de telecomunicaciones de 2003, su prestador de servicios de telecomunicaciones está obligado legalmente a recopilar y almacenar datos sobre el uso que hace de la red. El sr. Seitlinger se dio cuenta de que dicha obtención y almacenamiento de sus datos personales no eran, en ningún caso, necesarios a los efectos técnicos de enviar la información de A a B en la red. Así como tampoco lo era la recogida y almacenamiento de dichos datos, ni siquiera de forma remota, a efectos de la facturación. El sr. Seitlinger ciertamente no había dado su consentimiento al uso de sus datos personales. El único motivo para la obtención y el almacenamiento de dichos datos extras era la existencia de la Ley austriaca de telecomunicaciones de 2003.

Por tanto, presentó un recurso ante el Tribunal Constitucional austriaco en el cual alegaba que las obligaciones legales de su proveedor de telecomunicaciones

212 TJUE, Asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitling y Otros*, de 8 de abril de 2014.

violaban sus derechos fundamentales, con arreglo a lo dispuesto en el artículo 8 de la Carta de la UE.

El TJUE emite una resolución relativa únicamente a los elementos constitutivos de la petición de decisión preliminar, mientras que el tribunal nacional sigue siendo competente de resolver acerca del litigio original.

En principio, el Tribunal de Justicia deberá responder a las cuestiones que se le formulan. No puede negarse a emitir una decisión preliminar, basándose en que dicha respuesta no será pertinente ni oportuna respecto del litigio principal. Sin embargo, podrá negarse si la cuestión no entra dentro de su ámbito de competencias.

Por último, si los derechos de protección de datos, que están garantizados por el artículo 16 del TFUE, son violados supuestamente por una institución u organismo de la UE durante el tratamiento de datos personales, el interesado podrá someter el asunto al Tribunal General del TJUE (artículo 32, apartados 1 y 4, del Reglamento de protección de datos de las instituciones de la UE). Esto mismo resulta aplicable a las resoluciones del SEPD relacionadas con dichas violaciones (artículo 32, apartado 3, del Reglamento de protección de datos de las instituciones de la UE).

Si bien el Tribunal General del TJUE es competente para resolver en asuntos relacionados con el Reglamento de protección de datos de las instituciones de la UE, cuando es una persona en calidad de miembro del personal de una institución u organismo de la UE quien interpone un recurso, dicha persona deberá recurrir al Tribunal de la Función Pública de la Unión Europea.

Ejemplo: El asunto *Comisión Europea contra The Bavarian Lager Co. Ltd*[213] ilustra los recursos disponibles contra las actividades o las resoluciones de las instituciones y organismos de la UE que resultan pertinentes para la protección de datos.

Bavarian Lager solicitó a la Comisión Europea acceso al acta completa de una reunión celebrada por la Comisión y que supuestamente hacía referencia a cuestiones jurídicas relevantes para la empresa. La Comisión había denegado la solicitud de acceso de la empresa basándose en intereses de protección de

213 TJUE, asunto C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd*, de 29 de junio de 2010.

datos superiores.[214] Contra dicha resolución, Bavarian Lager había interpuesto, en aplicación del artículo 32 del Reglamento de protección de datos de las instituciones de la UE, un recurso ante el TJUE, de manera más concreta, ante el Tribunal de Primera Instancia (el precursor del Tribunal General). En su resolución sobre el asunto T-194/04, *Bavarian Lager contra Comisión*, el Tribunal de Primera Instancia anuló la decisión de la Comisión de denegar la solicitud de acceso. La Comisión Europea recurrió dicha decisión al Tribunal de Justicia del TJUE. El Tribunal de Justicia dictó sentencia (en Gran Sala) anulando la sentencia del Tribunal de Primera Instancia y confirmando la denegación de la solicitud de acceso.

5.3.4. Sanciones

En el Derecho del CdE, el artículo 10 del Convenio nº 108 establece las sanciones y recursos adecuados que cada Parte deberá establecer para las violaciones de las disposiciones de derecho nacional que aplican los principios básicos de la protección de datos, contemplados en el Convenio nº 108.[215] **Según el Derecho de la Unión**, el artículo 24 de la Directiva de protección de datos establece que los Estados miembros «adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas [...]».

Ambos instrumentos conceden un amplio margen de discrecionalidad a los Estados miembros a la hora de elegir las sanciones y recursos adecuados. Ningún instrumento jurídico ofrece orientaciones especiales sobre la naturaleza o el tipo de sanciones adecuadas ni tampoco se ofrecen ejemplos de sanciones.

Sin embargo,

> *«aunque los Estados miembros disfrutan de un margen de discrecionalidad a la hora de determinar qué medidas son las más adecuadas para salvaguardar los derechos que las personas físicas extraen del Derecho de la Unión, de conformidad con el principio de cooperación leal, contemplado*

214 Para obtener un análisis del argumento, véase el documento: SEPD (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling* (Acceso público a los documentos que contienen datos personales después de la sentencia Bavarian Lager), Bruselas, SEPD, disponible en inglés: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

215 TEDH, *I. contra Finlandia*, nº 20511/03, de 17 de julio de 2008; TEDH, *K.U. contra Finlandia*, nº 2872/02, de 2 de diciembre de 2008.

en el artículo 4, apartado 3, del TUE, deberán observarse, sin embargo, los requisitos mínimos de eficacia, equivalencia, proporcionalidad y efecto disuasorio».[216]

El TJUE ha sostenido de forma repetida que el Derecho nacional no tiene libertad plena para establecer sanciones.

Ejemplo: En el asunto *Von Colson y Kamann contra Land Nordrhein-Westfalen*,[217] el TJUE destacó que todos los Estados miembros a quienes está dirigida una directiva están obligados a adoptar, en sus sistemas jurídicos nacionales, todas las medidas necesarias para garantizar que tienen plena eficacia, de conformidad con el objetivo que persiguen. El Tribunal sostuvo que, aunque los Estados miembros son libres para elegir las formas y medios de garantizar la aplicación de una Directiva, dicha libertad no afecta a la obligación que les ha sido impuesta. En concreto, un recurso legal efectivo debe permitir a la persona física ejercer y hacer valer el derecho en cuestión hasta su máxima expresión. Para lograr una verdadera protección eficaz, los recursos deberán desembocar en un procedimiento penal o compensatorio que tenga por resultado la imposición de sanciones con efecto disuasorio.

En lo que atañe a las sanciones contra los incumplimientos de la legislación de la Unión por parte de las instituciones y organismos de la UE, debido a la existencia de una remisión especial al Reglamento de protección de datos de las instituciones de la UE, están previstas sanciones únicamente en forma de acciones disciplinarias. Según el artículo 49 del Reglamento, «el 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 [...]».

216 FRA (2012), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package* (Dictamen de la Agencia de los Derechos Fundamentales de la Unión Europea relativo a la propuesta de paquete de reforma en materia de protección de datos), Viena, de 1 de octubre de 2012, p. 27 (versión española no disponible).

217 TJUE, C-152/84, C-14/83, *Sabine von Kolson y Elisabeth Kamann contra Land Nordrhein-Westfalen*, de 10 de abril de 1984.

6

Flujos transfronterizos de datos

UE	Materias cubiertas	CdE
Flujos transfronterizos de datos		
Directiva de protección de datos, artículo 25, apartado 1 TJUE, asunto C-101/01, *Bodil Lindqvist*, de 6 de noviembre de 2003	Definición	Convenio nº 108, Protocolo adicional, artículo 2, apartado 1
Libre circulación de los datos		
Directiva de protección de datos, artículo 1, apartado 2	Entre los Estados miembros de la UE	
	Entre las Partes Contratantes del Convenio nº 108	Convenio nº 108, artículo 12, apartado 2
Directiva de protección de datos, artículo 25	A los terceros países con un nivel adecuado de protección de datos	Convenio nº 108, Protocolo adicional, artículo 2, apartado 1
Directiva de protección de datos, artículo 26, apartado 1	A los terceros países en casos específicos	Convenio nº 108, Protocolo adicional, artículo 2, apartado 2, letra a)
Flujo limitado de datos a los terceros países		
Directiva de protección de datos, artículo 26, apartado 2 Directiva de protección de datos, artículo 26, apartado 4	Cláusulas contractuales	Convenio nº 108, Protocolo adicional, artículo 2, apartado 2, letra b) Guía para la elaboración de cláusulas contractuales
Directiva de protección de datos, artículo 26, apartado 2	Normas corporativas vinculantes	

UE	Materias cubiertas	CdE
Ejemplos: Acuerdo PNR UE-EE. UU Acuerdo SWIFT UE-EE. UU	Acuerdos internacionales especiales	

La Directiva de protección de datos no solo establece la libre circulación de datos entre los Estados miembros sino que también incluye disposiciones sobre los requisitos para la transferencia de datos personales a terceros países de fuera de la UE. El CdE también reconoce la importancia de aplicar normas para los flujos transfronterizos de datos a terceros países y, por ello, adoptó el Protocolo adicional al Convenio nº 108 en 2001. Dicho Protocolo asumió las principales características de la regulación sobre flujos transfronterizos de datos de las partes del Convenio y de los Estados miembros de la UE.

6.1. Naturaleza de los flujos transfronterizos de datos

Puntos clave

- El flujo de datos transfronterizos de datos personales a un destinatario que está sometido a una jurisdicción extranjera.

El artículo 2, apartado 1, del Protocolo adicional al Convenio nº 108 describe el flujo de datos transfronterizo como la transferencia de datos personales a un destinatario que está sujeto a una jurisdicción extranjera. El artículo 25, apartado 1, de la Directiva de protección de datos regula la «transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia [...]». Dicha transferencia de datos únicamente está permitida si se realiza con arreglo a las normas establecidas en el artículo 2 del Protocolo Adicional al Convenio nº 108 y, en el caso de los Estados miembros de la UE, además, de conformidad con lo dispuesto en los artículos 25 y 26 de la Directiva de protección de datos.

Ejemplo: En el asunto *Bodil Lindqvist*,[218] el TJUE sostuvo que «la conducta que consiste en hacer referencia, en una página de Internet, 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».

El Tribunal puntualizó entonces que la Directiva también establecía normas específicas dirigidas a garantizar un control, por parte de los Estados miembros, de las transferencias de datos personales hacia terceros países.

Sin embargo, teniendo en cuenta, por un lado, el estado de desarrollo de Internet en el momento de la elaboración de la Directiva y, por otro, la inexistencia, en la Directiva, de criterios aplicables al uso de Internet, «no cabe presumir que el legislador comunitario tuviera la intención, en su momento, de incluir en el concepto de "transferencia a un país tercero [de datos]" la difusión [...] de datos en una página web, ni siquiera cuando dichos datos estén al alcance de personas de terceros países que disponen de los medios técnicos para poder acceder a ellos».

No obstante, si la Directiva se «interpreta en el sentido de que existe una "transferencia a un país tercero de datos" cada vez que se publican datos personales en una página web, dicha transferencia será forzosamente una transferencia a todos los países terceros en los que existen los medios técnicos necesarios para acceder a Internet. El régimen especial que prevé [la Directiva] se convertiría entonces necesariamente, por lo que se refiere a las operaciones en Internet, en un régimen de aplicación especial. En efecto, en cuanto la Comisión detectara [...] que un solo país tercero no garantiza un nivel de protección adecuado, los Estados miembros estarían obligados a impedir cualquier difusión de los datos personales en Internet».

El principio de que la simple publicación de datos (personales) no sea considerada como un flujo de datos transfronterizo se aplica asimismo a los registros públicos en línea o a los medios de comunicación de masas, como los periódicos (electrónicos) y la televisión. Solo las comunicaciones que están dirigidas a destinatarios específicos encajan en el concepto de «flujo de datos transfronterizo».

218 TJUE, asunto C-101/01, *Bodil Lindqvist*, de 6 de noviembre de 2003, apdos. 27, 68 y 69.

6.2. Libre circulación de datos entre los Estados miembros o entre las Partes Contratantes

Puntos clave

- La transferencia de datos personales a otro Estado miembro del Espacio Económico Europeo o a otra Parte Contratante del Convenio nº 108 no deberá tener limitaciones.

Según el artículo 12, apartado 2, del Convenio nº 108, **en virtud del Derecho del CdE** deberá existir libre circulación de los datos personales entre las Partes del Convenio. La legislación nacional no deberá limitar la exportación de datos personales a la Parte Contratante, salvo si:

- lo exige el carácter especial de los datos,[219] o
- la limitación es necesaria con el fin de evitar que se eludan las disposiciones jurídicas nacionales sobre los flujos transfronterizos de datos a terceros.[220]

De conformidad con el Derecho de la UE, el artículo 1, apartado 2, de la Directiva de protección de datos prohíbe las restricciones o prohibiciones de la libre circulación de datos entre los Estados miembros por motivos de la protección de datos. El ámbito de la libre circulación de datos ha sido ampliado por el Acuerdo sobre el Espacio Económico Europeo (EEE),[221] que incluía a Islandia, Liechtenstein y Noruega en el mercado interior.

Ejemplo: Si una filial de un grupo de empresas internacional, que está establecida en diversos Estados miembros de la UE, entre ellos Eslovenia y Francia, transfiere datos personales de Eslovenia a Francia, dicha circulación de datos no deberá quedar limitada ni prohibida por la legislación nacional eslovena.

219 Convenio nº 108, artículo 12, apartado 3, letra a).

220 *Ibid.,* artículo 12, apartado 3, letra b).

221 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.

Si la misma filial desea, sin embargo, transferir los mismos datos personales a la empresa matriz en los Estados Unidos, el exportador de datos esloveno deberá seguir el procedimiento establecido en la legislación eslovena para los flujos transfronterizos de datos a terceros países sin la protección de datos adecuada, salvo si la empresa matriz ha adoptado los principios de privacidad de puerto seguro, un código de conducta voluntario sobre un nivel de protección de datos adecuado (véase el apartado 6.3.1).

Los flujos transfronterizos de datos a los Estados miembros del EEE para fines distintos de la remisión al mercado interior, como para investigar delitos no están sujetos, sin embargo, a las disposiciones de la Directiva de protección de datos y, por lo tanto, no están contemplados por el principio de la libre circulación de datos. En lo que atañe al Derecho del CdE, todos los ámbitos están incluidos en el ámbito de aplicación del Convenio nº 108 y del Protocolo adicional al Convenio nº 108, aunque las Partes Contratantes podrán establecer excepciones. Todos los miembros del EEE también son Partes del Convenio nº 108.

6.3. Libre circulación de datos a terceros países

Puntos clave

- La transferencia de datos personales a terceros países no deberá estar limitada con arreglo a la legislación en materia de protección de datos, si:
  - se ha determinado el carácter adecuado de la protección de datos del destinatario; o
  - es necesario para los intereses específicos del interesado o legítimos intereses superiores de los demás, en especial importantes intereses públicos.
- El carácter adecuado de la protección de datos de un tercer país significa que los principales principios de protección de datos han sido aplicados de manera eficaz en la legislación nacional de dicho país.
- Según el Derecho de la UE, la Comisión Europea evalúa el carácter adecuado de la protección de datos en un tercer país. Según el Derecho del CdE, será la legislación nacional quien regule el modo en que se evalúa el carácter adecuado.

6.3.1. Libre circulación de datos debido a la existencia de una protección adecuada

El Derecho del CdE permite que la legislación nacional autorice la libre circulación de los datos a Estados que no sean contratantes, si el Estado u organización destinatarios garantizan un nivel adecuado de protección para la transferencia prevista.[222] La legislación nacional decide el modo en que se evalúa el nivel de protección de datos en un país extranjero y quién debe evaluarlo.

Con arreglo al Derecho de la UE, el artículo 25, apartado 1, de la Directiva de protección de datos establece la libre circulación de datos a terceros países con un nivel adecuado de protección de datos. El requisito de nivel adecuado en lugar del de equivalencia posibilita que se distingan diferentes formas de aplicar la protección de datos. Según el artículo 25, apartado 6, de la Directiva, la Comisión Europea es competente para valorar el nivel de protección de datos en los países extranjeros mediante decisiones sobre el carácter adecuado de la protección y realizar consultas sobre la evaluación al Grupo del artículo 29, quien ha contribuido sustancialmente a la interpretación de los artículos 25 y 26.[223]

Una conclusión de que existe un carácter adecuado por parte de la Comisión tiene efectos vinculantes. Si la Comisión Europea publica en el *Diario Oficial de la Unión Europea* una decisión sobre el carácter adecuado de la protección para un determinado país, todos los países miembros del EEE y sus órganos estarán obligados a seguir la decisión, lo cual significa que los datos pueden circular a dicho país, sin seguir un procedimiento de comprobación o de autorización ante las autoridades nacionales.[224]

La Comisión Europea también puede evaluar partes del sistema jurídico de un país o limitarse a temas individuales. Por ejemplo, la Comisión emitió una decisión sobre el carácter adecuado de la protección que concernía exclusivamente a la legislación

222 Convenio nº 108, Protocolo adicional, artículo 2, apartado 1.

223 Véanse, por ejemplo, Grupo del artículo 29 (2003), *Documento de trabajo sobre transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de protección de datos de la UE a las normas corporativas vinculantes para las transferencias de datos internacionales*, WP 74, Bruselas, de 3 de junio de 2003; y el documento del Grupo 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, de 25 de noviembre de 2005.

