

Universidad de Cantabria
Facultad de Derecho
Departamento de derecho público



TESIS DOCTORAL

**LOS DERECHOS FUNDAMENTALES
Y LAS NORMAS DE PROTECCIÓN
DE DATOS PERSONALES**
PRÁCTICA EMPRESARIAL Y CIUDADANA

María Montserrat Velasco Nájera

Dirigida por:

Dr. D. Antonio Magdaleno Alegría

Santander, 2017

ÍNDICE

ÍNDICE DE ABREVIATURAS.	11
INTRODUCCIÓN.....	15
CAPITULO PRIMERO. UNA VISIÓN TEMPORAL: ANTECEDENTES DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL	18
1. Intimidad, Privacidad y Derechos.	18
1.1. Una visión temporal.....	22
1.2. La civilización y los datos personales.	28
2. Normas internacionales y europeas.	29
2.1. Del Derecho a la Intimidad al Derecho a la Protección de Datos.	30
2.1.1 La declaración de Thomas Coole, de 1888 en relación al “derecho a no ser moleestado”.	32
2.1.2 La fundamentación de Samuel Warren y Louis Brandeis en 1890 sobre el Derecho a la privacidad.	35
2.1.3 El artículo 12 y el artículo 19 de la Declaración Universal de Derechos Humanos en 1948.	38
2.1.4 El Pacto Internacional de los Derechos Civiles y políticos de 1966.	41
2.1.5 El artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Roma 1950.....	43
2.2. La Informática y el cambio en los sistemas de información a partir de 1960.	44
2.2.1 Resolución 509 de la Asamblea General de Consejo de Europa, sobre Los Derechos Humanos y los nuevos logros científicos y técnicos de 1968.	46
2.2.2 Resolución del Comité de Ministros de 1973, sobre la protección de las personas respecto a los bancos de datos electrónicos en el sector privado.	47
2.2.3 La Resolución del Comité de Ministros de 1974, sobre la protección de las personas respecto a los bancos de datos electrónicos en el sector público.....	48
2.2.4 La regulación en leyes nacionales de los Estados Miembros del entonces Mercado Común Europeo a partir de 1970. Visión general.	49

2.2.5	Resolución del Parlamento Europeo, de 8 de mayo de 1979, sobre la tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática	52
3.	El derecho a la Protección de Datos Personales como Derecho autónomo respecto al Derecho a la intimidad y a la privacidad.	53
3.1.	El Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981.	58
3.2.	La Recomendación de la Comisión Europea 81/679/CEE, de 29 de julio, relativa al Convenio del Consejo de Europa 108 y la recomendación de su firma y ratificación por los Estados miembros.	60
3.3.	La Directiva 95/46/CE, de 24 de octubre, 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.	61
3.4.	El artículo 8.1 de la Carta de Derechos Fundamentales de la Unión Europea, Niza, 7 de diciembre de 2000. El Reconocimiento del Derecho sustantivo, autónomo y fundamental a la Protección de Datos Personales. El Tratado de Lisboa.	67
3.5.	El Supervisor Europeo de Protección de Datos y el Grupo de Trabajo del Artículo 29.	70
4.	Anexo orientativo: las regulaciones europeas en materia de protección de datos	71
4.1.	Reglamentos.	72
4.2.	Directivas.	72
4.3.	Decisiones de la Comisión.	74

CAPÍTULO SEGUNDO. EL FUTURO DE LA PROTECCIÓN A LOS DERECHOS

FUNDAMENTALES A TRAVÉS DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES. ... 78

1.	Los denominados Nuevos Derechos Fundamentales generados por la Sociedad de la Comunicación y el Conocimiento.	78
2.	El nuevo Reglamento Europeo y del Consejo de 27 de abril de 2016 de protección de datos personales.	84
2.1.	El espacio de libertad, seguridad y justicia, ELSJ.	84
2.2.	El Reglamento 2016/679 de protección de datos de la Unión Europea (RGPD)	86

CAPÍTULO TERCERO. LAS NORMATIVAS ESPAÑOLAS DE PROTECCIÓN DE DATOS

PERSONALES..... 89

3.	El artículo 18.4 de la Constitución Española de 1978.	94
3.1.	Naturaleza jurídica del derecho a la protección de datos personales en la CE 1978 ...	94
3.2.	Novedad y avance respecto a su tiempo. La nueva dimensión espacio-temporal de los derechos fundamentales. Sociedad e individuo.	105
3.3.	Consideración del derecho a la protección de datos como Derecho Fundamental de configuración legal. Su contenido esencial.	109
4.	La Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar	112
5.	La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORDAT).	114
6.	La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).....	120
7.	La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre: Independencia y autonomía del Derecho Fundamental a la Protección de Datos personales respecto al Derecho a la Intimidad.....	124
7.1.	El poder de disposición y de Control del individuo sobre sus datos personales.	128
7.2.	La obligación de hacer y la obligación de no hacer con carácter previo a cualquier relación.	132

CAPÍTULO CUARTO. LA PROTECCIÓN DE DATOS PERSONALES COMO GARANTÍA DE

OTROS DERECHOS 138

1.	Algunas Ideas previas. Los cambios tecnológicos de la última década (2007-2017)	138
1.1.	El clouding (nube) o almacenamiento y tratamiento de datos en grandes servidores interconectados por una red de comunicaciones.	140
1.2.	El big data, o tratamiento masivo de datos.....	143
1.3.	El internet de las cosas o internet of things (abreviado IoT).....	145
2.	El objeto de regulación en la protección de datos personales.	146
2.1.	El artículo 1 LOPD	146