224 Para consultar una lista continuamente actualizada de países que han recibido una decisión sobre el carácter adecuado de la protección, véase la página de inicio de la Comisión Europea, Dirección General de Justicia, disponible en: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

comercial privada.[225] También existen diversas decisiones sobre el carácter adecuado para las transferencias basadas en acuerdos entre la UE y otros Estados. Dichas decisiones hacen referencia exclusivamente a un único tipo de transferencia de datos, como la transferencia de los registros de nombres de los pasajeros por parte de las compañías aéreas a las autoridades extranjeras de control fronterizo cuando la compañía aérea vuela desde la UE a determinados destinos extranjeros (véase el apartado 6.4.3). En la práctica más reciente de transferencias de datos basadas en acuerdos especiales entre la UE y terceros países, se ha descartado generalmente la necesidad de emitir una decisión sobre el carácter adecuado de la protección, puesto que se presume que el propio acuerdo ya ofrece un nivel adecuado de protección de datos.[226]

Una de las decisiones de adecuación más importantes no se refiere en realidad a un conjunto de disposiciones jurídicas,[227] sino que, en su lugar, hace referencia a algo parecido a un código de conducta, conocido como los principios de privacidad de puerto seguro que fueron redactados entre la UE y los Estados Unidos para las empresas estadounidenses. La adhesión al puerto seguro se obtiene mediante un compromiso voluntario declarado ante el Departamento de Comercio de Estados Unidos y se documenta en una lista publicada por dicho departamento. Dado que uno de los elementos importantes del carácter adecuado es la eficacia de la aplicación de la protección de datos, el marco de puerto seguro también establece un cierto nivel de control estatal: podrán adherirse al puerto seguro únicamente aquellas empresas que estén bajo la supervisión de la Comisión Federal de Comercio de los Estados Unidos.

225 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.

226 Por ejemplo, el Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (DO 2012 L 215, pp. 5 a 14) o el 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 8, pp. 11 a 16.

227 Comisión Europea (2000), 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 2000 L 215.

6.3.2. Libre circulación de datos en casos específicos

Con arreglo al Derecho del CdE, el artículo 2, apartado 2, del Protocolo adicional al Convenio nº 108 permite la transferencia de datos personales a terceros países cuando no exista un nivel adecuado de protección de datos, siempre que la transferencia esté prevista por la legislación nacional y sea necesaria para:

- el interés específico del interesado, o
- los intereses legítimos prevalentes de otros, en especial importantes intereses públicos.

Conforme al Derecho de la UE, el artículo 26, apartado 1, de la Directiva de protección de datos incluye disposiciones que son similares a las disposiciones contempladas en el Protocolo adicional al Convenio nº 108.

En virtud de la Directiva, los intereses del interesado podrán justificar la libre circulación de datos a un tercer país si:

- el interesado ha dado su consentimiento inequívoco a la transferencia de los datos;
- el interesado establece, o pretende establecer, una relación contractual que exige de forma clara que los datos sean transferidos a un destinatario en el extranjero;
- se ha celebrado un contrato entre el responsable del tratamiento y un tercero en interés del interesado;
- la transferencia es necesaria para la salvaguardia del interés vital del interesado;
- en el caso de que la transferencia de datos tenga lugar desde un registro público; esto constituye un ejemplo de intereses superiores en el público en general para poder acceder a la información almacenada en registros públicos.

Los legítimos intereses de los demás podrán justificar la libre circulación transfronteriza de datos:[228]

228 Directiva de protección de datos, artículo 26, apartado 1, letra d).

- debido a un interés público importante, distinto de los asuntos de la seguridad pública o nacional, ya que estas no se encuentran contempladas en la Directiva de protección de datos; o

- para reconocer, ejercer o defender un derecho en un procedimiento judicial.

Los casos mencionados anteriormente deben entenderse como excepciones a la regla de que las transferencias de datos sin limitaciones a otros países exigen un nivel adecuado de protección de datos en el país destinatario. Las excepciones deben interpretarse siempre de forma restrictiva, tal como el Grupo del artículo 29 ha subrayado de forma repetida en el contexto del artículo 26, apartado 1, de la Directiva de protección de datos, en especial si el consentimiento es la supuesta base para la transferencia de datos.[229] El Grupo del artículo 29 ha concluido que las normas generales relativas al alcance jurídico del consentimiento también son aplicables al artículo 26, apartado 1, de la Directiva. Si, en el contexto de las relaciones laborales, por ejemplo, no queda claro que el consentimiento que han dado los empleados no ha sido un consentimiento libre, las transferencias de datos no estarán basadas en el artículo 26, apartado 1, letra a), de la Directiva. En dichos casos, será aplicable lo dispuesto en el artículo 26, apartado 2, el cual exige a las autoridades nacionales de protección de datos que emitan una autorización para las transferencias de datos.

6.4. Circulación limitada de datos a terceros países

Puntos clave

- Antes de exportar datos a terceros países que no garantizan un nivel adecuado de protección de datos, podría requerirse al responsable del tratamiento que someta el flujo de datos previsto a examen por parte de la autoridad de supervisión.
- El responsable del tratamiento que desee exportar datos deberá demostrar dos cuestiones durante dicho examen:
  - que existe una base jurídica para realizar la transferencia de datos al destinatario, y

229 Véase, en particular, Grupo 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, de 25 de noviembre de 2005.

  - que se han adoptado medidas para salvaguardar la protección adecuada de los datos en el destinatario.
- Las medidas para establecer una protección de datos adecuada en el destinatario pueden incluir:
  - estipulaciones contractuales entre el responsable de datos que exporta datos y el destinatario extranjero de los datos; o
  - normas corporativas vinculantes, normalmente aplicables a las transferencias de datos dentro de un grupo multinacional de empresas.
- Las transferencias de datos a autoridades extranjeras también pueden quedar reguladas por un acuerdo internacional especial.

La Directiva de protección de datos y el Protocolo adicional al Convenio nº 108 permiten que la legislación nacional establezcan regímenes para los flujos transfronterizos de datos a terceros países que no garanticen un nivel adecuado de protección de datos, en la medida en que el responsable del tratamiento ha celebrado acuerdos especiales para asegurar salvaguardas adecuadas de protección de datos en el destinatario y en la medida en que el responsable del tratamiento pueda demostrar este hecho a la autoridad competente. Este requisito únicamente se recoge de forma expresa en el Protocolo adicional al Convenio nº 108. Sin embargo, también se considera un procedimiento tipo con arreglo a la Directiva de protección de datos.

6.4.1. Cláusulas contractuales

Tanto en el **Derecho del CdE** como en el **Derecho de la UE** se hace mención a las cláusulas contractuales entre el responsable del tratamiento que exporta datos y el destinatario en el tercer país, como un medio posible de salvaguardar un nivel suficiente de protección de datos en el destinatario.

A **escala de la UE**, la Comisión Europea, con la ayuda del Grupo del artículo 29, ha desarrollado cláusulas contractuales tipo que han sido certificadas oficialmente por una Decisión de la Comisión como prueba de una protección de datos adecuada.[230] Dado que las decisiones de la Comisión son vinculantes en su totalidad en los Estados miembros, las autoridades nacionales encargadas de la supervisión de los flujos transfronterizos de datos deberán reconocer dichas cláusulas contractuales tipo en sus procedimientos.[231] Por tanto, si el responsable de la exportación de datos y

230 Directiva de protección de datos, artículo 26, apartado 4.

231 TFUE, artículo 288.

el destinatario en el tercer país acuerdan y firman estas cláusulas, deberán proporcionar a la autoridad de supervisión pruebas suficientes de que se han aplicado las garantías adecuadas.

La existencia de cláusulas contractuales tipo en el marco jurídico de la UE no prohíbe a los responsables del tratamiento que formulen otras cláusulas contractuales *ad hoc*. Deberán establecer, sin embargo, el mismo nivel de protección que el que proporcionan las cláusulas contractuales tipo. Las características más importantes de este tipo de cláusulas contractuales son:

- cláusulas de tercer beneficiario, las cuales permiten a los interesados ejercer derechos contractuales incluso cuando no son una de las partes del contrato;

- el destinatario de los datos o el importador accede a someterse al procedimiento de la autoridad nacional de supervisión y/o de los tribunales del responsable del tratamiento que exporta datos, en caso de litigio.

En la actualidad, están disponibles dos series de cláusulas tipo para las transferencias de responsable del tratamiento a responsable del tratamiento, que el responsable del tratamiento que exporta datos puede elegir.[232] Para las transferencias de responsable del tratamiento a encargado del tratamiento, existe una única serie de cláusulas contractuales tipo.[233]

En el contexto del **Derecho del CdE**, el Comité Consultivo del Convenio nº 108 redactó una guía de elaboración de cláusulas contractuales.[234]

232 La serie I está incluida en el anexo de la Decisión de la Comisión Europea (2001), 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; la serie II está incluida en el anexo de la Decisión de la Comisión (2004), 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.

233 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.

234 CdE, Comité Consultivo del Convenio nº 108 (2002), *Guía de elaboración de cláusulas contractuales que regulan la protección de datos durante la transferencia de datos personales a terceros no vinculados por un nivel adecuado de protección de los datos*.

6.4.2. Normas Corporativas Vinculantes

Es muy frecuente que las Normas Corporativas Vinculantes (BCR) multilaterales impliquen a diversas autoridades europeas de protección de datos al mismo tiempo.[235] Para que dichas reglas puedan ser aprobadas, junto con el proyecto de BCR deberán enviarse los formularios de solicitud normalizados a la autoridad principal.[236] La autoridad principal será identificable en el formulario de solicitud normalizado. Dicha autoridad informará posteriormente a todas las autoridades de supervisión de los países miembros del EEE en los que están establecidas filiales del grupo, aunque su participación en el proceso de evaluación de las BCR es voluntaria. Aunque no es vinculante, todas las autoridades de protección de datos afectadas deberían incorporar el resultado de la evaluación en sus procedimientos formales de concesión de licencias.

6.4.3. Acuerdos internacionales especiales

La UE ha celebrado acuerdos especiales para dos tipos de transferencias de datos:

Registros de Nombres de Pasajeros

Los datos de los Registros de Nombres de Pasajeros (PNR) son recopilados por las compañías aéreas durante el procedimiento de reserva e incluyen, entre otros datos, los nombres, direcciones, información sobre tarjetas de crédito y los números de asientos de los pasajeros aéreos. Según la legislación de los EE. UU., las compañías aéreas están obligadas a poner estos datos a disposición del Departamento de Seguridad del Territorio Nacional antes de la salida del pasajero. Esto es aplicable a los vuelos con destino a o con salida desde los Estados Unidos.

235 El contenido y la estructura de las normas corporativas vinculantes adecuadas se explican en el documento del Grupo del artículo 29 (2008), *Documento de trabajo por el que se establece un marco para la estructura de las Normas Corporativas Vinculantes*, WP 154, Bruselas, de 24 de junio de 2008; y en el documento del Grupo del artículo 29 (2008), *Documento de trabajo por el que se establece un cuadro con los elementos y los principios de las Normas Corporativas Vinculantes*, WP 153, Bruselas, de 24 de junio de 2008.

236 Grupo del artículo 29 (2007), *Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfer of personal data* (Recomendación 1/2007 sobre la solicitud tipo de aprobación de las normas corporativas vinculantes a la transferencia de datos personales), WP 133, Bruselas, de 10 de enero de 2007, (disponible en inglés).

Para asegurar una adecuada protección de los datos PNR en consonancia con las disposiciones de la Directiva 95/46/CE, se adoptó en 2004 un "paquete PNR".[237] El paquete incluía la adecuación del tratamiento de datos llevado a cabo por el Departamento de Seguridad Interior de los EEUU (DHS).

Tras la anulación por el TJUE del "paquete PNR"[238] la UE y los Estados Unidos firmaron dos acuerdos separados con una doble finalidad. En primer lugar, establecer una base jurídica para la divulgación de los datos PNR a las autoridades de EEUU y, en segundo lugar, establecer una protección de datos adecuada en el país destinatario.

El primer acuerdo sobre el modo en que los países de la UE y los Estados Unidos comparten y gestionan los datos, firmado en 2012, presentaba diversas carencias y fue sustituido en el mismo año por otro acuerdo, a fin de garantizar una mayor seguridad jurídica.[239] El nuevo acuerdo proporciona mejoras significativas. Dicho acuerdo limita y aclara los fines para los que puede utilizarse la información, como los delitos graves de carácter transnacional y el terrorismo y establece el periodo durante el que los datos pueden ser conservados: después de seis meses los datos deben ser despersonalizados y enmascarados. En caso de que sus datos se hayan utilizado de forma incorrecta, cualquier persona tiene derecho a recurrir por vía administrativa y judicial con arreglo a la legislación de los EE. UU. También tiene derecho a acceder a sus propios datos PNR y solicitar la rectificación por parte del Departamento de Seguridad del Territorio Nacional, lo cual incluye la posibilidad de supresión, si la información es inexacta.

El Acuerdo, que entró en vigor el 1 de julio de 2012, permanecerá en vigor durante un periodo de siete años, hasta 2019.

237 Decisión del consejo 2004/496/CE de 17 de mayo de 2004 sobre la conclusión de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América para el tratamiento y la transferencia de datos PNR por Transportistas Aéreos al Departamento de Seguridad Interior de los Estados Unidos, Oficina de Aduanas y Protección de Fronteras, DOCE 2004 L 183, p. 83, y Decisión de la Comisión 2004/535/CE de 14 de mayo de 2004 sobre la protección adecuada de los datos personales contenidos en el Registro de Nombres de Pasajeros de los pasajeros aéreos transferidos a la Oficina de Aduanas y Protección de Fronteras. DOCE 2004 L 235, pp. 11-22.

238 CJEU, Asuntos acumulados C-317/04 y C-318/04, *Parlamento Europeo contra Consejo de la Unión Europea*, 30 de mayo de 2006, apdos. 57, 58 y 59, en los que el Tribunal declaró que tanto la decisión de adecuación como el acuerdo relativo al tratamiento de datos están excluidos del ámbito de la Directiva.

239 Decisión 2012/472/UE del Consejo, de 26 de abril de 2012, relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, DO 2012 L 215/4. El texto del Acuerdo figura adjunto a la presente Decisión, DO 2012 L 215, pp. 5 a 14.

En diciembre de 2011, el Consejo de la Unión Europea aprobó la celebración de un Acuerdo actualizado UE-Australia sobre el tratamiento y transferencia de datos PNR.[240] El acuerdo entre la UE y Australia sobre los datos PNR es un paso más en la agenda de la UE, la cual incluye las directrices generales sobre los datos PNR,[241] la creación de un sistema EU-PNR[242] y la negociación de acuerdos con terceros países.[243]

Datos de mensajería financiera

La Sociedad de Telecomunicaciones Interbancarias Mundiales (*Society for Worldwide Interbank Financial Telecommunication* – SWIFT), con sede en Bélgica, que es la encargada del tratamiento de la mayoría de transferencias mundiales de dinero entre bancos europeos, operaba con un centro "espejo" en los Estados Unidos comenzó a recibir solicitudes de remisión de datos al Departamento del Tesoro de los Estados Unidos con fines de investigación del terrorismo.[244]

240 Decisión 2012/381/UE del Consejo, de 13 de diciembre de 2011 relativa a la celebración del Acuerdo entre la Unión Europea y Australia sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por los transportistas aéreos al Servicio de Aduanas y de Protección de las Fronteras de Australia, DO 2012 L 186/3. El texto del Acuerdo, que reemplazaba a otro anterior de 2008, se adjunta a la presente Decisión, DO 2012 L 186, pp. 4 a 16.

241 Véase, en particular, la Comunicación de la Comisión de 21 de septiembre de 2010 sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países, COM(2010) 492 final, Bruselas, de 21 de septiembre de 2010. Véase también Grupo de Trabajo del Artículo 20 (2010) Dictamen *7/2010 sobre la Comunicación de la Comisión Europea sobre enfoque global a las transferencias de datos de Registro de Nombres de Pasajeros (PNR) a terceros países*, WP 178, Bruselas 12 de noviembre de 2010.

242 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, de 2 de febrero de 2011. En abril de 2011, el Parlamento Europeo solicitó a la FRA que emitiese un dictamen sobre dicha propuesta y sobre su cumplimiento con la Carta de Derechos Fundamentales de la Unión Europea. Véase el documento: FRA (2011), *Opinion 1/2011 – Passenger Name Record* (Dictamen 1/2011 – Registro de nombres de los pasajeros), Viena, de 14 de junio de 2011 (versión española no disponible).

243 La UE está negociando un nuevo acuerdo PNR con Canadá, que reemplazará al acuerdo de 2006, actualmente en vigor.

244 Véanse, en este contexto, Grupo del artículo 29 (2011), *Dictamen 14/2011 relativo a la prevención del blanqueo de capitales y la financiación del terrorismo*, WP 186, Bruselas, de 13 de junio de 2011; Grupo 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, de 22 de noviembre de 2006; el documento de la Comisión belga de la protección de la privacidad (*Commission de la protection de la vie privée*) (2008), «*Control and recommendation procedure initiated with respect to the company SWIFT scrl*» (Procedimiento de control y de recomendación incoado respecto de la empresa SWIFT scrl), Decisión, de 9 de diciembre de 2008 (versión española no disponible).