2.2.	El objeto del nuevo Reglamento Europeo 2016/679 de protección de datos personales (RGPD).	153
3.	Ámbito de aplicación.	154
3.1.	La regulación establecida en la LOPD de 1999 y su Reglamento de 2007	155
3.1.1	El concepto de territorialidad.....	155
3.1.2	El concepto de aplicación subjetiva.	156
3.1.3	El concepto de aplicación objetiva.....	157
3.2.	Las cuestiones que planteaba la regla general sobre el ámbito de aplicación de la LOPD.....	158
3.3.	Ámbito de aplicación del nuevo RGPD.	163
4.	La realidad sin regulación: las Transferencias Internacionales de Datos personales	164
4.1.	Las conexiones en cloud computing o en nube según la AEPD.	165
4.2.	Deberes del responsable de tratamiento de datos en nube.	168
4.3.	El movimiento internacional de Datos de Carácter Personal.....	170
4.3.1	La Sentencia de puerto seguro en EEUU del Tribunal de Justicia de la Unión Europea (TJUE) de 6 de octubre de 2015.....	174
4.3.2	La desprotección jurídica del ciudadano ante las TID.....	182
4.4.	Las normas europeas que establece el nuevo RGPD para las TID.....	196
4.4.1	Las excepciones a la norma general de las TID.....	200
4.4.2	La cooperación internacional en el ámbito del derecho a la protección de datos personales.	201
4.4.3	Las normas corporativas vinculantes.....	203
4.4.4	Las Autoridades de control independientes.....	206
5.	Las múltiples excepciones a la aplicación de la Ley de Protección de datos personales.	207
5.1.	La denominada excepción doméstica de tratamiento de datos personales.	207
5.2.	Las excepciones sobre materias clasificadas.	218
5.2.1	Las materias clasificadas.....	220
5.2.2	El terrorismo y la delincuencia organizada.	227
5.2.3	La Directiva 2016/680, relativa a la protección de las personas físicas en relación al tratamiento de datos personales para prevención de infracciones penales.	231
5.3.	Otras exclusiones.....	233

6.	Las Definiciones y conceptos aclaratorios en la LOPD y en el RGPD.	
	Controversia entre teoría y práctica.	233
6.1.	Definición de dato personal.	234
6.2.	Definición de Fichero.	242
6.3.	Definición de fuente accesible al público.	246
6.3.1	Los datos personales accesibles al público no por ello están exentos de protección.	248
6.3.2	La accesibilidad general no es sinónimo de fuente accesible al público.	249
6.3.3	Las fuentes de datos personales accesibles al público.	250
A.	El censo promocional.	251
B.	Las listas de profesionales.	252
C.	Los repertorios telefónicos y las Guías de servicios de comunicaciones electrónicas.	253
7.	Los Principios (que son derechos y obligaciones en la práctica) de la Protección de Datos de Carácter Personal.	254
7.1.	La calidad de los Datos.	256
7.1.1	La pertinencia del tratamiento.	257
7.1.2	El deber de actualización y rectificación.	258
7.1.3	La cancelación de datos.	261
7.1.4	Recogida de datos por medios fraudulentos, desleales e ilícitos.	261
7.2.	El derecho a ser informado.	262
7.3.	El Consentimiento del Afectado.	268
7.3.1	Excepciones a la obligación de recabación del consentimiento.	270
7.3.2	Supuestos de habilitación para el tratamiento y cesión sin consentimiento	270
7.3.3	Supuestos de tratamiento y cesión sin consentimiento.	271
7.3.4	El derecho de oposición.	272
7.4.	El consentimiento de los menores de edad	276
7.5.	La práctica empresarial frente a los principios de la protección de datos.	280
8.	La vertiente más conflictiva: los Datos especialmente protegidos. El artículo 16 de la Constitución. Derechos fundamentales y realidad.	282
8.1.	La ponderación como sistema de solución de conflictos entre DDFF	290
8.2.	La proporcionalidad, la idoneidad y la intervención mínima como principios para el ejercicio de otros derechos y libertades frente a la protección de datos personales.	301

8.3.	La protección de datos y otros DDFF, en referencia a los datos especialmente protegidos del artículo 16 CE.....	306
8.3.1	Los libros bautismales y la protección de datos.....	307
8.3.2	La videovigilancia, los sistemas de grabación y visualización de imágenes.	315
A.	Los Servicios de videovigilancia y la seguridad privada.	318
B.	La videovigilancia en el entorno laboral. La Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo de 2016.	324
C.	El uso de dispositivos de videograbación volantes o drones.....	331
D.	La biometría.....	333
8.3.3	La información personal que se publica en los medios de comunicación.	336
A.	El derecho a la protección de datos y su relación con el derecho a la libertad de expresión e información.....	338
A.1	La libertad de expresión e información de los usuarios anónimos en las redes sociales y otros medios de comunicación.	345
A.2	La libertad de expresión e información a través de los medios profesionales de comunicación.	352
B.	La fuerte controversia y las consecuencias negativas de la publicación de información personal en prensa y en Boletines Oficiales.	367
C.	Las repercusiones de la reciente Sentencia Google. El denominado derecho al olvido (Derecho de supresión, artículo 17 RGPD).	370
D.	El Derecho de supresión de información personal en internet y reinserción social.	376
8.3.4	La libertad sindical y la protección de datos.	378
8.3.5	Intimidad, honor y protección de datos.	383
8.3.6	Datos relativos a la salud.	386
9.	La Seguridad de los Datos.	399
9.1.	La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: el método MAGERIT.	404
9.2.	El Instituto Nacional de Ciberseguridad, INCIBE.....	409
9.3.	Anexo orientativo: Aplicación de los niveles de seguridad.	411
10.	El Deber de Secreto.....	418
11.	La Cesión de Datos: Comunicación de Datos personales con consentimiento previo del Interesado.....	420
12.	El control de Acceso a los Datos Personales por cuenta de Terceros.	426