Desde la perspectiva de la UE, no existía un fundamento jurídico suficiente para divulgar estos datos, esencialmente europeos, que eran accesibles desde los Estados Unidos únicamente porque uno de los centros de tratamiento del servicio de datos de SWIFT tenía su sede en dicho país. En 2010, se celebró un acuerdo especial entre la UE y Estados Unidos, conocido como Acuerdo SWIFT, para establecer la base jurídica necesaria para dichas transferencias y garantizar una protección de datos adecuada.[245]

En virtud de dicho acuerdo, se siguen facilitando al Departamento del Tesoro de los Estados Unidos los datos financieros almacenados por SWIFT 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 el espacio único de pagos en euros (SEPA).

EUROPOL debe recibir una copia de cada solicitud del Departamento del Tesoro de los Estados Unidos y comprobar si se cumplen los principios del Acuerdo SWIFT.[246] Si se confirma que es así, SWIFT deberá facilitar la información financiera directamente al Departamento del Tesoro de los Estados Unidos. El departamento deberá almacenar los datos financieros en un entorno físico seguro al que puedan únicamente acceder los analistas dedicados a la investigación del terrorismo o su financiación, y los datos se interconectarán con otras bases de datos. En general, los datos financieros recibidos por SWIFT se suprimirán a más tardar cinco años después de su recepción. Los datos financieros que son relevantes para investigaciones o acciones

245 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 la presente Decisión, DO 2010 L 195, pp. 5 a 14.

246 La Autoridad Conjunta de Supervisión de Europol ha llevado a cabo auditorías sobre las actividades de Europol en esta área, cuyos resultados están disponibles en: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

judiciales podrán ser conservados durante el tiempo que resulte necesario para dichas investigaciones o acciones judiciales.

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 así como a las autoridades responsables del mantenimiento del orden público o de lucha contra el terrorismo de los Estados miembros 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 en un Estado miembro de la UE, el compartir 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 en caso de que se considere que compartir datos es esencial para la prevención de una amenaza grave e inmediata contra la seguridad pública.

Supervisores independientes, incluida una persona designada por la Comisión Europea, vigilarán el cumplimiento de los principios del Acuerdo SWIFT.

Los interesados tienen derecho a obtener una confirmación de la autoridad responsable de la protección de datos en la UE competente de que se han cumplido sus derechos en materia de protección de datos. Los interesados también tienen derecho de rectificación, supresión o bloqueo de sus datos personales obtenidos y almacenados por el Departamento del Tesoro de los EE. UU., 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 es válido durante cinco años, hasta agosto de 2015, y se prorrogará automáticamente por periodos sucesivos de un año, a menos que una de las partes notifique a la otra por escrito por vía diplomática, con seis meses de antelación, su intención de no prorrogar el acuerdo.

7

Protección de datos en el contexto de la policía y justicia penal

UE	Materias cubiertas	CdE
	En general	Convenio nº 108
	Policía	Recomendación sobre la policía
		TEDH, *B.B. contra Francia*, nº 5335/06, de 17 de diciembre de 2009
		TEDH, *S. and Marper contra el Reino Unido*, nº 30562/04 y 30566/04, de 4 de diciembre de 2008
		TEDH, *Vetter contra Francia*, nº 59842/00, de 31 de mayo de 2005
	Delitos informáticos	Convenio sobre la Ciberdelincuencia
Protección de datos en el contexto de la cooperación transfronteriza de las autoridades policiales y judiciales		
Decisión marco de protección de datos	En general	Convenio nº 108 Recomendación sobre la policía
Decisión Prüm	Para los datos especiales: Impresiones digitales, ADN, vandalismo, etc.	Convenio nº 108 Recomendación sobre la policía
Decisión de EUROPOL Decisión de EUROJUST Reglamento Frontex	Por las agencias especiales	Convenio nº 108 Recomendación sobre datos policiales

Decisión Schengen II Reglamento VIS Reglamento EURODAC Decisión CIS	**Por los sistemas de información conjunta especiales**	Convenio nº 108 Recomendación sobre la policía TEDH, *Dalea contra Francia*, nº 964/07, de 2 de febrero de 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.

7.1. Derecho del CdE sobre la protección de datos en los asuntos de la policía y justicia penal

Puntos clave

- El Convenio nº 108 y la Recomendación sobre la policía del CdE abarcan 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.

A escala europea, el Convenio nº 108 abarca todos los ámbitos del tratamiento de datos personales, y sus disposiciones pretenden regular el tratamiento de datos personales en general. Por consiguiente, el Convenio nº 108 se aplica a la protección de datos en los ámbitos de la policía y justicia penal aunque las Partes Contratantes podrán limitar su aplicación.

Las funciones legales de las autoridades de policía y justicia penal con frecuencia requieren el tratamiento de datos personales que pueden implicar graves consecuencias para las personas físicas afectadas. La Recomendación sobre datos policiales adoptada por el CdE en 1987 proporciona orientaciones a las Partes Contratantes sobre cómo deben aplicar los principios del Convenio nº 108 en el contexto del tratamiento de datos personales por parte de las autoridades policiales.[247]

247 CdE, 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, de 17 de septiembre de 1987.

7.1.1. 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, con arreglo al artículo 8, apartado 1, del CEDH. Muchas de las sentencias del TEDH tratan sobre la justificación de dichas injerencias.[248]

Ejemplo: En el asunto *B.B. contra Francia*,[249] el TEDH decidió que la inclusión de un delincuente sexual convicto en una base de datos nacional judicial, entraba dentro del ámbito de aplicación del artículo 8 del CEDH. Sin embargo, dado que se habían aplicado las suficientes garantías de protección de datos, como el derecho del interesado a solicitar la supresión de los datos, la duración limitada del almacenamiento de datos y el acceso limitado a dichos datos, se había encontrado el justo equilibrio entre los intereses opuestos públicos y privados en juego. El Tribunal concluyó que no había existido una violación del artículo 8 del CEDH.

Ejemplo: En el asunto *S. and Marper contra el Reino Unido*,[250] ambos demandantes habían sido acusados de delitos, aunque no habían sido condenados. Sin embargo, la policía conservaba y almacenaba sus impresiones dactilares, perfiles de ADN y muestras de células. La ley permite la conservación ilimitada de datos biométricos cuando una persona ha sido sospechosa de un delito, incluso si el sospechoso fue posteriormente absuelto o puesto en libertad. El TEDH sostuvo que una conservación generalizada e indiscriminada de datos personales, que no está limitada en el tiempo y cuando las personas físicas absueltas únicamente tenían posibilidades limitadas para solicitar la supresión, constituía una injerencia desproporcionada con el derecho al respeto a la vida privada de los demandantes. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

Muchas otras sentencias del TEDH abordan la justificación de la injerencia en el derecho a la protección de datos mediante la vigilancia.

248 Véase, por ejemplo, TEDH, *Leander contra Suecia*, nº 9248/81, de 26 de marzo de 1987; TEDH, *M.M. contra el Reino Unido*, nº 24029/07, de 13 de noviembre de 2012; TEDH, *M.K. contra Francia*, nº 19522/09, de 18 de abril de 2013.

249 TEDH, *B.B. contra Francia*, nº 5335/06, de 17 de diciembre de 2009.

250 TEDH, *S. and Marper contra el Reino Unido*, nº 30562/04 y 30566/04, de 4 de diciembre de 2008, apdos. 119 y 125.

Ejemplo: En el asunto *Allan contra el Reino Unido,*[251] las autoridades grabaron de manera secreta las conversaciones privadas de un preso con un amigo en el área de visita de la prisión y con otro acusado en una celda. El TEDH sostuvo que el uso de dispositivos de grabación de audio y vídeo en la celda del demandante, el área de visitas de la prisión y sobre un compañero de prisión suponía una injerencia en el derecho a la vida privada del demandante. Como no existía un sistema legal para regular 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 el asunto *Klass y otros contra Alemania,*[252] los demandantes reclamaron que diversos actos legislativos alemanes que permitían la vigilancia secreta de correo, correo postal y telecomunicaciones violaban el artículo 8 del CEDH, en especial porque no se informó a la persona afectada de las medidas de vigilancia y no pudo recurrir a los tribunales una vez que dichas medidas habían finalizado. El TEDH sostuvo que la amenaza de vigilancia condujo necesariamente a una injerencia en la libertad de comunicación entre los usuarios de los servicios postales y de telecomunicaciones. Sin embargo, consideró que se habían aplicado las suficientes garantías contra los posibles abusos. El legislador alemán tenía fundamentos para considerar dichas medidas necesarias en una sociedad democrática para los intereses de la seguridad nacional y para prevenir desórdenes o actos delictivos. El Tribunal concluyó que no había existido una violación del artículo 8 del CEDH.

Dado que el tratamiento de datos por parte de las autoridades policiales puede tener un impacto significativo sobre las personas afectadas, es especialmente necesario que existan normas detalladas en materia de protección de datos para el correcto mantenimiento de las bases de datos en ese ámbito. La Recomendación del CdE sobre la policía pretendía abordar la cuestión ofreciendo orientaciones sobre cómo deben recopilarse los datos para labores policiales; cómo deben ser conservados los ficheros de datos en este ámbito; a quiénes se les permite tener acceso a estos ficheros, incluidas las condiciones de transferencia de datos a las autoridades policiales extranjeras; cómo los interesados deben poder ejercer sus derechos de protección de datos y cómo debe aplicarse el control por parte de las autoridades

251 TEDH, *Allan contra el Reino Unido*, nº 48539/99, de 5 de noviembre de 2002.

252 TEDH, *Klass y otros contra Alemania*, nº 5029/71, de 6 de septiembre de 1978.

independientes. También se tiene en cuenta la obligación de proporcionar una seguridad de datos adecuada.

La recomendación no permite una recopilación de datos abierta e indiscriminada por parte de las autoridades policiales. Limita la recopilación de datos personales por parte de las autoridades policiales a lo que sea necesario para la prevención de un peligro real o la supresión de un delito específico. Cualquier recopilación de datos adicional debería estar basada en la legislación nacional específica. El tratamiento de datos sensibles deberá limitarse a lo que sea una absoluta necesidad en el contexto de una investigación particular.

Cuando los datos personales se recopilan sin el conocimiento del interesado, este deberá ser informado de la recogida de los datos, tan pronto como dicha divulgación ya no represente un obstáculo para las investigaciones. La recopilación de datos mediante vigilancia técnica u otros medios automatizados también debería estar basada en disposiciones legales específicas.

Ejemplo: En el asunto *Vetter contra Francia*,[253] unos testigos anónimos habían acusado de homicidio al demandante. Dado que el demandante iba regularmente a casa de un amigo, la policía instaló dispositivos de escucha en ese lugar con la autorización del juez instructor. Basándose en la solidez de las conversaciones que fueron grabadas, el demandante fue detenido y enjuiciado por homicidio. Interpuso una demanda para que la grabación fuera declarada inadmisible como prueba, alegando, en particular, que no había estado prevista por la ley. En opinión del TEDH, la cuestión era si el uso de los dispositivos de escucha se había realizado «de conformidad con la ley». La intervención de locales privados no entraba manifiestamente en el ámbito de aplicación de los artículos 100 y ss. del Código de Enjuiciamiento Penal, dado que dichas disposiciones estaban relacionadas con la intercepción de líneas telefónicas. El artículo 81 del Código no indicaba con razonable claridad el alcance ni el modo de ejercicio del criterio arbitrario de las autoridades de permitir la vigilancia de las conversaciones privadas. En consecuencia, el demandante no había disfrutado del grado de protección mínimo a que tienen derecho los ciudadanos en un Estado de derecho en una sociedad democrática. El Tribunal concluyó que había existido una violación del artículo 8 del CEDH.

253 TEDH, *Vetter contra Francia*, nº 59842/00, de 31 de mayo de 2005.

La recomendación concluye estableciendo que, cuando se almacenen datos personales, debería hacerse una clara distinción entre: los datos administrativos y los datos policiales; los diferentes tipos de interesados, como sospechosos, condenados, víctimas y testigos; y los datos que se consideran hechos concretos y aquellos basados en sospechas o especulaciones.

La finalidad de los datos policiales deberá quedar estrictamente limitada. Esto tiene consecuencias respecto de la comunicación de los datos policiales a terceros: la transferencia o comunicación de dichos datos en el sector de la policía debería estar condicionado regirse a si existe o no un interés legítimo en el intercambio de la información. La transferencia o la comunicación de dichos datos fuera del sector policial debería permitirse únicamente cuando exista una obligación o autorización legal clara. Las transferencias o comunicaciones de carácter internacional deberán quedar limitadas a las autoridades policiales extranjeras y han de estar basadas en disposiciones jurídicas especiales, posiblemente acuerdos internacionales, salvo si resultan necesarias para evitar un peligro grave e inminente.

El tratamiento de datos por parte de la policía deberá ser objeto de una supervisión independiente para garantizar el cumplimiento con la legislación nacional en materia de protección de datos. Los interesados deberán disponer de todos los derechos de acceso incluidos en el Convenio nº 108. En los casos en los que los derechos de acceso de los interesados hayan sido limitados, con arreglo a lo dispuesto en el artículo 9 del Convenio nº 108, en interés de la eficacia de las investigaciones policiales, el interesado deberá tener derecho, con arreglo a la legislación nacional, a recurrir a la autoridad nacional de supervisión en materia de protección de datos o a otro órgano independiente.

7.1.2. 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. El CdE adoptó, por tanto, un instrumento jurídico internacional, el Convenio sobre la Ciberdelincuencia, también conocido como el Convenio de Budapest, para tratar la cuestión de los delitos cometidos contra y a través de redes electrónicas.[254] Dicho Convenio está abierto, asimismo, para la

254 Consejo de Europa, Comité de Ministros (2001), Convenio sobre la Ciberdelincuencia, CETS nº 185, Budapest, de 23 de noviembre de 2001, que entró en vigor el 1 de julio de 2004.

adhesión por parte de Estados no miembros del Consejo de Europa y, a mediados de 2013, se adhirieron como parte al Convenio cuatro Estados de fuera del CdE (Australia, la República Dominicana, Japón y los Estados Unidos) y otros doce no miembros lo han firmado o han sido invitados a adherirse.

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 los poderes procedimentales que comprenden el registro de redes informáticas y la intercepción de comunicaciones en el contexto de la lucha contra la ciberdelincuencia. Por último, permite una cooperación internacional eficaz. Un protocolo adicional al Convenio trata la tipificación de la propaganda racista y xenófoba en redes informáticas.

Si bien el Convenio no es realmente un instrumento para fomentar la protección de datos, sí que tipifica, en cambio, actividades que es posible que violen el derecho de protección de los datos del interesado. También obliga a las Partes Contratantes, a la hora de aplicar el Convenio, que prevé una protección adecuada de los derechos humanos y de las libertades y, en particular, de los derechos garantizados con arreglo al CEDH, como el derecho a la protección de datos.[255]

7.2. Derecho de la UE sobre la protección de datos en asuntos policiales y penales

Puntos clave

- En el ámbito de la UE, la protección de datos en el sector de la policía y justicia penal únicamente está regulada en el contexto de la cooperación transfronteriza de las autoridades policiales y judiciales.
- Existen sistemas de protección de datos especiales para la Oficina Europea de Policía (EUROPOL) y la unidad de cooperación judicial de la UE (EUROJUST), que son organismos de la UE que prestan asistencia y promueven la aplicación transfronteriza de la ley.

255 *Ibid.,* artículo 15, apartado 1.

- Los regímenes especiales de protección de datos también existen para los sistemas comunes de información que están establecidos a escala europea para el intercambio de información transfronterizo entre las autoridades policiales y judiciales competentes. Ejemplos importantes de lo anterior son los sistemas Schengen II, el Sistema de Información de Visados (VIS) y EURODAC, un sistema centralizado que contienen datos relativos a las impresiones dactilares de los nacionales de terceros países que solicitan asilo en uno de los Estados miembros.

La Directiva de protección de datos no es aplicable al ámbito de la policía y justicia penal. En el apartado 7.2.1 se describen los instrumentos jurídicos más importantes en este ámbito.

7.2.1. La Decisión marco de protección de datos

La Decisión marco 2008/977/JAI del Consejo relativa a la protección de datos tratados en el marco de la cooperación policial y judicial en materia penal (*Decisión marco de protección de datos*)[256] tiene por objeto brindar protección a las personas físicas cuando sus datos personales sean tratados con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecutar sanciones penales. Las autoridades competentes que trabajan en el ámbito de la policía y justicia penal actúan en nombre de los Estados miembros o de la UE. Dichas autoridades son agencias u organismos de la UE, así como autoridades de los Estados miembros.[257] La aplicabilidad de la Decisión marco queda limitada a garantizar la protección de datos en la cooperación transfronteriza entre estas autoridades y no se amplía a la seguridad nacional.

La Decisión marco de protección de datos está basada, en gran medida, en los principios y definiciones incluidos en el Convenio nº 108 y en la Directiva de protección de datos.

Los datos deberán ser utilizados solamente por la autoridad competente y únicamente para el fin para el que fueron transmitidos o puestos a disposición. El Estado miembro receptor deberá respetar las limitaciones en el intercambio de datos establecidas por la legislación del Estado miembro transmisor. Sin embargo, en determinadas condiciones, se permite el uso de los datos con un fin distinto por parte del Estado receptor. El registro y la documentación de las transmisiones constituyen

256 Consejo de la Unión Europea (2008), Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (*Decisión marco de protección de datos)*, DO 2008 L 350.

257 *Ibid.,* artículo 2, letra h).

un deber específico de las autoridades competentes a fin de ayudar a aclarar las responsabilidades derivadas de las reclamaciones. Las transferencias ulteriores de datos recibidos en el transcurso de una actividad de cooperación transfronteriza a terceros, requiere el consentimiento del Estado miembro en que los datos tienen su origen, aunque existen excepciones en casos urgentes.

Las autoridades competentes deberán adoptar las medidas de seguridad necesarias para proteger los datos personales contra cualquier forma ilícita de tratamiento.

Cada Estado miembro deberá garantizar que una o más autoridades nacionales de supervisión independientes se encarguen en su territorio de asesorar y vigilar la aplicación de las disposiciones adoptadas con arreglo a la Decisión marco de protección de datos. También entenderán de las solicitudes que cualquier persona le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales por parte de las autoridades competentes.

El interesado tendrá derecho a ser informado sobre el tratamiento de sus datos personales, y tendrá derecho de acceso, rectificación, supresión y bloqueo. Cuando el ejercicio de dichos derechos sea denegado por motivos importantes, el interesado deberá tener derecho a recurrir ante la autoridad nacional de supervisión y/o tribunal competentes. Si la persona sufre daños y perjuicios como consecuencia de las violaciones de la legislación nacional que aplica la Decisión marco de protección de datos, dicha persona tendrá derecho a obtener reparación del responsable del tratamiento.[258] En general, los interesados tendrán derecho a un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional de aplicación de la Decisión marco de protección de datos.[259]

La Comisión Europea ha propuesto una reforma, que está compuesta por un Reglamento general de protección de datos,[260] y una Directiva general de protección de

258 *Ibid.,* artículo 19.

259 *Ibid.,* artículo 20.

260 Comisión Europea (2012), Propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos), COM(2012) 11 final, Bruselas, de 25 de enero de 2012.

datos.[261] Esta nueva Directiva sustituirá a la actual Decisión marco de protección de datos y aplicará los principios y normas generales a la cooperación policial y judicial en materia penal.

7.2.2. Instrumentos jurídicos más específicos en materia de protección de datos en la cooperación transfronteriza en materia policial y de aplicación de la ley

Además de la Decisión marco de protección de datos, el intercambio de información entre los Estados miembros en materia policial y de aplicación de la ley queda regulado por una serie de instrumentos jurídicos, tales 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, y la Decisión del Consejo relativa a las disposiciones de cooperación entre las unidades de información financiera de los Estados miembros para el intercambio de información.[262]

Es importante señalar que la cooperación transfronteriza[263] entre las autoridades competentes implica de forma creciente el intercambio de datos de inmigración. Este ámbito del Derecho no pertenece a los asuntos de la policía y justicia penal aunque, en muchos aspectos, resulta relevante para el trabajo de las autoridades policiales y judiciales. Esto mismo puede predicarse de los datos sobre las mercancías que se importan o se exportan a la UE. La eliminación de controles fronterizos interiores dentro de la UE ha aumentado el riesgo de fraude, haciendo necesario que los Estados miembros intensifiquen su cooperación, en especial mejorando el

261 Comisión Europea (2012), Propuesta de 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 a la libre circulación de dichos datos (Directiva general de protección de datos), COM(2012) 10 final, Bruselas, de 25 de enero de 2012.

262 Consejo de la Unión Europea (2009), Decisión marco 2009/315/JAI, 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.

263 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, de 7 de diciembre de 2012.

intercambio transfronterizo de información, para detectar y enjuiciar de forma más eficaz las violaciones de las legislaciones aduaneras nacionales y de la UE.

La decisión Prüm

La Decisión 2008/615/JAI del Consejo 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,[264] es un importante ejemplo de cooperación transfronteriza institucionalizada para el intercambio de los datos conservados a escala nacional. El Tratado de Prüm era un acuerdo internacional de cooperación policial, firmado en 2005 por Bélgica, Alemania, España, Francia, Luxemburgo, Países Bajos y Austria.[265]

El objetivo de la decisión Prüm es ayudar a los Estados miembros a mejorar el intercambio de información a fin de prevenir y combatir la delincuencia en tres ámbitos: terrorismo, delincuencia transfronteriza y migración ilegal. Para ello, la Decisión establece disposiciones relativas a:

- el acceso automatizado a perfiles de ADN, datos de impresiones digitales y a 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.

Las bases de datos que están disponibles en virtud de la decisión Prüm quedan plenamente regidas por la legislación nacional, aunque el intercambio de datos queda, además, regulado por la decisión y, de forma más reciente, por la Decisión marco de

264 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.

265 Tratado 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, en: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

protección de datos. Los órganos competentes de control de dichos flujos de datos son las autoridades nacionales de supervisión de la protección de datos.

7.2.3. La protección de datos en EUROPOL y EUROJUST

EUROPOL

EUROPOL, la agencia de la UE en materia policial, tiene su sede en La Haya, con unidades nacionales de EUROPOL (UNE) en cada Estado miembro. EUROPOL fue creada en 1998; su estatuto jurídico como institución de la UE se basa en la Decisión del Consejo por la que se crea la Oficina Europea de Policía (*Decisión de EUROPOL*).[266] El objetivo de EUROPOL es ayudar a prevenir e investigar la delincuencia organizada, terrorismo y otras formas de delincuencia grave, que se especifican en el anexo de la Decisión de EUROPOL, cuando afecten a dos o más Estados miembros.

Para lograr sus objetivos, EUROPOL ha creado el Sistema de Información de EUROPOL, el cual proporciona una base de datos para que los Estados miembros intercambien información e inteligencia en materia penal a través de sus ENU. El Sistema de Información de EUROPOL puede utilizarse para poner a disposición datos relacionados con: las personas sospechosas, o condenadas por delitos que entran dentro de la competencia de EUROPOL, o las personas sobre las cuales hay indicios concretos de que cometerán dichos delitos. EUROPOL y las ENU podrán introducir datos directamente en el Sistema de Información de EUROPOL y extraer datos del mismo. Únicamente la parte que ha introducido los datos en el sistema podrá modificarlos, corregirlos o suprimirlos.

Cuando sea necesario para el desempeño de sus tareas, EUROPOL podrá almacenar, modificar y utilizar datos relacionados con delitos en ficheros de trabajo de análisis. Los ficheros de trabajo de análisis están abiertos con fines de ordenar, tratar o utilizar datos para facilitar investigaciones penales concretas, efectuadas por EUROPOL junto con los Estados miembros de la UE.

266 Consejo de la Unión Europea (2009), Decisión del Consejo, de 6 de abril de 2009 por la que se crea la Oficina Europea de Policía (Europol), DO 2009 L 121. Véase, asimismo, la propuesta de Reglamento que prevé, por tanto, un marco legal para una nueva Europol, que sucederá y sustituirá a la Europol creada por la Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol), y a la CEPOL creada por la Decisión 2005/681/JAI del Consejo, por la que se crea la Escuela Europea de Policía (CEPOL), COM(2013) 173 final.

En respuesta a los nuevos desarrollos, se creó en EUROPOL el Centro Europeo de Ciberdelincuencia que comenzó a funcionar el 1 de enero de 2013.[267] El centro sirve como centro de información de la UE sobre la ciberdelincuencia, contribuyendo a acelerar las reacciones en caso de delitos en línea, desarrollar y desplegar capacidades forenses digitales y proporcionar mejores prácticas relacionadas con las investigaciones de la ciberdelincuencia. El centro está enfocado en la ciberdelincuencia que:

- sea cometida por grupos organizados para generar grandes ganancias delictivas, como el fraude en línea;
- provoque un grave perjuicio a la víctima, como en el caso de la explotación sexual infantil en línea;
- afecte a la infraestructura y a los servicios de información indispensables de la UE.

Se refuerza el sistema de protección de datos que regula las actividades de EUROPOL. La decisión de EUROPOL establece en su artículo 27 que resultan aplicables los principios establecidos en el Convenio nº 108 y en la Recomendación sobre datos policiales relativos al tratamiento de datos automatizados y no automatizados. Las transmisiones de datos entre EUROPOL y los Estados miembros también deberán cumplir las normas incluidas en la Decisión marco de protección de datos.

A fin de garantizar el cumplimiento de la legislación de protección de datos aplicable y, en particular, que no se vulneran los derechos de las personas físicas mediante el tratamiento de datos personales, la Autoridad Común de Control (ACC) independiente de EUROPOL vigilará y controlará las actividades de EUROPOL.[268] 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 los datos. Toda persona que no esté satisfecha con la decisión de EUROPOL relativa al ejercicio de dichos derechos, podrá recurrir al Comité de Recursos de la ACC.

Si el perjuicio producido es consecuencia de errores de derecho o de hecho en los datos que son almacenados o tratados por EUROPOL, la víctima podrá recurrir

267 Véase, asimismo, SEPD (2012), *Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión Europea al Consejo y al Parlamento Europeo sobre la creación de un centro europeo de ciberdelincuencia*, Bruselas, de 29 de junio de 2012.

268 Decisión de EUROPOL, artículo 34.

únicamente a los tribunales que sean competentes en el Estado miembro en que se haya producido el hecho que originó el perjuicio.[269] EUROPOL compensará al Estado miembro si el daño o perjuicio ha sido consecuencia del incumplimiento de EUROPOL de sus obligaciones legales.

EUROJUST

EUROJUST, creada en 2002, es un organismo de la UE, con sede en La Haya, que promueve la cooperación judicial en las investigaciones y actuaciones judiciales relacionadas con la delincuencia grave, que afecten al menos a dos Estados miembros.[270] EUROJUST tiene competencia para:

- fomentar y mejorar la coordinación de las investigaciones y de las actuaciones judiciales entre las autoridades competentes de diversos Estados miembros;

- facilitar la ejecución de solicitudes y de 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 tendrá atribuidas las competencias necesarias para desempeñar las tareas que resulten necesarias para estimular y mejorar la cooperación judicial. Además, los miembros nacionales actuarán conjuntamente como un colegio para realizar las tareas especiales de EUROJUST.

EUROJUST podrá tratar datos personales en la medida en que esto 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 un delito o haber participado en su comisión, si el delito es competencia de EUROJUST, o han sido condenadas por tal delito. EUROJUST también podrá tratar determinada información relacionada con testigos o víctimas de delitos que sean de

269 *Ibid.,* artículo 52.

270 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*).

su competencia.[271] En circunstancias excepcionales, EUROJUST podrá, durante un periodo limitado, tratar datos personales más amplios relativos a las circunstancias de una infracción, cuando 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 ellos datos personales. EUROJUST podrá, asimismo, cooperar e intercambiar datos personales con terceros países y organizaciones.

Respecto de la protección de datos, EUROJUST deberá garantizar un nivel de protección equivalente al menos al de los principios del Convenio nº 108 del Consejo de Europa 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.[272]

Se ha creado una ACC independiente en EUROJUST con la labor de controlar el tratamiento de datos personales realizado por EUROJUST. Las personas físicas podrán recurrir a la ACC si no están satisfechas con la respuesta que EUROJUST proporciona a su solicitud de acceso, rectificación, bloqueo o supresión de datos personales. En los casos en que EUROJUST trate datos personales de forma ilícita, será responsable, con arreglo al Derecho nacional del Estado en que radica su sede, los Países Bajos, de todo perjuicio causado al interesado.

7.2.4. Protección de datos en los sistemas comunes de información a escala de la UE

Además del intercambio de datos entre los Estados miembros y la creación de autoridades de la UE especializadas en la lucha contra la delincuencia transfronteriza, se han creado a escala de la UE diversos sistemas comunes de información que sirven como plataforma para el intercambio de datos entre las autoridades nacionales y de la UE competentes, para fines específicos de aplicación de la ley, incluida la legislación aduanera y sobre inmigración. Algunos de estos sistemas fueron desarrollados a partir de acuerdos multilaterales que, posteriormente, fueron complementados

271 Versión consolidada de la Decisión 2002/187/JAI del Consejo, modificada por Decisión 2003/659/JAI del Consejo y por la Decisión 2009/426/JAI del Consejo, artículo 15, apartado 2.

272 Normas del Reglamento interno de Eurojust relativas al tratamiento y a la protección de datos personales, DO 2005 C 68/01, de 19 de marzo de 2005, p. 1.

con instrumentos jurídicos y sistemas de la UE, como el Sistema de Información de Schengen, el Sistema de Información de Visados, EURODAC, EUROSUR o el Sistema de Información Aduanera.

La Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud (eu-LISA),[273] creada en 2012, es responsable de la gestión operativa a largo plazo del Sistema de Información de Schengen de segunda generación (SIS II), el Sistema de Información de Visados (VIS) y EURODAC. La función principal de la Agencia es garantizar el funcionamiento eficaz, seguro y continuo de los sistemas de información de gran magnitud. También es responsable 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, diversos 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*), que tiene por objeto crear un espacio para la libre circulación de las personas, no obstaculizado por controles fronterizos dentro del territorio Schengen.[274] Para contrarrestar la amenaza a la seguridad pública que se puede derivar de la apertura de fronteras, se reforzaron los controles fronterizos en las fronteras exteriores del espacio Schengen, al tiempo que se estableció una estrecha cooperación entre las autoridades nacionales de policía y de justicia.

Como consecuencia de la adhesión de otros Estados al Acuerdo de Schengen, el sistema Schengen fue integrado finalmente en el marco jurídico de la UE por el Tratado de Amsterdam.[275] La aplicación de esta decisión tuvo lugar 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, sirve a todos los Estados

273 Reglamento (UE) nº 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.

274 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.

275 Comunidades Europeas (1997), Tratado de Amsterdam 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.

miembros, más Islandia, Liechtenstein, Noruega y Suiza.[276] 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 C-SIS lo utilizan las autoridades nacionales de control fronterizo, policiales, aduaneras, de visado y judiciales en todo el Espacio Schengen. Cada Estado miembro utiliza una copia nacional del C-SIS, que se conoce como Sistema Nacional de Información Schengen (N-SIS), que es actualizada constantemente, actualizando de este modo el C-SIS. Se consulta el sistema N-SIS y este informará de la existencia de una descripción cuando:

- la persona no tenga derecho de entrada o de estancia en el territorio Schengen;
- la persona u objeto es buscado por las autoridades judiciales o policiales;
- se ha denunciado a la persona como desaparecida; o
- se ha informado de que los bienes, como billetes de banco, automóviles, camionetas, armas de fuego y documentos de identidad, han sido robados o son objetos perdidos.

En caso de una descripción, deberán iniciarse actividades de seguimiento a través de los Sistemas Nacionales de Información Schengen.

El sistema SIS II ha incorporado nuevas funcionalidades, como la posibilidad de introducir: datos biométricos, como impresiones dactilares y fotografías; o nuevas categorías de descripciones, como embarcaciones, aeronaves, contenedores o medios de pago robados; y descripciones mejoradas sobre personas y objetos; copias de órdenes de detención europeas (ODE) sobre personas buscadas para su detención, entrega o extradición.

276 Reglamento (CE) nº 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 Europa 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.

La Decisión 2007/533/JAI relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (Decisión Schengen II) incorpora el Convenio nº 108: «Los datos personales que se traten en aplicación de la presente decisión se protegerán de conformidad con el Convenio nº 108 del Consejo de Europa».[277] Cuando el uso de los datos personales por parte de las autoridades nacionales policiales se lleve a cabo en aplicación de la Decisión Schengen II, las disposiciones del Convenio nº 108, así como las disposiciones contempladas en la Recomendación sobre datos policiales, deberán aplicarse en la legislación nacional.

La autoridad nacional de supervisión competente de cada Estado miembro supervisa el sistema nacional N-SIS. En particular, deberá comprobar la calidad de los datos que el Estado miembro introduce en el sistema C-SIS a través del N-SIS. La autoridad nacional de supervisión velará 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. Las autoridades nacionales de supervisión y el SEPD cooperarán y garantizarán una supervisión coordinada del SIS, mientras que el SEPD es responsable de la supervisión del C-SIS. En aras de la transparencia, cada dos años se remitirá al Parlamento Europeo, al Consejo y al sistema eu-LISA un informe conjunto sobre las actividades realizadas.

Los derechos de acceso de las personas físicas relativos al SIS II podrán ejercerse en cualquier Estado miembro, ya que cada N-SIS es una copia exacta del C-SIS.

Ejemplo: En el asunto *Dalea contra Francia*,[278] se le había denegado al demandante un visado de visita a Francia, ya que las autoridades francesas habían informado al Sistema de Información Schengen de que debería denegársele la entrada. El demandante intentó sin éxito acceder y rectificar o suprimir los datos ante la Comisión francesa de protección de datos y, en última instancia, ante el Consejo de Estado francés. El TEDH resolvió que el hecho de informar sobre el demandante al Sistema de Información de Schengen se había producido de conformidad con la ley y había perseguido el fin legítimo de proteger la seguridad nacional. Dado que el demandante no demostró el modo en que había sufrido como resultado de la denegación de entrada en el espacio Schen-

277 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, artículo 57.