13. Los Derechos de las Personas en la LOPD.	428
13.1. Derecho a la Impugnación de valoraciones respecto a la personalidad del afectado.	429
13.1.1 La conducta penitenciaria.	434
13.1.2 Las valoraciones de las entidades de crédito y solvencia patrimonial.....	436
13.2. Derecho de Consulta Gratuita al Registro General de Protección de Datos.	437
13.3. Derecho de Acceso a los Datos Personales propios del interesado.	439
13.4. Derecho de Rectificación y Cancelación.....	442
13.5. La Agencia Española de Protección de Datos, como Control y Garantía para el ejercicio de los Derechos de las Personas.....	444
13.6. Derecho a Indemnización y Responsabilidad del Titular del Fichero.	446
13.6.1 La inclusión de una persona física en un fichero de solvencia.	448
13.6.2 El daño o lesión sobre la vulneración del derecho a la protección de datos personales.	449
14. Los derechos de las personas en el nuevo Reglamento de protección de datos de la Unión Europea (RGPD) desde la perspectiva del consentimiento.	451
14.1. El consentimiento informado.....	453
14.2. Los derechos de supresión y limitación del tratamiento,.....	454
14.3. El derecho a la portabilidad de los datos	455
14.4. El derecho de oposición a la elaboración de perfiles personales.....	455
15. Las obligaciones del responsable del tratamiento de datos personales en el nuevo RGPD desde la perspectiva tecnológica.	457
15.1. El Representante del responsable del tratamiento que no tenga establecimiento en la UE.	458
15.2. Infracciones y sanciones	459
15.3. El Delegado de protección de datos (Data Protection Officer, DPO)	459
15.4. La anonimización y la seudonimización.	462
15.5. Principio o norma de neutralidad tecnológica.....	467
15.6. Principio de privacidad desde el diseño y por defecto.....	468
15.7. Principio de transparencia.	470
15.8. Obligación de evaluación del impacto de las tecnológicas empleadas en el tratamiento de datos.	472

CAPÍTULO QUINTO. SOLUCIONES GLOBALES A PROBLEMAS GLOBALES. AUTORREGULACIÓN EMPRESARIAL Y CERTIFICACIÓN DE TITULARES DE DATOS PERSONALES, UN OBJETIVO MUNDIAL.	476
1. Algunas ideas previas sobre conceptos utilizados en la práctica.....	478
1.1. La autorregulación.	478
1.1.1 La autorregulación en los antecedentes de la normativa sobre protección de datos.	480
1.1.2 La autorregulación en las relaciones internacionales empresariales.	483
1.2. Los códigos de conducta o códigos tipo.	488
1.3. La certificación para empresas.	491
1.4. La identidad electrónica: la certificación, la firma digital, el certificado electrónico y el Documento Nacional de identidad electrónico (DNle).	494
2. La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).....	497
3. La autorregulación y las empresas.....	505
3.1. La autorregulación como oportunidad y como riesgo.	509
3.2. La certificación de los ciudadanos. El control de la información personal.	517
3.3. Realidades de autorregulación en sectores empresariales.	521
3.3.1 Autocontrol para las empresas de publicidad.	523
3.3.2 Autorregulación para empresas con actividades en Internet.....	525
A. Especial referencia a las redes sociales	527
B. Especial referencia a las grandes corporaciones de venta y alquiler de bienes y servicios.	532
C. Especial referencia a las entidades de crédito y financieras.....	533
3.3.3 Autorregulación para los medios de comunicación audiovisual.....	534
3.3.4 Autorregulación para los sectores relacionados con la salud, ...	539
3.4. La Autoridad de control de protección de datos y la norma autorregulada.	540
3.5. Anexo orientativo: la visión de la protección de datos en las certificaciones de seguridad.	546
CONCLUSIONES Y PROPUESTAS.	552
BIBLIOGRAFÍA	565

ANEXO A BIBLIOGRAFÍA. SITIOS WEB DE INTERÉS.....	598
SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL.	604
SENTENCIAS DEL TRIBUNAL SUPREMO.	606

Los Derechos Fundamentales y las normas de protección de datos personales.
Práctica empresarial y ciudadana.

Dña. María Montserrat Velasco Nájera

Dirigida por: Dr. D. Antonio Magdaleno Alegría, Profesor de la Universidad de Cantabria.

ÍNDICE DE ABREVIATURAS.

AAPP	Administraciones Públicas.
ADSL	Técnica de codificación de la señal para su transmisión por redes de telecomunicaciones.
AEAP	Asociación Española de Agencias de Publicidad.
AEAT	Agencia Estatal de Administración Tributaria.
AECE	Asociación Española de Comercio Electrónico.
AEPD	Agencia Española de Protección de Datos.
AN	Audiencia Nacional.
ATC	Auto del Tribunal Constitucional.
ATS	Auto del Tribunal Supremo.
BCR	Binding Corporate Rules. Normas Corporativas Vinculantes.
BOE	Boletín Oficial del Estado.
CC	Código Civil.
CCAA	Comunidades Autónomas.
CE	Constitución Española.
CEPD	Consejo Europeo de Protección de Datos.
CP	Código Penal.
DCCE	Derecho Constitucional Común Europeo.
DDFF	Derechos Fundamentales.
DDHH	Derechos Humanos.
DNI	Documento Nacional de Identidad.

DPO	Data Protection Officer Delegado de protección de datos.
EEE	Espacio Económico Europeo.
EEUU	Estados Unidos de Norteamérica.
ELSJ	Espacio de Libertad, Seguridad y Justicia.
FJ	Fundamento Jurídico de una Sentencia mencionada.
FIES	Fichero de Internos de Especial Seguimiento.
GPS	Sistema de Posicionamiento Global.
GT29	Grupo de trabajo del artículo 29 de la Directiva 95/46
INE	Instituto Nacional de Estadística.
INSALUD	Instituto Nacional de la Salud.
INSS	Instituto Nacional de la Seguridad Social.
INTERPOL	Organización Internacional de Policía Criminal.
IoT	Internet de las Cosas.
IP	Internet Protocol: Protocolo de transmisión de información por Internet.
ITU	International Telecommunication Union; Unión Internacional de Telecomunicaciones (UIT).
ISO	International Organization for Standardization.
LCAP	Ley de Contratos de las Administraciones Públicas.
LOLS	Ley Orgánica de Libertad Sindical.
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.
LRAP	Ley 41/2002 de 14 de noviembre, básica reguladora de la autonomía del

paciente

LSP	Ley de Seguridad Privada.
LSSI	Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
NIF	Número de Identificación Fiscal.
OCDE	Organización para la Cooperación y el Desarrollo Económico.
OMS	Organización Mundial de la Salud.
ONU	Organización de Naciones Unidas.
RAE	Real Academia de la Lengua Española.
RAI	Registro de Aceptaciones Impagadas.
RGPD	Reglamento de la Unión Europea en referencia al REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, también denominado como Reglamento General de Protección de Datos.
SAN	Sentencia de la Audiencia Nacional.
SIS	Sistema de Información Schengen.
SMS	Protocolo para el servicio de envío de mensajes cortos.
STC	Sentencia del Tribunal Constitucional.
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos.
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea.
STS	Sentencia del Tribunal Supremo.
SEPD	Supervisor Europeo de Protección de Datos.
TC	Tribunal Constitucional.
TEDH	Tribunal Europeo de Derechos Humanos.

TID	Transferencia(s) Internacional(es) de datos.
TJCE	Tribunal de Justicia de las Comunidades Europeas.
TS	Tribunal Supremo.
TSJ	Tribunal Superior de Justicia.
TUE	Tratado de la Unión Europea.
UE	Unión Europea.

INTRODUCCIÓN

El estudio del derecho fundamental a la protección de datos personales continúa siendo novedoso como consecuencia de los incesantes avances y las nuevas posibilidades que facilitan las tecnologías de la información y la comunicación. Lógicamente los aludidos cambios tecnológicos generan la necesidad de adecuar las normas de protección de datos. De hecho, el presente estudio se ha realizado entre la vigencia de la LOPD y la aprobación del nuevo Reglamento Europeo de Protección de datos personales. Posiblemente, entre la conclusión del presente trabajo y su defensa pública se producirán nuevos acontecimientos que impliquen la necesidad de su estudio.

La protección de datos personales es una cuestión multidisciplinar donde no sólo intervienen normas jurídicas, sino también las técnicas de tratamiento de datos personales, en las que las tecnologías de la comunicación e información juegan un papel decisivo. Los sistemas normativos prestan atención a la defensa del derecho fundamental a la protección de datos personales como consecuencia de las potencialidades que implica la posibilidad del tratamiento masivo de datos.

Todo avance tecnológico está en consonancia con el desarrollo de la humanidad. Sin el progreso de los ciudadanos, como individuos, y sin la evolución social, como grupo, no existiría la civilización. La tecnología, en cualquier caso, está acompañada de elementos humanos indispensables para su extensión en el entorno social. La evolución de la Teoría de los Derechos Fundamentales, como consecuencia del desarrollo de las tecnologías de la información y las comunicaciones, se convierte en un resultado de las propias acciones de los ciudadanos. En el escenario internacional se manifiesta la necesidad de una nueva regulación que tenga en cuenta los riesgos y los derechos de las personas, no sólo las ventajas plausibles de la situación actual. La evolución permanente de los sistemas de comunicación e información también implica la necesidad de articular nuevas formas de protección de los derechos de la personalidad, entre los que destacan los derechos a la intimidad, al honor y la propia imagen, cuya colisión con las libertades de expresión e información se enfrenta en este momento a situaciones diversas, que requieren de soluciones normativas eficaces. Como

afirmó la STC 53/1985, de 11 de abril, los derechos fundamentales no incluyen solamente “derechos subjetivos de defensa de los individuos frente al Estado, y garantías institucionales, sino también deberes positivos por parte de éste”. Los derechos fundamentales son los componentes estructurales básicos, “tanto del conjunto del orden jurídico objetivo como de cada una de las ramas que lo integran, en razón de que son la expresión jurídica de un sistema de valores que, por decisión del constituyente, ha de informar el conjunto de la organización jurídica y política”. A través del sometimiento de todos los poderes a la Constitución, no solamente se infiere *la obligación negativa* del Estado de no lesionar la esfera individual o institucional protegida por los DDFF, sino también la *obligación positiva* de contribuir a la efectividad de tales derechos y de los valores que representan, aun cuando el ciudadano no promueva una pretensión subjetiva. El legislador recibe de los derechos fundamentales los impulsos y líneas directivas, e incumpliría su obligación (como legislador) si no estableciera las directrices para su defensa y su eficacia, dejando al derecho (o valor fundamental) vacío de contenido, lo que equivale a su inutilidad social e individual, incumpliendo el mandato constitucional consagrado en el artículo 9.2 CE.

Desde el artículo 18.4 CE de 1978 hasta el nuevo Reglamento Europeo de Protección de datos Personales de 2016 han sucedido cambios sustanciales que afectan al derecho fundamental a la protección de datos. El presente estudio muestra esa línea temporal analizando a los autores que fueron pioneros en el estudio de la Ley Orgánica de Protección de Datos de Carácter Personal de 1999 (LOPD) y su Reglamento de desarrollo de 2007. A la citada normativa están obligadas tanto las Administraciones Públicas como los operadores privados, entre los que cabe destacar las empresas, asociaciones y organizaciones de todo tipo. Se trata de los *responsables de ficheros o tratamientos*. La presente exposición se centra en la actuación de los operadores privados y la repercusión en los ciudadanos de la eficacia de su actuación y protección utilizando como elementos de análisis la CE y jurisprudencia del TC, la normativa nacional e internacional de protección de datos, así como los pronunciamientos de los tribunales internos e internacionales, sin olvidar los pronunciamientos de la Agencia española de protección de datos.

Desde otro punto de vista, el análisis se fundamenta en los fuertes vínculos existentes entre la conducta de los ciudadanos, los DDFF, la sociedad de la información, el comercio electrónico y el desarrollo empresarial a nivel global. Todo ello ha transformado profundamente la realidad social. La actual situación presenta diferentes aspectos cuestionables: ¿los medios empleados son suficientes para la protección efectiva de los datos personales?, ¿los obligados al cumplimiento de la norma (en especial los responsables de las empresas y los profesionales autónomos) comprenden su transcendencia y significado?, ¿cuentan éstos con suficiente orientación y facilidades para la ejecución de sus obligaciones, tal y como sucede en el Derecho Tributario, donde el Estado provee de formularios y documentación, no expuesta a interpretación?

Como se tratará de demostrar a lo largo del presente estudio, el futuro de la protección de datos, como base para la protección de otros derechos fundamentales, debe descansar sobre dos conceptos ligados a la práctica en protección de datos. En primer lugar, se debe optar por la *autorregulación*, esto es, por normas voluntariamente asumidas por los responsables y encargados del tratamiento de datos. En segundo lugar, por la autoprotección de los titulares de los datos, los distintos agentes implicados en la protección de datos (especialmente los poderes públicos) deben favorecer una mejor y mayor cultura sobre los derechos fundamentales, en especial referencia al derecho fundamental a la protección de datos personales. En ambos casos, la utilización de herramientas ya existentes, como las certificaciones de personalidad o los documentos de identidad electrónicos (DNle), no contradicen la libertad del individuo, muy al contrario, lo protegen frente a usos indebidos.