278 TEDH, *Dalea contra Francia* (dec), nº 964/07, de 2 de febrero de 2010.

gen, y teniendo en cuenta que se habían aplicado las medidas suficientes para protegerle contra decisiones arbitrarias, la injerencia en su derecho al respeto a la vida privada había sido proporcionada. Por tanto, la reclamación del demandante con arreglo al artículo 8 fue declarada inadmisible.

El Sistema de Información de Visados

El Sistema de Información de Visados (VIS), que también opera la Agencia eu-LISA, se desarrolló para dar apoyo a la aplicación de la política común de visados de la UE.[279] El sistema VIS permite a los Estados Schengen intercambiar datos sobre visados a través de un sistema que conecta los consulados de los Estados Schengen situados en países de fuera de la UE con los puntos de paso de las fronteras exteriores de todos los Estados Schengen. El sistema VIS trata datos relacionados con las solicitudes de visados para estancia de corta duración en, y para tránsito a través del, espacio Schengen. El sistema VIS permite a las autoridades fronterizas verificar, con la ayuda de datos biométricos, si la persona que presenta un visado es su legítimo titular e identificar a las personas sin documentos o con documentos fraudulentos.

Según el Reglamento (CE) nº 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*), solo pueden registrarse en el VIS datos relacionados con el solicitante, sus visados, las fotografías, las impresiones dactilares, los vínculos con solicitudes anteriores, y los expedientes de solicitud de personas que le acompañan.[280] El acceso al VIS para introducir, modificar o suprimir los datos estará reservado exclusivamente a las autoridades competentes en materia de visados de los Estados miembros, mientras que el acceso para consultar los datos se concede a las autoridades en materia de visados y a las autoridades competentes para realizar controles en los puntos de paso de las fronteras exteriores, controles de inmigración y asilo. En determinadas

279 Consejo de la Unión Europea (2004), Decisión del Consejo, de 8 de junio de 2004, por la que se establece el Sistema de Información de Visados (VIS), DO 2004 L 213; Reglamento (CE) nº 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 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.

280 Artículo 5 del Reglamento (CE) nº 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 (*Reglamento VIS*), DO 2008 L 218.

condiciones, las autoridades nacionales de policía competentes y EUROPOL podrán solicitar acceso a los datos introducidos en el VIS a efectos de prevenir, detectar e investigar delitos de terrorismo y otros delitos.[281]

EURODAC

El nombre EURODAC hace referencia a dactilogramas o impresiones dactilares. Es un sistema centralizado que contiene datos relativos a impresiones dactilares de nacionales de terceros países que solicitan asilo en uno de los Estados miembros de la UE.[282] El sistema ha estado en funcionamiento desde enero de 2003, y su finalidad es ayudar a determinar el Estado miembro responsable del examen de las solicitudes de asilo presentadas en un Estado miembro por un nacional de un tercer país (*Reglamento de Dublín II*).[283] Los datos personales en EURODAC podrán utilizarse únicamente para el fin de facilitar la aplicación del Reglamento de Dublín II; cualquier otro uso será objeto de sanciones.

EURODAC está compuesto por una unidad central, operada por la Agencia eu-LISA, para almacenar y comparar 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 las personas que no son nacionales de un Estado de la UE o que son apátridas, que tienen al menos catorce años, que solicitan asilo en su territorio, o que han sido interceptadas por un cruce no autorizado de su frontera exterior. Los Estados miembros también podrán tomar y transmitir las impresiones dactilares de nacionales de fuera de la UE o de apátridas que han sido encontrados en su territorio sin autorización.

281 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.

282 Reglamento (CE) nº 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) nº 407/2002 del Consejo, de 28 de febrero de 2002, por el que se establecen determinadas normas de desarrollo del Reglamento (CE) nº 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 de EURODAC*).

283 Reglamento (CE) nº 343/2003 del Consejo, de 18 de febrero de 2003, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados miembros por un nacional de un tercer país, DO 2003 L 50 (*Reglamento de Dublín II*).

Los datos relativos a impresiones dactilares se almacenan en la base de datos EURODAC únicamente de forma pseudonimizada. En el caso de que se produzca una correspondencia, se revelará al segundo Estado miembro el pseudónimo, junto con el nombre del primer Estado miembro que transmite los datos relativos a impresiones dactilares. Dicho segundo Estado miembro requerirá al primer Estado miembro puesto que, según el Reglamento de Dublín II, es dicho primer Estado miembro quien es responsable del tratamiento de la solicitud de asilo.

Los datos personales almacenados en EURODAC y relacionados con los solicitantes de asilo se conservan durante un periodo de diez años a partir de la fecha en que se tomaron las impresiones dactilares, salvo si el interesado obtiene la ciudadanía de un Estado miembro de la UE. En dicho caso, los datos deberán borrarse de inmediato. Los datos relacionados con nacionales extranjeros interceptados por un cruce no autorizado de la frontera exterior se almacenan por un periodo de dos años. Dichos 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.

Además de todos los Estados miembros de la UE, también aplican el sistema EURODAC, sobre la base de acuerdos internacionales, Islandia, Noruega, Liechtenstein y Suiza.

EUROSUR

El Sistema Europeo de Vigilancia de Fronteras (*EUROSUR*)[284] está diseñado para mejorar el control de las fronteras exteriores de Schengen con el fin de detectar, prevenir y combatir la inmigración ilegal y la delincuencia transfronteriza. Sirve para mejorar el intercambio de información y la cooperación operativa entre los centros nacionales de coordinación y la Agencia Frontex, la agencia de la UE encargada de desarrollar y aplicar el nuevo concepto de la gestión integrada de las fronteras.[285] Sus objetivos generales son los siguientes:

284 Reglamento (UE) nº 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.

285 Reglamento (UE) nº 1168/2011 del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, que modifica el Reglamento (CE) nº 2007/2004 del Consejo, por el que se crea una Agencia Europea para la gestión de la cooperación operativa en las fronteras exteriores de los Estados miembros de la Unión Europea, DO 2011 L 394 (*Reglamento Frontex*).

- 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.[286]

Comenzó a funcionar el 2 de diciembre de 2013 en todos los Estados miembros con fronteras exteriores y comenzará a funcionar, a partir del 1 de diciembre de 2014, en el resto de Estados. El Reglamento se aplicará a la vigilancia de las fronteras terrestres, marítimas exteriores y aéreas de los Estados miembros.

Sistema de Información Aduanera

Otro importante sistema común de información establecido a escala de la UE es el Sistema de Información Aduanera (CIS).[287] Con la creación de un mercado interior, se abolieron todos los controles y formalidades relativas a la circulación de mercancías dentro del territorio de la UE, lo cual aumentó el riesgo de fraude. Este riesgo fue contrarrestado por la intensificación de la cooperación entre las administraciones aduaneras de los Estados miembros. La finalidad del CIS es ayudar a los Estados miembros a prevenir, investigar y perseguir las infracciones graves de las normativas aduanera y agrícola nacionales y de la UE.

La información contenida en el CIS incluye datos personales relacionados con mercancías, medios de transporte, empresas, personas, retenciones, embargos o

286 Véanse asimismo: Comisión Europea (2008), Comunicación de la Comisión al Consejo, al Parlamento Europeo, 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, de 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, SEC(2011) 1536 final, Bruselas, de 12 de diciembre de 2011, p. 18.

287 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 (CE) nº 515/97 del Consejo 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 del Consejo, de 30 de noviembre de 2009, sobre la utilización de la tecnología de la información a efectos aduaneros, DO 2009 L 323 (*Decisión CIS*).

confiscaciones de mercancías y de dinero en efectivo. Dicha información puede utilizarse únicamente con fines de observación, informe, realización de inspecciones específicas o para análisis estratégicos u operativos relacionados con personas sospechosas de infringir las disposiciones aduaneras.

El acceso al CIS 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 que establecen el Reglamento No. 515/97 y el Convenio CIS,[288] así como las disposiciones de la Directiva de protección de datos, el Reglamento de protección de datos de las instituciones de la UE, el Convenio nº 108 y la Recomendación sobre datos policiales. El SEPD es responsable de la supervisión del cumplimiento del CIS con el Reglamento (CE) nº 45/2001 y convoca a una reunión al menos una vez al año con todas las autoridades nacionales de protección de datos competentes para las cuestiones de supervisión relacionados con el CIS.

288 *Ibid*.

8

Otras legislaciones europeas específicas en materia de protección de datos

UE	Materias cubiertas	CdE
Directiva de protección de datos Directiva sobre la privacidad en las comunicaciones electrónicas	**Comunicaciones electrónicas**	Convenio nº 108 Recomendación sobre los servicios de telecomunicación
Directiva de protección de datos, artículo 8, apartado 2, letra b)	**Relaciones laborales**	Convenio nº 108 Recomendación sobre el empleo
		TEDH, *Copland contra el Reino Unido*, nº 62617/00, de 3 de abril de 2007
Directiva de protección de datos, artículo 8, apartado 3	**Datos médicos**	Convenio nº 108 Recomendación sobre datos médicos
		TEDH, *Z. contra Finlandia*, nº 22009/93, de 25 de febrero de 1997
Directiva sobre ensayos clínicos	**Ensayos clínicos**	
Directiva de protección de datos, artículo 6, artículo 1, letras b) y e), artículo 13, apartado 2.	**Estadísticas**	Convenio nº 108 Recomendación sobre datos estadísticos
Reglamento (CE) nº 223/2009 relativo a la estadística europea TJUE, asunto C-524/06, *Huber contra Bundesrepublik Deutschland*, de 16 de diciembre de 2008	**Estadística oficial**	Convenio nº 108 Recomendación sobre datos estadísticos

Directiva 2004/39/CE relativa a los mercados financieros Reglamento (UE) No. 648/2012 relativo a los derivados extrabursátiles, las entidades de contrapartida central y los registros de operaciones Reglamento (CE) nº 1060/2009 sobre las agencias de calificación crediticia Directiva 2007/64/CE sobre servicios de pago en el mercado interior	Datos financieros	Convenio nº 108 Recomendación 90(19) sobre los datos de carácter personal utilizados con fines de pago y otras operaciones conexas TEDH, *Michaud contra Francia*, nº 12323/11, de 6 de diciembre de 2012

Se han adoptado instrumentos jurídicos especiales a escala europea, en diversas instancias, que aplican las normas generales del Convenio nº 108 o de la Directiva de protección de datos de forma más detallada a situaciones específicas.

8.1. 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 en las comunicaciones electrónicas.
- La confidencialidad de las comunicaciones electrónicas afecta no solo al contenido de la comunicación sino también a los datos de tráfico, como la información sobre quiénes se comunican entre sí, en qué momento y durante cuánto tiempo, así como a los datos de localización, tales como desde dónde se han comunicado los datos.

Las redes de comunicaciones tienen un mayor riesgo potencial de injerencias no justificadas en el ámbito personal de los usuarios, puesto que proporcionan posibilidades técnicas añadidas de escucha y de vigilancia de las comunicaciones a través de dichas redes. En consecuencia, se consideró necesario establecer disposiciones especiales en materia de protección de datos para abordar los riesgos especiales para los usuarios de los servicios de comunicaciones.

En 1995, el CdE emitió una Recomendación sobre la protección de los datos en el ámbito de los servicios de telecomunicación, especialmente en lo que se refiere a

los servicios telefónicos.[289] Según dicha recomendación, los fines de la obtención y tratamiento de datos personales en el contexto de las telecomunicaciones deben limitarse a: la conexión de los usuarios a la red, la puesta a disposición del servicio de telecomunicación determinado, la facturación y la verificación del pago, así como garantizar un funcionamiento técnico óptimo y el desarrollo de la red y del servicio.

También se prestó una atención especial 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 las normas detalladas en este ámbito.

En lo que atañe al **marco jurídico de la UE,** tras un primer intento en 1997, se adoptó en 2002 una Directiva sobre privacidad y comunicaciones electrónicas (*Directiva sobre la privacidad en las comunicaciones electrónicas*), que fue modificada en 2009, a fin de completar y especificar las disposiciones de la Directiva de protección de datos para el sector de las telecomunicaciones.[290] La aplicación de la Directiva sobre la privacidad en las comunicaciones electrónicas se limita a los servicios de comunicación en las redes electrónicas públicas.

La Directiva sobre la privacidad en las comunicaciones electrónicas distingue tres categorías de datos principales, generados durante una comunicación:

- los datos que constituyen el contenido de los mensajes enviados durante la comunicación; estos datos son estrictamente confidenciales;

289 CdE, 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, de 7 de febrero de 1995.

290 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) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores, DO 2009 L 337.

- los datos necesarios para establecer y mantener la comunicación, denominados datos de tráfico, tales como la información sobre los interlocutores, tiempo y duración de la comunicación;

- dentro de los datos de tráfico, existen datos que hacen especial referencia a la localización del dispositivo de comunicación, denominados datos de localización; dichos datos son, a su vez, datos sobre la localización *de los usuarios* de los dispositivos de comunicación y especialmente relevantes en relación con los usuarios de dispositivos de comunicación móvil.

Los datos de tráfico pueden ser utilizados por el prestador de servicios únicamente para fines de facturación y para la prestación técnica del servicio. Con el consentimiento del interesado, sin embargo, estos datos podrán ser relevados a otros responsables del tratamiento que ofrezcan servicios con valor añadido, como proporcionar información respecto de la localización del usuario junto a una estación de metro o una farmacia, o la previsión meteorológica para dicha localización.

El resto de accesos a los datos sobre comunicaciones en redes electrónicas, como el acceso con fines de investigación de delitos, deberá cumplir, según lo dispuesto en el artículo 15 de la Directiva sobre la privacidad en las comunicaciones electrónicas, los requisitos de las injerencias justificadas en el derecho a la protección de datos, tal como contempla el artículo 8, apartado 2, del CEDH y que ha quedado confirmado en los artículos 8 y 52 de la Carta.

Las modificaciones realizadas en la Directiva sobre la privacidad en las comunicaciones electrónicas a partir de 2009[291] introdujeron los siguientes cambios:

- Las restricciones al envío de correos electrónicos con fines de marketing directo se ampliaron a los servicios de mensajes cortos, los servicios de mensajería multimedia y otros tipos de aplicaciones similares; se prohíben los correos electrónicos de marketing, salvo si se obtiene el consentimiento previo. A falta de dicho consentimiento, los clientes anteriores únicamente podrán ser contactados con correos electrónicos de marketing, si han facilitado su dirección de correo electrónico y no se han opuesto a ello.

291 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) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores, DO 2009 L 337.

- Se estableció una obligación para los Estados miembros de proporcionar recursos judiciales contra las violaciones de la prohibición de comunicaciones no solicitadas.[292]

- Ya no se permite el establecimiento de cookies, programas informáticos de control y registro de las acciones de los usuarios de un ordenador, sin el consentimiento del usuario del ordenador. La legislación nacional deberá regular de forma más detallada el modo en que el consentimiento debe ser expresado y obtenido para que ofrezca una protección suficiente.[293]

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 supervisión competente deberá ser informada de inmediato. Los abonados deberán ser informados cuando los posibles daños y perjuicios sean consecuencia de una violación de datos.[294]

La Directiva sobre la conservación de datos[295] (invalidada el 8 de abril de 2014) obligaba a los prestadores de servicios de comunicación a que mantuvieran disponibles los datos de tráfico, en especial con el fin de luchar contra los delitos graves, durante un periodo de seis meses, como mínimo, y no superior a dos años, con independencia de que el prestador todavía necesitara dichos datos con fines de facturación o para el suministro técnico del servicio.

Los Estados miembros de la UE nombrarán autoridades públicas independientes responsables de controlar la seguridad de los datos conservados.

---

292 Véase la Directiva modificada, artículo 13.

293 Véase *Ibid.,* artículo 5; véase asimismo el Grupo del artículo 29 (2012), *Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies*, WP 194, Bruselas, de 7 de junio de 2012.

294 Véase, asimismo, Grupo 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, de 5 de abril de 2011 (versión española no disponible).

295 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.

La conservación de los datos de telecomunicaciones supone una injerencia clara en el derecho a la protección de datos[296] Si esta injerencia está o no justificada es una cuestión que ha sido impugnada en diversos procedimientos judiciales en los Estados miembros de la UE.[297]

Ejemplo: En el asunto *Digital Rights Ireland y Seitlinger y Otros*,[298] el TJUE declaró inválida la Directiva sobre la conservación de datos. Según el Tribunal, "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".

Una cuestión esencial en el contexto de las comunicaciones electrónicas resulta la injerencia por parte de las autoridades públicas. Los medios de vigilancia o intercepción de las comunicaciones, como los dispositivos de escucha o grabación, están autorizados únicamente si están previstos por la ley y constituyen una medida necesaria en una sociedad democrática para: proteger la seguridad del Estado, la seguridad pública, los intereses monetarios del Estado o la represión de infracciones penales; o proteger al interesado o los derechos y libertades de los demás.

Ejemplo: En el asunto *Malone contra el Reino Unido,*[299] se había acusado al demandante de una serie de infracciones relacionadas con el comercio fraudulento de bienes robados. Durante el juicio, se descubrió que una conversación telefónica del demandante había sido interceptada sobre la base de una autorización del Secretario de Estado del Ministerio del Interior (*Secretary of State for the Home Department*) del Reino Unido. A pesar de que la forma en que se interceptó la comunicación del demandante era legítima de conformidad con la legislación nacional, el TEDH consideró que no había existido una norma jurídica relativa al alcance y el modo de ejercicio de la discrecionalidad de que gozaban

296 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)*, de 31 de mayo de 2011.

297 Tribunal Constitucional Federal de Alemania (*Bundesverfassungsgericht*), 1 BvR 256/08, de 2 de marzo de 2010; Tribunal Constitucional Federal de Rumanía (*Curtea Constituțională a României*), nº 1258, de 8 de octubre de 2009; Tribunal Constitucional de la República Checa (*Ústavní soud České republiky*), nº 94/2011 Rec., de 22 de marzo de 2011.

298 TJUE, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger y Otros,* de 8 de abril de 2014, apdo. 65.

299 TEDH, *Malone contra el Reino Unido*, nº 8691/79, de 2 de agosto de 1984.

las autoridades públicas en este ámbito y que la injerencia se derivaba de la existencia de la práctica en cuestión y que, por lo tanto, no había sido realizada «de conformidad con la ley». El Tribunal sostuvo que había existido una violación del artículo 8 del CEDH.

8.2. 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 la Directiva 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 entre el empresario y los empleados. Las circunstancias del consentimiento deben valorarse de manera cuidadosa.

No existe un marco jurídico específico en la UE que regule el tratamiento de datos en el contexto del empleo. En la Directiva de protección de datos únicamente se hace una referencia específica a las relaciones laborales en el artículo 8, apartado 2, de la Directiva, que hace referencia al tratamiento de datos sensibles. Por lo que respecta al CdE, la Recomendación de datos de empleo se adoptó en 1989 y está en estos momentos en proceso de actualización.[300]

En un documento de trabajo del Grupo del artículo 29 puede encontrarse una encuesta de los problemas relacionados con la protección de datos más comunes en el contexto laboral.[301] El grupo de trabajo analizó la importancia del consentimiento como base jurídica para el tratamiento de datos de empleo[302] y consideró que el

300 Consejo de Europa, Comité de Ministros (1989), Recomendación Rec(89)2 del Comité de Ministros a los Estados miembros sobre la protección de los datos de carácter personal utilizados con fines de empleo, de 18 de enero de 1989. Véase, asimismo, Comité consultivo del Convenio nº 108, Estudio sobre la Recomendación nº R (89) 2 sobre la protección de los datos de carácter personal utilizados con fines de empleo y sugerir propuestas para la revisión de la citada Recomendación, de 9 de septiembre de 2011.

301 Grupo del artículo 29 (2001), *Dictamen 8/2001 sobre el tratamiento de datos de carácter personal en el contexto laboral*, WP 48, Bruselas, de 13 de septiembre de 2001.

302 Grupo 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, de 25 de noviembre de 2005.

desequilibrio económico entre el empresario que solicita el consentimiento y el empleado que da el consentimiento planteará con frecuencia dudas sobre si el consentimiento es o no libre. Por tanto, las circunstancias en las que se solicita el consentimiento deberán considerarse de forma cuidadosa a la hora de valorar la validez del consentimiento en el contexto laboral.

Un problema común en materia de protección de datos en el entorno laboral típico actual es el alcance legítimo del control de las comunicaciones electrónicas de los empleados en el lugar de trabajo. Con frecuencia se indica 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. La siguiente sentencia del TEDH resulta de especial interés en este contexto:

> Ejemplo: En el asunto *Copland contra el Reino Unido*,[303] el uso del teléfono, el correo electrónico y de Internet por una empleada de una universidad fue objeto de vigilancia de forma secreta, a fin de averiguar si estaba haciendo un uso excesivo de los servicios de dicha institución con fines personales. El TEDH sostuvo que las llamadas telefónicas desde las instalaciones profesionales quedan 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 que deriva del control del uso personal de Internet, quedaban protegida por el artículo 8 del CEDH. En el caso de la demandante, no existían disposiciones que regulasen las circunstancias en que los empresarios podrían controlar el uso del teléfono, el correo electrónico y de 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.

Según la Recomendación del CdE sobre empleo, los datos personales recopilados con fines laborales deberán ser obtenidos directamente del empleado individual.

Los datos personales recopilados para la contratación deberán 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 individuales. Los datos sobre juicios de valor deben estar basados en evaluaciones lícitas y

303 TEDH, *Copland contra el Reino Unido*, nº 62617/00, de 3 de abril de 2007.

honestas y no deben ser insultantes en el modo en que han sido formulados. Esto viene requerido por los principios de un tratamiento de datos leal y de exactitud de los datos.

Un aspecto específico de la legislación de protección de datos en la relación entre el empresario y el empleado es el papel que juegan los representantes de los trabajadores. Dichos representantes pueden recibir los datos personales de los empleados únicamente en la medida en que sea necesario para permitirles representar los intereses de los empleados.

Los datos personales sensibles recopilados con fines laborales únicamente podrán ser tratados en casos particulares y de acuerdo con las garantías establecidas en la legislación nacional. Los empresarios podrán preguntar a los empleados o a los solicitantes de empleo sobre su estado de salud o podrán someterlos a un reconocimiento médico únicamente si esto resulta necesario para: determinar su idoneidad para el empleo; cumplir las exigencias de la medicina preventiva; o permitir la concesión de prestaciones sociales. Los datos de salud no podrán ser obtenidos de otras fuentes distintas al empleado afectado, excepto cuando se haya obtenido un consentimiento expreso e informado o cuando quede establecido por la legislación nacional.

Con arreglo a la Recomendación sobre empleo, los empleados deberán ser informados en relación con la finalidad del tratamiento de sus datos personales, el tipo de datos personales almacenados, las entidades a las que deben comunicarse de forma periódica los datos, así como la finalidad y la base jurídica de dichas comunicaciones. Los empresarios deberían informar, asimismo, con antelación, a sus empleados sobre la introducción o la adaptación de sistemas automatizados para el tratamiento de datos personales de los empleados o para controlar los movimientos o la productividad de los empleados.

Los empleados deberán 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 deberán, además, tener derecho a impugnar dicho juicio. Sin embargo, estos derechos podrán estar limitados temporalmente para fines de investigaciones internas. Si se deniega al empleado el acceso, la rectificación o supresión de los datos personales de empleo, la legislación nacional deberá establecer los procedimientos adecuados para impugnar dicha denegación.

8.3. Datos médicos

Puntos 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, con arreglo al artículo 8, apartado 1, de la Directiva de protección de datos y, con arreglo al artículo 6 del Convenio nº 108. A su vez, los datos médicos están sometidos a un régimen de tratamiento de datos más estricto que los datos no sensibles.

> Ejemplo: En el asunto *Z. contra Finlandia*,[304] el ex marido de la demandante, que estaba infectado con VIH, había cometido una serie de delitos sexuales, por los que fue posteriormente condenado por homicidio, basándose en el hecho de que había expuesto conscientemente a sus víctimas al riesgo de infección por VIH. El tribunal nacional ordenó que la sentencia completa así como las actuaciones judiciales debían seguir siendo confidenciales 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, y su sentencia incluyó los nombres completos tanto de la demandante como de su ex marido. El TEDH sostuvo que la 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 a 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 conceder acceso a la situación médica y a la identidad de la demandante, tal como fue descrito en la sentencia del tribunal de apelación, tras un periodo de solo diez años desde que se dicta la sentencia violaría el artículo 8 del CEDH.

El artículo 8, apartado 3, de la Directiva de protección de datos permite el tratamiento de datos médicos cuando resulte necesario para la prevención o el

304 TEDH, *Z. contra Finlandia*, nº 22009/93, de 25 de febrero de 1997, apdos. 94 y 112; véase, asimismo, TEDH, *M.S. contra Suecia*, nº 20837/92, de 27 de agosto de 1997; TEDH, *L.L. contra Francia*, nº 7508/02, de 10 de octubre de 2006; TEDH, *I. contra Finlandia*, nº 20511/03, de 17 julio de 2008; TEDH, *K.H. y otros contra Eslovaquia*, nº 32881/04, de 28 de abril de 2009; TEDH, *Szuluk contra el Reino Unido*, nº 36936/05, de 2 de junio de 2009.

diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la 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.[305]

La Recomendación del CdE sobre datos médicos de 1997 aplica los principios del Convenio nº 108 al tratamiento de datos en el ámbito médico de forma más detallada.[306] Las normas propuestas son conformes a aquellas incluidas en la Directiva de protección de datos, en relación con los fines legítimos del tratamiento de datos médicos, las necesarias obligaciones de secreto profesional de las personas que emplean los datos de salud, así como los derechos de los interesados a la transparencia, acceso, rectificación y supresión. Además, los datos médicos que han sido tratados de forma lícita por parte de los profesionales sanitarios no podrán ser transferidos a las autoridades policiales excepto si se proporcionan «garantías suficientes para evitar una difusión que contravenga el respeto a [...] la vida privada, garantizado con arreglo al artículo 8 del CEDH».[307]

Además, la Recomendación sobre datos médicos incluye disposiciones especiales relativas a los datos médicos de los fetos y las personas discapacitadas, así como sobre el tratamiento de datos genéticos. Se reconoce expresamente que es motivo justificado para conservar durante un periodo más prolongado la investigación científica, aunque esto suele requerir que los datos se anonimicen. El artículo 12 de la Recomendación sobre datos médicos propone una normativa detallada para las situaciones en que los investigadores precisan datos personales y los datos anonimizados no resultan suficientes.

La pseudonimización 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 pseudonimización en el contexto de la protección de datos se explica con más detalle en el apartado 2.1.3.

Tanto a escala nacional como europea, ha existido un intenso debate sobre las iniciativas de almacenar en un expediente médico electrónico los datos relativos al

305 Véase, asimismo, TEDH, *Biriuk contra Lituania*, nº 23373/03, de 25 de noviembre de 2008.

306 CdE, Comité de Ministros (1997), Recomendación Rec(97)5 a los Estados miembros relativa a la protección de los datos médicos, de 13 de febrero de 1997.

307 TEDH, nº 1585/09, *Avilkina y otros contra Rusia*, de 6 de junio de 2013, apdo. 53 (sentencia no definitiva).

tratamiento médico de los pacientes.[308] Un aspecto particular de contar con sistemas a escala nacional es su disponibilidad en distintos países, lo que resulta una cuestión de especial interés en la UE en el contexto de la asistencia sanitaria transfronteriza.[309]

Otro ámbito sobre el que se debaten nuevas disposiciones son los ensayos clínicos, en otras palabras, la experimentación de nuevos medicamentos en pacientes, en un entorno de investigación documentada; de nuevo, esta cuestión tiene importantes repercusiones en la protección de datos. Los ensayos clínicos de productos médicos para uso humano están regulados por la Directiva 2001/20/CE del Parlamento Europeo y del Consejo, de 4 de abril de 2001 relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros sobre la aplicación de buenas prácticas clínicas en la realización de ensayos clínicos de medicamentos de uso humano (*Directiva de ensayos clínicos*).[310] En diciembre de 2012, la Comisión Europea propuso un reglamento para sustituir la Directiva de ensayos clínicos, con el objetivo de hacer que los procedimientos de ensayo sean más uniformes y eficaces.[311]

Existen muchas iniciativas pendientes a escala europea, de carácter legislativo o de otro tipo, relacionadas con los datos personales en el sector sanitario.[312]

308 Grupo 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, de 15 de febrero de 2007.

309 Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, DO 2011 L 88.

310 Directiva 2001/20/CE del Parlamento Europeo y del Consejo, de 4 de abril de 2001, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros sobre la aplicación de buenas prácticas clínicas en la realización de ensayos clínicos de medicamentos de uso humano, DO 2001 L 121.

311 Comisión Europea (2012), Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE, COM(2012) 369 final, Bruselas, de 17 de julio de 2012.

312 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, de 27 de marzo de 2013.

8.4. Tratamiento de datos con fines estadísticos

Puntos clave

- Los datos recopilados con fines estadísticos no pueden utilizarse para otros fines.
- Los datos recopilados de forma legítima para cualquier fin podrán utilizarse posteriormente con fines estadísticos, siempre que la legislación nacional establezca las garantías adecuadas que deberán cumplir los usuarios. A tal efecto, debería preverse una especial anonimización o pseudonimización antes de transmitir los datos a terceros.

En la Directiva de protección de datos, el tratamiento de datos con fines estadísticos se menciona en el contexto de las posibles excepciones a los principios de protección de datos. En el artículo 6, apartado 1, letra b), de la Directiva se especifica que puede dejarse de aplicar el principio de limitación a una finalidad específica a favor de un uso posterior de los datos con fines estadísticos, aunque la legislación nacional deberá establecer también todas las garantías necesarias. El artículo 13, apartado 2, de la Directiva permite que la legislación nacional establezca limitaciones a los derechos de acceso si los datos se van a tratar exclusivamente con fines estadísticos. De nuevo, la legislación nacional deberá establecer las garantías apropiadas. En este contexto, la Directiva de protección de datos establece el requisito específico de que ninguno de los datos adquiridos o creados durante el estudio estadístico podrá ser utilizado para decisiones concretas sobre los interesados.

Aunque los datos que hayan sido recogidos de forma lícita para cualquier fin por un responsable del tratamiento pueden ser reutilizados por dicho responsable para sus propios fines estadísticos (la denominada estadística secundaria), los mismos deberán ser anonimizados o pseudonimizados, dependiendo del contexto, antes de transmitirlos a un tercero con fines estadísticos, excepto si el interesado ha dado su consentimiento o está especialmente previsto por la legislación nacional. Lo anterior deriva del requisito de la existencia de garantías oportunas, según lo establecido en el artículo 6, apartado 1, letra b), de la Directiva de protección de datos.

Los casos más importantes de uso de datos con fines estadísticos son las estadísticas oficiales, realizadas por las oficinas de estadística nacionales y de la UE, que se basan en las legislaciones nacionales y europeas sobre estadística oficial. Según estas legislaciones, los ciudadanos y las empresas están obligados normalmente a comunicar datos a las autoridades estadísticas. Los funcionarios que trabajan en las

oficinas de estadística están vinculados por las obligaciones de secreto profesional que deben observar de forma cuidadosa, ya que resultan fundamentales para el elevado nivel de confianza ciudadana que es necesaria cuando los datos se ponen a disposición de las autoridades de estadística.

El Reglamento (CE) nº 223/2009 relativo a la estadística europea (*Reglamento de la estadística europea*) incluye normas fundamentales para la protección de datos en la estadística oficial y puede considerarse, por tanto, pertinente para las disposiciones sobre la estadística oficial a escala nacional.[313] El Reglamento mantiene el principio de que las operaciones de estadística oficial precisan disponer de una base jurídica que sea lo suficientemente precisa.[314]

> Ejemplo: En el asunto *Huber contra Bundesrepublik Deutschland*,[315] el TJUE consideró que la recopilación y la conservación de datos personales por parte de una autoridad con fines estadísticos no era motivo suficiente por sí mismo para que el tratamiento fuera lícito. También era necesario que la legislación que regulaba el tratamiento de datos personales cumpliera el requisito de necesidad, lo cual no se producía en dicho contexto.

En el contexto del CdE, en 1997 se adoptó la Recomendación sobre datos estadísticos, que abarca la realización de estadísticas tanto en el sector público como en el sector privado.[316] Dicha recomendación introdujo principios que coincidían con las principales normas de la Directiva de protección de datos descritas anteriormente. Se proporcionan normas más detalladas en relación con algunas cuestiones.

313 Reglamento (CE) nº 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) nº 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) nº 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.

314 Este principio se establecerá de forma más detallada el Código de buenas prácticas de las estadísticas europeas de Eurostat, el cual deberá ofrecer, con arreglo a lo dispuesto en el artículo 11 del Reglamento de la estadística europea, orientaciones éticas sobre cómo llevar a cabo las estadísticas oficiales, incluido el uso considerado que debe hacerse de los datos personales; disponible en: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

315 TJUE, asunto C-524/06, *Huber contra Bundesrepublik Deutschland*, de 16 de diciembre de 2008; véase, en particular, el apdo. 68.

316 Consejo de Europa, Comité de Ministros (1997), Recomendación Rec(97)18 a los Estados miembros relativa a la protección de los datos de carácter personal recopilados y tratados con fines estadísticos, de 30 de septiembre de 1997.

Mientras que los datos que han sido recopilados por un responsable del tratamiento con fines estadísticos no pueden ser utilizados para ningún otro fin, los datos que han sido recopilados con fines no estadísticos pueden ponerse a disposición para un uso estadístico posterior. La Recomendación sobre datos estadísticos permite incluso comunicar los datos a terceros si esto se realiza únicamente con fines estadísticos. En dichos casos, las partes deberán acordar y hacer constar por escrito el alcance del uso legítimo posterior para estadística. Dado que lo anterior no puede sustituir el consentimiento del interesado, se presume que existirán las garantías adecuadas adicionales, establecidas en la legislación nacional, para reducir el riesgo de un uso incorrecto de los datos personales, tales como la obligación de anonimizar o pseudonimizar los datos antes de transmitirlos.