Se desconoce si la LOPD será revisada. A principios de 2017 sigue en vigor (con algunas matizaciones lógicas). En el presente texto se expone el reto que supondrá el nuevo Reglamento Europeo de Protección de Datos personales, con la intención de analizar su contenido y formular algunas propuestas de *lege ferenda*.

CAPITULO PRIMERO. UNA VISIÓN TEMPORAL: ANTECEDENTES DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Desarrollando una línea de análisis temporal, se abordaron los conceptos de intimidad, privacidad y protección de datos, con el antecedente de los Estados Unidos de América, pero centrando la atención en la normativa internacional y europea.

1. Intimidad, Privacidad y Derechos.

Con carácter previo al estudio del derecho a la protección de los datos de carácter personal, se considera de interés esbozar unos breves apuntes sobre los conceptos de intimidad y privacidad, pues los mismos han tenido una gran influencia en su construcción conceptual¹.

Aunque el presente estudio se realizará desde una perspectiva jurídica, se iniciará con algunas consideraciones sobre la evolución del pensamiento en las ideas de intimidad y privacidad, conceptos que, si bien suelen ser empleados como sinónimos, en realidad tienen claras diferencias en su desarrollo. Se abordará la intimidad como Derecho, pero eso no obvia para que en algunos momentos se argumente con ideas no propiamente jurídicas (filosóficas o sociales) o con hechos y fenómenos que se han producido o se producen en la actualidad. El mundo interior de un ser humano puede no tener trascendencia jurídica. Sólo si la intimidad es perturbada o se desea excluir del conocimiento de los demás, se podría inducir un derecho a la intimidad, pues como ámbito interior y secreto no es conocido por el derecho. La relevancia jurídica de la intimidad se explica en su incidencia sobre el desarrollo de la personalidad individual y social; de lógica se deduce que, si una persona quiere o necesita su vida íntima, no tiene porqué desplazarse a un lugar aislado, sino que basta con el respeto so-

¹ En todo el texto se hablará de protección de datos de carácter personal cuando se hable de protección de datos, salvo que se aclare la expresión debido a la exposición de conceptos.

cial en el marco jurídico a su aislamiento momentáneo o reservado a determinados aspectos personales, que no signifiquen su exclusión social².

El Derecho a la Intimidad es un Derecho Fundamental con fuerte vinculación con la Libertad de la Persona y con su dignidad. Remontando en la Historia, todas las sociedades trataron la intimidad como un ámbito personal que no se comparte con los demás. En la definición de la Real Academia de la Lengua Española, íntimo es lo más interior e interno, y la intimidad se define como la zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia. La privacidad se define como el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión. Lo privado se define como lo que se ejecuta a la vista de pocos, familiar y domésticamente, sin formalidad ni ceremonia alguna, particular y personal de cada individuo o que no es de propiedad pública o estatal, sino que pertenece a particulares³. La palabra intimidad tiene su origen en la voz latina *intimus*: zona espiritual y reservada de una persona, así como de un grupo o una familia. También se define por la soledad de la persona consigo misma, que puede ser interpretado como un derecho a la soledad. Sólo los seres humanos racionales tienen percepción de la intimidad, al tener conciencia y realizar acciones⁴. La intimidad personal confiere también un *derecho al secreto*, que ciertos aspectos de los seres humanos no sean conocidos, que otros no sepan cómo somos, qué sentimos, qué hacemos. Según SERRANO ALONSO, *el ser humano es el centro y razón de ser del Derecho, ya que éste trata de regular las diversas situaciones en que la persona puede encontrarse en su vida en sociedad*⁵. El Derecho civil regula especialmente las relaciones privadas del individuo, y dentro del derecho civil, la parte que estudia la situación de la persona se denomina Derecho de la persona. En el ámbito del Derecho Privado español destaca la definición del profesor ALBADALEJO el cual entendió que “*La intimidad es el poder concedido a la perso-*

² DE DOMINGO, T., *¿Conflictos entre derechos fundamentales?*, Madrid, 2001, pág. 273 y ss..

³ Diccionario de la Real Academia Española en su edición on-line. REAL ACADEMIA ESPAÑOLA, ., *Diccionario de la Real Academia Española*, España, 2012.

⁴ GARCÍA SAN MIGUEL, L., *Estudios sobre el derecho a la intimidad*, Madrid, 1992, pág. 15-35.

⁵ SERRANO ALONSO, E., *Derecho de la persona*, Madrid, 1992, pág. 5.

na sobre el conjunto de actividades que forman parte de su círculo íntimo, personal y familiar, poder que le permite excluir a los extraños de entrometerse en él y de darle una publicidad que no desee el interesado"⁶. En esta definición de intimidad se pueden diferenciar dos aspectos, uno que trata de excluir a los demás, la propia persona no quiere dar información sobre sí misma; otro aspecto es *el control de la persona sobre su propia información*⁷.

Lo privado y lo íntimo se oponen a lo público en el Derecho, no se tiene porqué argumentar en exceso que la diferencia entre intimidad y privacidad existe, aunque en muchas ocasiones (y en muchas traducciones) se consideran sinónimos. La privacidad se debe a elementos contemporáneos evolucionados históricamente. La intimidad va unida al ser humano, a su esencia y a su libertad. La intimidad como Derecho se mantiene en una evolución histórica, pues se otorga a la intimidad una protección acorde con la civilización correspondiente y con los instrumentos jurídicos de los que se disponía en ese momento. En cualquier caso, el concepto de intimidad es controvertido, adolece de imprecisión y es difícilmente definible con unanimidad doctrinal, la cual se presenta generalmente como ambigua, general y poco rigurosa para resolver los problemas que atentan contra el derecho a la intimidad personal. Muy probablemente por esa denominada "*tricotomía de lo íntimo, privado y público*", sin delimitación conceptual clara, las tecnologías de la información del siglo XX no encontrarían cómo limitarse ante el derecho a la intimidad o ante la privacidad del individuo⁸. La doctrina continuó formando definiciones a la intimidad, como la reseñada por SABATER,

⁶ ALBADALEJO, M., *Derecho Civil I*, Madrid, 2002, pág. 494-495.