Las personas que se dedican profesionalmente a realizar estudios estadísticos deberán quedar vinculadas por el deber de secreto profesional con arreglo a la legislación nacional, como es habitual para las estadísticas oficiales. Lo anterior deberá ampliarse también a los entrevistadores, si han sido contratados para recopilar datos de los interesados o de otras personas.

Si una encuesta estadística que emplea datos personales no está prevista por la ley, los interesados deberán dar su consentimiento al uso de sus datos para que dicha encuesta sea lícita o, al menos, deberán tener la posibilidad de oponerse al tratamiento. Si los datos personales se recopilan con fines estadísticos, entrevistando a personas, deberá informarse de forma clara a dichas personas sobre si proporcionar esos datos es o no obligatorio, con arreglo a la legislación nacional. Los datos sensibles nunca deben ser recopilados de un modo en que pueda identificarse a la persona física, a menos que así lo permita expresamente la legislación nacional.

Si una encuesta estadística no puede realizarse sin datos anónimos, y resulta necesario utilizar datos personales, los datos recopilados a tal efecto deberán anonimizarse tan pronto como sea posible. Los resultados de la encuesta estadística no deberán permitir, al menos, que los interesados sean identificados, excepto si ello no representa un riesgo manifiesto.

Después de finalizar el análisis estadístico, los datos personales podrán tanto suprimirse como hacerse anónimos. En dicho caso, la Recomendación sobre datos estadísticos propone que los datos de identificación se conserven de forma separada al resto de datos personales, lo cual implica, por ejemplo, que los datos deben pseudonimizarse y que tanto la clave de cifrado como la lista con los sinónimos de identificación deberán almacenarse de forma separada a los datos pseudonimizados.

8.5. Datos financieros

Puntos clave

- A pesar de que los datos financieros no son datos sensibles con arreglo al Convenio nº 108 ni a la Directiva de protección de datos, su tratamiento requiere garantías especiales que garanticen la exactitud y la seguridad de los datos.
- Los sistemas de pago electrónico necesitan una protección de datos integrada, la denominada «privacidad por diseño».
- En este ámbito, se plantean problemas específicos en materia de protección de datos derivados de la necesidad de aplicar los mecanismos adecuados de autenticación.

Ejemplo: En el asunto *Michaud contra Francia*,[317] el demandante, un abogado francés, impugnaba su obligación, con arreglo a la legislación francesa, de informar sobre las sospechas relativas a las posibles actividades de blanqueo de capitales por parte de sus clientes. El TEDH observó que exigir a los abogados que proporcionen a las autoridades administrativas información sobre otra persona que ha llegado a su poder a través de intercambios con esa otra persona, constituía una injerencia en el derecho al respeto a su vida privada y correspondencia, con arreglo al artículo 8 del CEDH, puesto que dicho concepto cubre 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. Teniendo en cuenta que los abogados estaban sometidos a la obligación de informar sobre sospechas únicamente en circunstancias muy limitadas, el TEDH declaró que dicha obligación era proporcionada, y concluyó que no había existido una violación del artículo 8.

En la Recomendación Rec(90)19 del CdE de 1990, se desarrolló una aplicación del marco jurídico general de protección de datos, tal como se incluía en el Convenio nº 108, en el contexto de los pagos.[318] Dicha recomendación aclara el alcance de la recopilación y usos lícitos de los datos en el contexto de los pagos, en particular,

317 TEDH, *Michaud contra Francia*, nº 12323/11, de 6 de diciembre de 2012; véanse, asimismo, TEDH, *Niemietz contra Alemania*, nº 13710/88, de 16 de diciembre de 1992, apdo. 29, y TEDH, *Halford contra el Reino Unido*, nº 20605/92, de 25 de junio de 1997, apdo. 42.

318 CdE, Comité de Ministros (1990), Recomendación nº R Rec(90) 19 relativa a la protección de los datos personales utilizados para el pago y otras operaciones conexas, de 13 de septiembre de 1990.

mediante tarjetas de pago. Propone asimismo a los legisladores nacionales normas detalladas sobre los límites de la comunicación de los datos de pagos a terceros, sobre los plazos de conservación de los datos, así como la transparencia, la seguridad de los datos y los flujos transfronterizos de datos y, por último, sobre el control y los recursos. Las soluciones propuestas se corresponden con lo que quedó recogido posteriormente en el marco general de protección de datos de la UE de la Directiva de protección de datos.

Se han elaborado una serie de instrumentos jurídicos que regulan los mercados de instrumentos financieros y las actividades de las entidades de crédito y las empresas de inversión.[319] Otros instrumentos jurídicos ayudan a luchar contra las operaciones con información privilegiada y la manipulación del mercado.[320] Las cuestiones más importantes en estos ámbitos que tienen un impacto sobre la protección de datos son:

- la conservación de los registros sobre transacciones financieras;
- 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;

319 Comisión Europea (2011), Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los mercados de instrumentos financieros, por la que se deroga la Directiva 2004/39/CE del Parlamento Europeo y del Consejo, COM(2011) 656 final, Bruselas, de 20 de octubre de 2011; Comisión Europea (2011), Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los mercados de instrumentos financieros y por el que se modifica el Reglamento [EMIR] relativo a los derivados OTC, las entidades de contrapartida central y los registros de operaciones, COM(2011) 652 final, Bruselas, de 20 de octubre de 2011; Comisión Europea (2011), Propuesta de Directiva del Parlamento Europeo y del Consejo 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, y por la que se modifica la Directiva 2002/87/CE del Parlamento Europeo y del Consejo, relativa a la supervisión adicional de las entidades de crédito, empresas de seguros y empresas de inversión de un conglomerado financiero, COM(2011) 453 final, Bruselas, de 20 de julio de 2011.

320 Comisión Europea (2011), Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las operaciones con información privilegiada y la manipulación del mercado (abuso de mercado), COM(2011) 651 final, Bruselas, de 20 de octubre de 2011; Comisión Europea (2011), Propuesta de Directiva del Parlamento Europeo y del Consejo sobre las sanciones penales aplicables a las operaciones con información privilegiada y la manipulación del mercado, COM(2011) 654 final, Bruselas, de 20 de octubre de 2011.

- 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 (AEVM).

También existen otras cuestiones de estos ámbitos que se abordan de forma específica, que incluyen la recopilación de datos sobre la situación financiera de los interesados[321] o el pago transfronterizo mediante transferencias bancarias, las cuales implican inevitablemente que se produzca la circulación de datos personales.[322]

321 Reglamento (CE) nº 1060/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, sobre las agencias de calificación crediticia, DO 2009 L 302; Comisión Europea, *Propuesta de reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (CE) nº 1060/2009 sobre las agencia de calificación crediticia*, COM(2010) 289 final, Bruselas, de 2 de junio de 2010.

322 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.

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.

EDRi, *An introduction to data protection*, Bruselas, disponible en: www.edri.org/files/paper06_datap.pdf.

Frowein, J. and Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlín, N. P. Engel Verlag.

Grabenwarter, C. and Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Múnich, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. and 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. and Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Amberes, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. and 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. and Brandeis, L. (1890), «The right to privacy», *Harvard Law Review,* Vol. 4, No. 5, pp. 193–220, disponible en: www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. and Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Capítulo 2

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.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, París, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. and Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, 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.

Tinnefeld, M., Buchner, B. and Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Múnich, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office [Oficina del Comisario de Información del Reino Unido] (2012), *Anonymisation: managing data protection risk. Code of practice*, disponible en: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Capítulos 3 a 5

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. and 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*, Saarbrücken, Éditions universitaires européennes.

Dammann, U. and Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (European Union Agency for Fundamental Rights) [Agencia de los Derechos Fundamentales de la Unión Europea] (2010), *Data Protection in the European Union: the role of National Data Protection 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 de conferencia), Viena, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luxemburgo, Oficina de Publicaciones.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office [Oficina del Comisario de Información del Reino Unido], *Privacy Impact Assessment*, disponible en: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

Capítulo 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. and 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.

Capítulo 7

Europol (2012), *Data Protection at Europol*, Luxemburgo, Oficina de Publicaciones, disponible en: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, La Haya, Eurojust.

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime,* Foro ERA, Vol. 13, No. 3, pp. 381–395.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and 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*, Centro del Derecho de las Relaciones Exteriores, Documento de trabajo del CLEER 2013/2,

disponible en: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Capítulo 8

Büllesbach, A., Gijrath, S., Poullet, Y. and Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. and Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. and De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. and 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. and Hamilton, A. (2012), *Data protection law and practice*, Londres, Sweet & Maxwell.

Jurisprudencia

Jurisprudencia seleccionada del Tribunal Europeo de Derechos Humanos

Acceso a los datos personales

Gaskin contra el Reino Unido, nº 10454/83, de 7 de julio de 1989
Godelli contra Italia, nº 33783/09, de 25 de septiembre de 2012
K.H. y otros contra Eslovaquia, nº 32881/04, de 28 de abril de 2009
Leander contra Suecia, nº 9248/81, de 26 de marzo de 1987
Odièvre contra Francia [GS], nº 42326/98, de 13 de febrero de 2003

Ponderación entre la protección de datos y la libertad de expresión

Axel Springer AG contra Alemania [GS], nº 39954/08, de 7 de febrero de 2012
Von Hannover contra Alemania, nº 59320/00, de 24 de junio de 2004
Von Hannover contra Alemania (nº 2) [GS], nos. 40660/08 y 60641/08, de 7 de febrero de 2012

Desafíos de la protección de datos en línea

K.U. contra Finlandia, nº 2872/02, de 2 de diciembre de 2008

Correspondencia

Amann contra Suiza [GS], nº 27798/95, de 16 de febrero de 2000

Bernh Larsen Holding AS y otros contra Noruega, nº 24117/08, de 14 de marzo de 2013
Cemalettin Canli contra Turquía, nº 22427/04, de 18 de noviembre de 2008
Dalea contra Francia, nº 964/07, de 2 de febrero de 2010
Gaskin contra el Reino Unido, nº 10454/83, de 7 de julio de 1989
Haralambie contra Rumanía, nº 21737/03, de 27 de octubre de 2009
Khelili contra Suiza, nº 16188/07, de 18 de octubre de 2011
Leander contra Suecia, nº 9248/81, de 26 de marzo de 1987
Malone contra el Reino Unido, nº 8691/79, de 26 de abril de 1985
McMichael contra el Reino Unido, nº 16424/90, de 24 de febrero de 1995
M.G. contra el Reino Unido, nº 39393/98, de 24 de septiembre de 2002
Rotaru contra Rumanía [GS], nº 28341/95, de 4 de mayo de 2000
S. and Marper contra el Reino Unido, nºs. 30562/04 y 30566/04, de 4 de diciembre de 2008
Shimovolos contra Rusia, nº 30194/09, de 21 de junio de 2011
Turek contra Eslovaquia, nº 57986/00, de 14 de febrero de 2006

Bases de datos sobre antecedentes penales

B.B. contra Francia, nº 5335/06, de 17 de diciembre de 2009
M.M. contra el Reino Unido, nº 24029/07, de 13 de noviembre de 2012

Bases de datos de ADN

S. and Marper contra el Reino Unido, nºs. 30562/04 y 30566/04, de 4 de diciembre de 2008.

Datos de GPS

Uzun contra Alemania, nº 35623/05, de 2 de septiembre de 2010

Datos de salud

Biriuk contra Lituania, nº 23373/03, de 25 de noviembre de 2008
I. contra Finlandia, nº 20511/03, de 17 de julio de 2008
L.L. contra Francia, nº 7508/02, de 10 de octubre de 2006
M.S. contra Suecia, nº 34209/96, de 2 de julio de 2002
Szuluk contra el Reino Unido, nº 36936/05, de 2 de junio de 2009
Z. contra Finlandia, nº 22009/93, de 25 de febrero de 1997

Identidad

Ciubotaru contra Moldavia, nº 27138/04, de 27 de abril de 2010
Godelli contra Italia, nº 33783/09, de 25 de septiembre de 2012
Odièvre contra Francia [GS], nº 42326/98, de 13 de febrero de 2003

Información relacionada con las actividades profesionales

Michaud contra Francia, nº 12323/11, de 6 de diciembre de 2012
Niemietz contra Alemania, nº 13710/88, de 16 de diciembre de 1992

Intercepción de las comunicaciones

Amann contra Suiza [GS], nº 27798/95, de 16 de febrero de 2000
Copland contra el Reino Unido, nº 62617/00, de 3 de abril de 2007
Cotlet contra Rumanía, nº 38565/97, de 3 de junio de 2003
Kruslin contra Francia, nº 11801/85, de 24 de abril de 1990
Lambert contra Francia, nº 23618/94, de 24 de agosto de 1998
Liberty y otros contra el Reino Unido, nº 58243/00, de 1 de julio de 2008
Malone contra el Reino Unido, nº 8691/79, de 26 de abril de 1985
Halford contra el Reino Unido, nº 20605/92, de 25 de junio de 1997
Szuluk contra el Reino Unido, nº 36936/05, de 2 de junio de 2009

Obligaciones para los sujetos de obligaciones (garantes)

B.B. contra Francia, nº 5335/06, de 17 de diciembre de 2009
I. contra Finlandia, nº 20511/03, de 17 de julio de 2008
Mosley contra el Reino Unido, nº 48009/08, de 10 de mayo de 2011

Fotografías

Sciacca contra Italia, nº 50774/99, de 11 de enero de 2005
Von Hannover contra Alemania, nº 59320/00, de 24 de junio de 2004

Derecho al olvido

Segerstedt-Wiberg y otros contra Suecia, nº 62332/00, de 6 de junio de 2006

Derecho de oposición

Leander contra Suecia, nº 9248/81, de 26 de marzo de 1987
Mosley contra el Reino Unido, nº 48009/08, de 10 de mayo de 2011

M.S. contra Suecia, nº 34209/96, de 2 de julio de 2002
Rotaru contra Rumanía [GS], nº 28341/95, de 4 de mayo de 2000

Categorías sensibles de datos

I. contra Finlandia, nº 20511/03, de 17 de julio de 2008
Michaud contra Francia, nº 12323/11, de 6 de diciembre de 2012
S. and Marper contra el Reino Unido, nºs. 30562/04 y 30566/04, de 4 de diciembre de 2008

Supervisión y ejecución (papel de los diferentes actores, incluidas las autoridades de protección de datos)

I. contra Finlandia, nº 20511/03, de 17 de julio de 2008
K.U. contra Finlandia, nº 2872/02, de 2 de diciembre de 2008
Von Hannover contra Alemania, nº 59320/00, de 24 de junio de 2004
Von Hannover contra Alemania (nº 2) [GS], nºs. 40660/08 y 60641/08, de 7 de febrero de 2012

Métodos de vigilancia

Allan contra el Reino Unido, nº 48539/99, de 5 de noviembre de 2002
Association «21 Décembre 1989» y otros contra Rumanía, nºs 33810/07 y 18817/08, de 24 de mayo de 2011
Bykov contra Rusia [GS], nº 4378/02, de 10 de marzo de 2009
Kennedy contra el Reino Unido, nº 26839/05, de 18 de mayo de 2010
Klass y otros contra Alemania, nº 5029/71, de 6 de septiembre de 1978
Rotaru contra Rumanía [GS], nº 28341/95, de 4 de mayo de 2000
Taylor-Sabori contra el Reino Unido, nº 47114/99, de 22 de octubre de 2002
Uzun contra Alemania, nº 35623/05, de 2 de septiembre de 2010
Vetter contra Francia, nº 59842/00, de 31 de mayo de 2005

Videovigilancia

Köpke contra Alemania, nº 420/07, de 5 de octubre de 2010
Peck contra el Reino Unido, nº 44647/98, de 28 de enero 2003

Muestras de voz

P.G. y J.H. contra el Reino Unido, nº 44787/98, de 25 de septiembre de 2001
Wisse contra Francia, nº 71611/01, de 20 de diciembre de 2005

Jurisprudencia seleccionada del Tribunal de Justicia de la Unión Europea

Jurisprudencia relacionada con la Directiva de protección de datos

Asunto C-73/07, *Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy*, de 16 de diciembre de 2008

[Concepto de «actividades periodísticas» en el sentido del artículo 9 de la Directiva de protección de datos]

Asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen*, de 9 de noviembre de 2010

[Proporcionalidad de la obligación legal de publicar datos personales sobre los beneficiarios de ciertos fondos agrícolas de la UE]

Asunto C-101/01, *Bodil Lindqvist*, de 6 de noviembre de 2003

[Legitimidad de la publicación de datos personales en Internet por parte de un particular sobre la vida privada de otros]

Asunto C-131/12, *Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos, Mario Costeja González*, Petición de decisión prejudicial planteada por la *Audiencia Nacional* (España), interpuesta el 9 de marzo de 2012, de 25 de mayo de 2012, pendiente

[Obligaciones de los proveedores de motores de búsqueda de abstenerse de mostrar los datos personales en los resultados de la búsqueda, a petición del interesado]

Asunto C-270/11, *Comisión Europea contra Reino de Suecia*, de 30 de mayo de 2013

[Multa por la no aplicación de una Directiva]

Asunto C-275/06, *Productores de Música de España (Promusicae) contra Telefónica de España SAU*, 29 de enero de 2008

[Obligación de los proveedores de acceso a Internet a divulgar la identidad de los usuarios de los programas de intercambio de archivos denominado «KaZaA» a la asociación de protección de la propiedad intelectual]

Asunto C-288/12, *Comisión Europea contra Hungría*, de 8 de abril de 2014

[Legitimidad de la destitución del supervisor nacional de protección de datos]

Asunto C-291/12, *Michael Schwarz contra Stadt Bochum*, Conclusiones del Abogado General, de 13 de junio de 2013

[Violación del Derecho primario de la UE por el Reglamento (CE) 2252/2004 que establece que las impresiones dactilares deben conservarse en los pasaportes]

Asunto C-360/10, *SABAM contra Netlog N.V.*, de 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]

Asuntos acumulados C-465/00, C-138/01 y C-139/01, *Rechnungshof contra Österreichischer Rundfunk y otros y Neukomm y Lauermann contra Österreichischer Rundfunk*, de 20 de mayo de 2003

[Proporcionalidad de la obligación legal de publicar datos personales sobre los salarios de los empleados de ciertas categorías de las instituciones del sector público]

Asuntos acumulados C-468/10 y C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado*, de 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]

Asunto C-518/07, *Comisión Europea contra la República Federal de Alemania*, de 9 de marzo de 2010

[Independencia de una autoridad nacional de control]

Asunto C-524/06, *Huber contra Bundesrepublik Deutschland*, de 16 de diciembre de 2008.

[Legitimidad de la conservación de datos sobre extranjeros en un registro estadístico]

Asunto C-543/09, *Deutsche Telekom AG contra Bundesrepublik Deutschland*, de 5 de mayo de 2011

[Necesidad de consentimiento renovado]

Asunto C-553/07, *College van burgemeester en wethouders van Rotterdam contra M.E.E. Rijkeboer*, de 7 de mayo de 2009

[Derecho de acceso del interesado]

Asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitling y Otros*, de 8 de abril de 2014
[Violación del Derecho primario de la UE por la Directiva sobre la conservación de datos]

Asunto C-614/10, *Comisión Europea contra República de Austria*, de 16 de octubre de 2012
[Independencia de una autoridad nacional de supervisión]

Jurisprudencia relacionada con el Reglamento de protección de datos de las instituciones de la UE

Asunto C-28/08 P, *Comisión Europea contra The Bavarian Lager Co. Ltd*, de 29 de junio de 2010
[Acceso a los documentos]

Asunto C-41/00 P, *Interporc Im- und Export GmbH contra Comisión de las Comunidades Europeas*, de 6 de marzo de 2003
[Acceso a los documentos]

Asunto F-35/08, *Pachtitis contra Comisión y EPSO*, de 15 de junio de 2010
[Uso de los datos personales en el contexto de empleo de las instituciones de la UE]

Asunto F-46/09, *V contra Parlamento*, de 5 de julio de 2011
[Uso de los datos personales en el contexto de empleo de las instituciones de la UE]

Índice de jurisprudencia

Jurisprudencia del Tribunal de Justicia de la Unión Europea

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado, asuntos acumulados C-468/10 y C-469/10, de 24 de noviembre de 2011 ..... 19, 23, 85, 88, 92, 93, 210

Bodil Lindqvist, asunto C-101/01, de 6 de noviembre de 2003 ..... 37, 38, 47, 50, 54, 102, 141, 143, 209

College van burgemeester en wethouders van Rotterdam contra M.E.E. Rijkeboer, asunto C-553/07, de 7 de mayo de 2009 ..... 113, 119, 210

Comisión Europea contra Hungría, asunto C-288/12, de 8 de abril de 2014 ..... 114, 129, 209

Comisión Europea contra la República Federal de Alemania, asunto C-518/07, de 9 de marzo de 2010 ..... 114, 128, 210

Comisión Europea contra Reino de Suecia, asunto C-270/11, de 30 de mayo de 2013 209

Comisión Europea contra República de Austria, asunto C-614/10, de 16 de octubre de 2012 ..... 114, 129, 211

Comisión Europea contra The Bavarian Lager Co. Ltd, asunto C-28/08 P, de 29 de junio de 2010 ..... 13, 29, 31, 115, 138, 211

Deutsche Telekom AG contra Bundesrepublik Deutschland, asunto C-543/09, de 5 de mayo de 2011 ..... 38, 65, 210

Digital Rights Ireland y Seitlinger y Otros, asuntos acumulados C-293/12 y C-594/12, de 8 de abril 2014 ..... 137, 186, 211

Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos, Mario Costeja González, Petición de decisión prejudicial planteada por la *Audiencia Nacional* (España), interpuesta el 9 de marzo de 2012, asunto C-131/12, de 25 de mayo de 2012, pendiente 209

Huber contra Bundesrepublik Deutschland, asunto C-524/06, de 16 de diciembre de 2008..... 67, 85, 88, 90, 181, 194, 210

Interporc Im- und Export GmbH contra Comisión de las Comunidades Europeas, asunto C-41/00 P, de 6 de marzo de 2003 .....31, 211

M.H. Marshall contra Southampton and South-West Hampshire Area Health Authority, asunto C-152/84, de 26 de febrero de 1986 115

Michael Schwarz contra Stadt Bochum, Conclusiones del Abogado General, asunto C-291/12, de 13 de junio de 2013 210

Pachtitis contra Comisión y EPSO, asunto F-35/08, de 15 de junio de 2010 211

Parlamento Europeo contra Consejo de la UE, asuntos acumulados C-317/04 and C-318/04, de 30 de mayo de 2006..... 153

Productores de Música de España (Promusicae) contra Telefónica de España SAU, asunto C-275/06, 29 de enero de 2008 .....13, 23, 34, 37, 42, 209

Rechnungshof contra Österreichischer Rundfunk y otros y Neukomm y Lauermann contra Österreichischer Rundfunk, asuntos acumulados C-465/00, C-138/01 y C-139/01, de 20 de mayo de 2003..... 88, 210

SABAM contra Netlog N.V., asunto C-360/10, de 16 de febrero de 2012 .....35, 210

Sabine von Colson y Elisabeth Kamann contra Land Nordrhein-Westfalen, asunto C-14/83, de 10 de abril de 1984 ..... 115, 140

Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy, asunto C-73/07, de 16 de diciembre de 2008..... 13, 24, 209

V contra Parlamento Europeo, asunto F-46/09, de 5 de julio de 2011 211

Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen, asuntos acumulados C-92/09 y C-93/09, de 9 de noviembre de 2010 ..... 13, 23, 32, 37, 41, 45, 67, 73, 209

Jurisprudencia del Tribunal Europeo de Derechos Humanos

Allan contra el Reino Unido, nº 48539/99, de 5 de noviembre de 2002 ..... 160, 208
Amann contra Suiza [GS], nº 27798/95, de 16 de febrero de 2000 ..... 39, 42, 45, 69, 70, 205, 207
Ashby Donald y otros contra Francia, nº 36769/08, de 10 de enero de 2013 34
Association «21 Décembre 1989» y otros contra Rumanía, nºs 33810/07 y 18817/08, de 24 de mayo de 2011 208
Association for European Integration and Human Rights y Ekimdzhiev contra Bulgaria, nº 62540/00, de 28 de junio de 2007 70
Avilkina y otros contra Rusia, nº 1585/09 de 6 de junio de 2013 (sentencia no definitiva) 191
Axel Springer AG contra Alemania [GS], nº 39954/08, de 7 de febrero de 2012 ..... 13, 25, 205

B.B. contra Francia, nº 5335/06, de 17 de diciembre de 2009 ..... 157, 159, 206, 207
Bernh Larsen Holding AS y otros contra Noruega, nº 24117/08, de 14 de marzo de 2013 ..... 37, 40, 206
Biriuk contra Lituania, nº 23373/03, de 25 de febrero de 2008 ..... 27, 115, 191, 206
Bykov contra Rusia [GS], nº 4378/02, de 10 de marzo de 2009 208

Cemalettin Canli contra Turquía, nº 22427/04, de 18 de noviembre de 2008 ..... 113, 120, 206
Ciubotaru contra Moldavia, nº 27138/04, de 27 de abril de 2010 ..... 113, 121, 207
Copland contra el Reino Unido, nº 62617/00, de 3 de abril de 2007 ..... 15, 181, 188, 207
Cotlet contra Rumanía, nº 38565/97, de 3 de junio de 2003 207

Dalea contra Francia, nº 964/07, de 2 de febrero de 2010 ..... 120, 158, 174, 206

Gaskin contra el Reino Unido, nº 10454/83, de 7 de julio de 1989 ..... 117, 205, 206
Godelli contra Italia, nº 33783/09, de 25 de septiembre de 2012 ..... 42, 117, 205, 207

Halford contra el Reino Unido, nº 20605/92, de 25 de junio de 1997 ..... 196, 207
Haralambie contra Rumanía, nº 21737/03,
de 27 de octubre de 2009 ..... 68, 81, 206

I. contra Finlandia, nº 20511/03,
de 17 de julio de 2008 ..... 15, 86, 100, 139, 190, 206, 207, 208
Iordachi y otros contra Moldavia, nº 25198/02, de 10 de febrero de 2009 69

K.H. y otros contra Eslovaquia, nº 32881/04,
de 28 de abril de 2009 ..... 68, 82, 117, 190, 205
K.U. contra Finlandia, nº 2872/02,
de 2 de diciembre de 2008 ..... 15, 115, 135, 139, 205, 208
Kennedy contra el Reino Unido, nº 26839/05, de 18 de mayo de 2010 208
Khelili contra Suiza, nº 16188/07, de 18 de octubre de 2011 ..... 67, 71, 206
Klass y otros contra Alemania, nº 5029/71, de
6 de septiembre de 1978 ..... 15, 160, 208
Köpke contra Alemania, nº 420/07, de 5 de octubre de 2010 ..... 46, 135, 208
Kopp contra Suiza, nº 23224/94, de 25 de marzo de 1998 69
Kruslin contra Francia, nº 11801/85, de 24 de abril de 1990 207

L.L. contra Francia, nº 7508/02, de 10 de octubre de 2006 ..... 190, 206
Lambert contra Francia, nº 23618/94, de 24 de agosto de 1998 207
Leander contra Suecia, nº 9248/81, de
26 de marzo de 1987 ..... 15, 67, 71, 72, 117, 124, 159, 205, 206, 207
Liberty y otros contra el Reino Unido, nº 58243/00, de 1 de julio de 2008 ..... 40, 207

M.G. contra el Reino Unido, nº 39393/98, de 24 de septiembre de 2002 206
M.K. contra Francia, nº 19522/09, de 18 de abril de 2013 ..... 121, 159
M.M. contra el Reino Unido, nº 24029/07, de
13 de noviembre de 2012 ..... 80, 159, 206
M.S. contra Suecia, nº 34209/96, de 2 de agosto de 1997 ..... 124, 190, 206, 208
Malone contra el Reino Unido, nº 8691/79,
de 2 de agosto de 1984 ..... 15, 70, 186, 206, 207
McMichael contra el Reino Unido, nº 16424/90, de 24 de febrero de 1995 206
Michaud contra Francia, nº 12323/11,
de 6 de diciembre de 2012 ..... 182, 196, 207, 208
Mosley contra el Reino Unido, nº 48009/08,
de 10 de mayo de 2011 ..... 13, 27, 124, 207
Müller y otros contra Suiza, nº 10737/84, de 24 de mayo de 1988 32

Niemietz contra Alemania, nº 13710/88,
de 16 de diciembre de 1992 ..... 39, 196, 207

Odièvre contra Francia [GS], nº 42326/98,
de 13 de febrero de 2003 ..... 42, 117, 205, 207

P.G. y J.H. contra el Reino Unido, nº 44787/98,
de 25 de septiembre de 2001 ..... 46, 208
Peck contra el Reino Unido, nº 44647/98,
de 28 de enero 2003 ..... 46, 67, 71, 208

Rotaru contra Rumanía [GS], nº 28341/95,
de 4 de mayo de 2000 ..... 39, 67, 70, 121, 206, 208

S. and Marper contra el Reino Unido, nºs. 30562/04 y 30566/04,
de 4 de diciembre de 2008. ..... 15, 80, 157, 159, 206, 208
Sciacca contra Italia, nº 50774/99, de 11 de enero de 2005 ..... 46, 207
Segerstedt-Wiberg y otros contra Suecia, nº 62332/00,
de 6 de junio de 2006 ..... 113, 121, 207
Shimovolos contra Rusia, nº 30194/09, de 21 de junio de 2011 ..... 70, 206
Silver y otros contra el Reino Unido, nºs 5947/72, 6205/73, 7052/75,
7061/75, 7107/75, 7113/75, de 25 de marzo de 1983 70
Szuluk contra el Reino Unido, nº 36936/05, de 2 de junio de 2009 ..... 190, 206, 207

Társaság a Szabadságjogokért contra Hungría, nº 37374/05, de
14 de abril de 2009 ..... 13, 30
Taylor-Sabori contra el Reino Unido, nº 47114/99, de
22 de octubre de 2002 ..... 67, 70, 208
The Sunday Times contra el Reino Unido, nº 6538/74, de 26 de abril de 1979 70
Turek contra Eslovaquia, nº 57986/00, de 14 de febrero de 2006 206

Uzun contra Alemania, nº 35623/05,
de 2 de septiembre de 2010 ..... 15, 45, 206, 208

Vereinigung bildender Künstler contra Austria, nº 68345/01, de
25 de enero de 2007 ..... 13, 33
Vetter contra Francia, nº 59842/00,
de 31 de mayo de 2005 ..... 70, 157, 161, 208

Von Hannover contra Alemania (nº 2) [GS], nºs. 40660/08 y 60641/08, de 7 de febrero de 2012 ..... 23, 26, 205, 208
Von Hannover contra Alemania, nº 59320/00, de 24 de junio de 2004 ..... 46, 205, 207, 208

Wisse contra Francia, nº 71611/01, de 20 de diciembre de 2005 ..... 46, 208

Z. contra Finlandia, nº 22009/93, de 25 de febrero de 1997 ..... 181, 190, 206

Jurisprudencia de los órganos jurisdiccionales nacionales

Tribunal Constitucional Federal de Alemania (*Bundesverfassungsgericht*), 1 BvR 256/08, de 2 de marzo de 2010 186

Tribunal Constitucional de la República Checa (*Ústavní soud České republiky*), nº 94/2011 Rec., de 22 de marzo de 2011 186

Tribunal Constitucional Federal de Rumanía (*Curtea Constituțională a României*), nº 1258, de 8 de octubre de 2009 186

Agencia de los Derechos Fundamentales de la Unión Europea
Consejo de Europa – Tribunal Europeo de Derechos Humanos

Manual de legislación europea en materia de la protección de datos

2014 — 218 pp. — 14,8 × 21 cm

ISBN 978-92-871-9948-5 (CdE)
ISBN 978-92-9239-330-4 (FRA)
doi:10.2811/53770

Más información sobre la Agencia de los Derechos Fundamentales de la Unión Europea está disponible en Internet. Es posible acceder a ella a través de la página web de FRA: fra.europa.eu.

Más información sobre el Consejo de Europa se encuentra disponible en el servidor de internet hub.coe.int.

Más información sobre la jurisprudencia del Tribunal Europeo de Derechos Humanos está disponible en la página web del Tribunal: echr.coe.int. El portal de búsqueda HUDOC proporciona acceso a las sentencias y decisiones en inglés y/o francés, las traducciones a otros idiomas, las notas informativas mensuales de casos, comunicados de prensa y otras informaciones sobre el trabajo del Tribunal.

10.2811/53770 TK-01-13-772-ES-C

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

El rápido desarrollo de las tecnologías de la información y la comunicación subraya la necesidad creciente de contar con una protección de datos personales sólida, un derecho garantizado tanto por los instrumentos de la Unión Europea (UE) como del Consejo de Europa (CdE). Los avances tecnológicos amplían las fronteras de, por ejemplo, la vigilancia, la intercepción de las comunicaciones y el almacenamiento de datos, lo cual plantea enormes desafíos al derecho a la protección de datos como tal. Este manual está diseñado para familiarizar a los profesionales del Derecho, que no están especializados en el ámbito de la protección de datos, con este ámbito de la legislación. El documento ofrece una visión general de los marcos jurídicos aplicables de la UE y del CdE. Incluye explicaciones sobre la jurisprudencia clave, proporcionando resúmenes de las principales sentencias del Tribunal Europeo de Derechos Humanos (TEDH) y del Tribunal de Justicia de la Unión Europea (TJUE). Cuando no existe dicha jurisprudencia, presenta ejemplos prácticos con situaciones hipotéticas. En resumen, este manual tiene por objeto ayudar a garantizar que se cumple el derecho a la protección de datos con vigor y determinación.

AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA
Schwarzenbergplatz 11 - 1040 Viena - Austria
Tel. +43 (1) 580 30-60 - Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

CONSEJO DE EUROPA
TRIBUNAL EUROPEO DE DERECHOS HUMANOS
67075 Estrasburgo Cedex - Francia
Tel. +33 (0) 3 88 41 20 00 - Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Oficina de Publicaciones

ISBN 978-92-871-9948-5 (CdE)
ISBN 978-92-9239-330-4 (FRA)