⁷ RÚIZ MIGUEL, C., *La configuración Constitucional del Derecho a la Intimidad*, Madrid, 1995.

⁸ Véase LUCENA CID, ISABEL VÍCTORIA; "El concepto de la intimidad en los nuevos contextos tecnológicos", *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*. , Valencia, 2014, pág. 26 y ss. , en especial comenta la autora las ideas de GARZÓN VALDES, PROSSE Y FROSSINI, entre otros. Véase también la posición de PÉREZ LUÑO, A., "La protección de los datos personales de carácter sanitario", *Derechos Humanos y protección de datos personales en el siglo XXI*, , 2013, pág. 118. El autor considera que el denominado *Ius solitudinis* tendría raíces filosóficas, pero para el derecho sólo tiene transcendencia jurídica cuando se convierte en un problema del individuo frente a la sociedad.

como “Derecho complejo que comprende y se vincula a su vez con varios derechos específicos que tienden a evitar intromisiones extrañas en áreas reservadas del ser humano”, como son el derecho a la inviolabilidad del domicilio, a la inviolabilidad de la correspondencia y de las comunicaciones privadas, a la propia imagen, al honor, a la privacidad informática, a no participar en la vida colectiva y aislarse voluntariamente, no siendo molestado. Se relaciona a su vez con “el derecho a no exteriorizar los pensamientos o las ideas, como parte de la libertad de expresión, la libertad religiosa o de creencias, la libertad de procreación y de preferencias sexuales, las libertades políticas y los derechos de carácter familiar”⁹. El Derecho debe adaptar sus estructuras y sus conceptos a la nueva realidad tecnológica.

⁹ Cita de CORDERO CUTILLAS, I., “Redefiniendo los derechos de la personalidad en el siglo XXI”, *Los derechos a la intimidad y a la privacidad en el siglo XXI*, , 2014, pág. 30. Cita el autor, además, el caso del Tribunal Supremo de EEUU *Griswold vs. Connecticut* de 1965. El Tribunal reconoció que estaban tratando en ese momento con un “derecho a la intimidad no menos importante que cualquier otro derecho cuidadosa y particularmente reservado a la gente” (...) “más antiguo que la Declaración de Derechos, más antiguo que nuestros partidos políticos y que nuestro sistema escolar” Los autores remarcaban que “los jueces no son legisladores” pues carecen de legitimación “científica o democrática para adoptar decisiones autónomas como si fuera un legislador” cita de CODERCH, junto con otros comentarios de ALBADALEJO, DÍAZ ALABART Y DE OTTO. Por este último, se reduciría la libertad de interpretación del juez, pues lo consideró un atentado contra los principios básicos del sistema, lesionando la seguridad jurídica por su imprevisibilidad, el principio de igualdad ante casos iguales con resoluciones diversas de diferentes jueces y la unidad del derecho en cuanto a jurisdicción única. En otra vertiente de la doctrina, los autores destacaron la gran labor de los Tribunales al completar la legislación y generando nuevas categorías de derechos adaptados a la realidad social, en especial, ponderando los derechos de libertad de expresión e información frente a los derechos de la personalidad, como es la intimidad y la propia imagen, sometidos a tratamientos incesantes por las tecnologías de la comunicación y la información. Véase recientemente la STS 1440/2013, de 18 de febrero, siguiendo los fundamentos jurídicos de la SAPM 627/2009, de 22 de marzo de 2011, interpretó que el derecho a la intimidad “tiene por objeto reservar al individuo un ámbito de su vida, vinculado con el respeto de su dignidad como persona (artículo 10.1 CE), frente a la acción y el conocimiento de los demás, sean estos poderes públicos o simples particulares. De suerte que el derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado, no sólo personal sino también familiar, frente a la divulgación del mismo por terceros y una publicidad no querida. No garantiza una intimidad determinada, sino el derecho a po-

1.1. Una visión temporal

En la sociedad primitiva el individuo se encontró determinado por su entorno, llevando una vida de costumbres, sumido en el grupo, sin que su libertad o la protección de la misma tuvieran relevancia. La *polis griega* no dio un valor determinado a la vida personal, debido a su idea de Estado y a la enorme dimensión de lo social¹⁰. La persona en la *polis griega* no fue tanto individuo con un *yo*, sino un *prosopon* o máscara del comediante. El griego fue ante todo un ser social, sujeto de todo tipo de críticas, sin autoconciencia. En la obra de ARISTÓTELES, *La Política*, el clásico autor consideró absurdo no organizar la natalidad de la ciudad, también sugirió al legislador regular los matrimonios, añadiendo comentarios sobre los hijos que se deben abandonar y a los que hay que mantener; señaló que no se debería criar a ningún niño defectuoso, como ejemplos de su visión. Si un filósofo como Aristóteles se planteó en aquella época estas posibilidades, considerándolas *deseables*, se puede llegar a la conclusión de que existía una perfecta ausencia o al menos deficiencia de intimidad personal. En cuestiones educativas, Aristóteles se mostró afín a las prácticas espartanas, en contra de la costumbre ateniense de que los padres eduquen a sus hijos libremente, pues la educación debería ser la misma para todos los ciudadanos; entonces, cada individuo enseñaba a sus hijos con su instrucción personal. Todo ello basado en el pensamiento aristotélico de que ningún ciudadano de la *Polis* se pertenecía a sí mismo, sino que

seerla, disponiendo a este fin de un poder jurídico sobre la publicidad de la información relativa al círculo reservado de su persona y familia, que se desea mantener al abrigo del conocimiento público. Lo que el artículo 18.1 de la CE garantiza, es, pues, el secreto sobre nuestra propia esfera de vida personal y, por tanto, veda que sean los terceros, particulares o poderes públicos, quienes decidan cuales son los contornos de nuestra vida privada”.

¹⁰ ORTEGA Y GASSET, J., *El Espectador*, Madrid, 2007.

todos pertenecían a la ciudad, al ser una parte de ella. La *Polis* era suficiente como para generar felicidad a sus ciudadanos¹¹.

En Roma no se sostuvo una idea muy alejada de la griega. MONTESQUIEU recuerda que en Roma se consideraba delito el adulterio o se regulaba las edades de matrimonio en cuanto a su propósito de renovación demográfica (nacimiento de hijos). Lo íntimo estaba subordinado a lo público en aspectos que ahora se considerarían intolerables¹².

Con el cristianismo se desarrolló una idea de espiritualidad basada en la autonomía del individuo y, por tanto, en la libertad de la persona. Esas ideas llevaron a la concepción de la intimidad y las libertades individuales actuales, a través de autores como SAN AGUSTÍN, para el cual lo íntimo se desarrolla en lo interior, donde habita el espíritu y por tanto se entra en comunión con Dios. Es una línea de pensamiento interiorista que se desarrolló a lo largo de la Edad Media, influyendo en autores posteriores como Kant o Descartes¹³.

SCHMIDT se expresó en otro sentido. Para este autor, la idea de los Derechos Fundamentales (en adelante DDFF) no apareció hasta llegado el siglo XVI, con el control del Estado por parte de los ciudadanos y con el reconocimiento de la intimidad en la religión a través de las ideas luteranas y puritanas. Al surgir una *libertad de religión* que anteriormente era difícil de sustanciar en el mundo romano y medieval, se manifestó un Derecho Fundamental a la intimidad. La libertad del individuo en la esfera íntima fue ilimitada, mientras que las limitaciones al Estado se ejercen por los ciudadanos, controlándolo¹⁴.

En el siglo XVI las ideas de la Edad Media sobre el poder y la sociedad comenzaron a transformarse. Las formas revolucionarias y cambiantes en el pensamiento convivie-

¹¹ Estas notas se encuentran en la obra de Aristóteles "*Política*". Aquí se toma como referencia la edición de 2006 de Espasa, ARISTÓTELES, *Política*; Espasa libros, Madrid, 2006. pero se tenían notas de la antigua edición de Austral de 1989, traducida por el Profesor Julián Marías y María Arujo, edición varias veces reimpresa, muy renombrada y tratada por la doctrina.

¹² MONTESQUIEU, C., *Del espíritu de las Leyes*, Madrid, 2012.

¹³ Referentes de este autor se consideran las obras "*Confesiones*" o en "*De vera Religione*"

¹⁴ SCHMITT, C., *Teoría de la Constitución (Verfassungslehre, 1928)*, Madrid, 2001.

ron con otras, como fue la Escuela de Teólogos y Juristas españoles del siglo XVI, que no abandonó la Escolástica medieval y la renovó, para contrastarla con la *Contrarreforma*. El Renacimiento introduce la vuelta a conceptos de Estados más abiertos, pero también las ideas y formas de gobiernos tiránicas, cercanas a las dictaduras como son las *Ciudades-Estado* o sus formas renacentistas en los Estados Italianos. MAQUIAVELO sería un buen ejemplo de estas ideas¹⁵. El Renacimiento supuso una modernidad frente a la Edad Media pero también una vuelta a las ideas y formas de gobierno clásicas de Grecia y Roma, tiempo en el que la dignidad de la persona no fue reconocida y con ello el Derecho a la intimidad se encontró en retroceso. Las teorías agustinas no estuvieron completamente al margen, en especial dentro de la esfera española de pensamiento. Como señala la doctrina¹⁶, filósofos como el español FRANCISCO SÁNCHEZ, postulaba la introspección como método de conocimiento y con ello realzaba el valor de la intimidad¹⁷.

El factor relevante en el Renacimiento fue el pensamiento luterano. La iglesia luterana pasó a ser una iglesia de Estado, pues la religión no fue considerado un asunto íntimo, sino que la adscripción a una religión se convirtió en un asunto político y, por tanto, público¹⁸. Los calvinistas defendían por su parte el poder secular para imponer los juicios de ortodoxia y moralidad. Existía un gobierno de los más *santos*, con un fuerte componente de *observación* de unos a los otros, para mantener ese nivel de moral exigido. Los puritanos huyeron de este orden persecutorio a América¹⁹, donde se dictaron normas más acordes con la intimidad, pero también se generaron circunstancias que controlaban aspectos de la conducta que se pueden considerar hoy insólitos.

¹⁵. MAQUIAVELO, N., *Discursos sobre la primera época de Tito Livio*, Madrid, 2005. “es necesario que sea uno solo aquél de cuyos métodos e inteligencia dependa la organización de la Ciudad.”

¹⁶ ABELLÁN GARCÍA, J., *El Pensamiento español de Séneca a Zubiri*, Madrid, 1977.

¹⁷ RÚIZ MIGUEL, C., *La configuración Constitucional del Derecho a la Intimidad*, Madrid, 1995.

¹⁸ SCHMITT, C., *Teoría de la Constitución (Verfassungslehre, 1928)*, Madrid, 2001.

¹⁹ TOCQUEVILLE, A., *La democracia en América*, Madrid, 2010. El autor realizó un estudio sobre este tema en su obra “*La democracia en América*” con relevantes ejemplos de normas y procedimientos. Se reseña en bibliografía la edición de 2010, pero se tienen notas de otras ediciones sobre los años 80, sin referenciar.

tos o absurdos. A modo de ejemplo, en la ley penal de Massachusetts un sacerdote católico expulsado de la colonia no podía volver a ella, bajo pena de muerte. Otro ejemplo es la imposición de estrictas fórmulas de culto, obligación de asistencia a los ritos religiosos, bajo pena, en algunos casos, de muerte; modos de hablar rigurosos, todo ello, hay que decir, votado y ejercido libremente (en una acepción limitada para nuestra concepción de la libertad) por los propios ciudadanos, pensando que las costumbres de los mismos eran aún más austeras que sus normas, por lo que se puede considerar que se olvidaron de su propia persecución religiosa en Europa, generando prácticamente un régimen político-religioso expuesto a todo tipo de excesos públicos²⁰. La Reforma luterana, con el principio del libre examen, propiciando una relación íntima del individuo con Dios sin intervención eclesiástica. Del mismo modo, en filosofía, todo lo que sea humano, “sea conciencia, creencia, voluntad o acción, es, por definición, libre. Hombre y libertad se van identificando”²¹. Junto con el liberalismo se generó el individualismo y la privacidad.²² Los autores representativos de este periodo de la historia serían, por excelencia, HOBBS Y LOCKE, tratados ampliamente por la doctrina del Derecho. Defendieron que “lo privado es una categoría deducida de un espacio sustraído de lo público”²³. Hobbes se centró en la propiedad y la esfera económica como origen de la sociedad, considerando que la necesidad de impedir la invasión de la propiedad ajena era un elemento fundamental. Únicamente el soberano, según Hobbes, tenía la potestad de invadir la propiedad de los súbditos. En las teorías de Hobbes, la privacidad tuvo un espacio mínimo, pues estaba subordinada

²⁰ ALEXIS DE TOCQUEVILLE comenta el caso de una joven que había sido multada por dejarse besar.

²¹ BEJAR MERINO, H., *El ámbito íntimo. Privacidad, individualismo y modernidad*, Madrid, 1990. pág.

24 “La esfera privada se dibuja como un bastión de no interferencia en lo que sería el último reducto de mi libertad. Con el reconocimiento de la privacidad como uno de los pivotes del pensamiento liberal, lo privado realza su valor a expensas de la vida pública” ... “la privacidad tiene una naturaleza paradójica: consecuencia del aislamiento respecto a la sociedad, sólo puede existir dentro de ella. La privacidad es una posesión de un ser que anhela la soledad pero que sabe que no puede vivir sin los demás a riesgo de dejar de ser humano.”

²² Obra citada. pág. 28

²³ HOBBS, T., *Leviatan*, Madrid, 2003.

a la concesión del soberano, no era una elección del individuo. En otra dirección, partiendo de la libertad individual, Locke expuso: “Donde no hay ley, no pueden los hombres librarse de la presión y de la violencia de los demás, que es en lo que consiste la libertad” (...) “Cada cual debe disponer, como bien le parezca, de su persona, de sus actos, de sus bienes y de todo cuanto le pertenece, sometiéndose a lo que ordenen las leyes bajo las cuales vive, para no verse sometido, de ese modo, a la voluntad arbitraria de otro, y poder seguir libremente la suya propia”²⁴. De las palabras reproducidas se infiere una auténtica diferenciación entre dos esferas, la pública y la privada. Esa diferenciación de esferas, el respeto a lo privado y el desarrollo de la individualidad de los ciudadanos generó el reconocimiento de derechos como el respeto a la vida doméstica, un límite al poder inviolable, incluyendo la propiedad privada como parte del individuo y sus derechos. El poder tuvo la obligación de no intervenir en la vida privada e individual de los ciudadanos para mantener su legitimidad política y moral. Todo un camino que fue recorrido a lo largo de los siglos XVII y XVIII²⁵.

Desde mediados del siglo XVII se desarrolló la Ilustración. Con este sentido del pensamiento humano se manifestó un importante derecho: *la información*. La Revolución Francesa sería su consecuencia. La Ilustración saca a *la luz* la oscuridad, lo secreto, lo que pocos controlaban. Con el paso del tiempo, ese Derecho deberá ser regulado, para evitar formas de abuso, contra otros derechos también muy importantes: el honor y la intimidad. Antes, las reformas revolucionarias y sus alusiones a lo *Antiguo*, generaron efectos colaterales que oscurecieron las intenciones de los que deseaban la modernidad, con episodios terroríficos y restricción de las libertades individuales. Autores como TOCQUEVILLE o CONSTANT hicieron amplia alusión a esa época²⁶. El Derecho

²⁴ LOCKE, J., *Segundo ensayo sobre el gobierno civil*, Madrid, 2003.

²⁵ BEJAR MERINO, H., *El ámbito íntimo. Privacidad, individualismo y modernidad*, Madrid, 1990, pág. 41. “sabido es que moral y política no son precisamente hermanas de sangre. La esfera privada será pasto de toda serie de desmanes a no ser que esté *legalmente protegida*. De otro modo, la arbitrariedad del poder acechará en silencio el ámbito del individuo”

²⁶ Estos autores no se tratan ampliamente, sólo se mencionan, pues el objetivo de este epígrafe es dar una referencia temporal al derecho a la protección de datos, desde los conceptos de los derechos a la intimidad y la privacidad. Las obras de Tocqueville y Constant, por tanto, sólo se nombran.

a la inviolabilidad del domicilio, por ejemplo, en el periodo postrevolucionario, fue una medida para garantizar la seguridad personal frente a la detención arbitraria, más que un reconocimiento del derecho a la intimidad.

La nueva nación americana tuvo una notable influencia en la evolución de los Derechos Fundamentales. TOCQUEVILLE apunta, por ejemplo, la capacidad espontánea de asociación, cooperación y fe en el provenir, capacidades que destaca de la nueva sociedad americana, indicativos de lo que hoy se llamaría *Sociedad Civil*. La esfera pública y la esfera privada formaron espacios y tiempos separados²⁷. CARL SCHMITT anotó que en la *Declaración francesa de Derechos del Hombre y del Ciudadano* no se reseñaron las nociones de derechos con conexiones a la intimidad, como es la libertad de religión²⁸. Esta noción era conocida probadamente por los franceses, pero no la incluyeron, por razones de vinculación con el Estado anterior. Los norteamericanos no tuvieron ese límite.

Los cambios tecnológicos en el siglo XIX ya apuntaban a nuevos cambios sociológicos y, por tanto, de derechos. La Revolución Industrial generó una sociedad de masas, poco a poco, concentrándose en las ciudades, compartiendo espacios reducidos donde no era posible el desarrollo individual por razones físicas. Todos se veían, todos se rozaban. Surgió un fenómeno social de hacinamiento, voluntario o simplemente marcado por condiciones económicas. Aun existiendo diferencias entre lo privado y lo público, la intimidad no tuvo una consideración prioritaria para la mayoría de la población que subsistía en esas circunstancias. Dentro del proceso urbano se produjo una doble vertiente de conductas: primero se realizó lo exterior, contrario de lo que es la intimidad, no dejando espacio para su desarrollo. Segundo, los factores de densidad

²⁷ HELENA BEJAR cita a Tocqueville: "El habitante se apega a cada uno de los intereses de su país como a los suyos propios. Se glorifica con la gloria de la nación; en los triunfos que esta obtiene cree reconocer su obra personal y ello le enorgullece, a la vez que se alegra de la prosperidad general de la que se beneficia. Experimenta por su patria un sentimiento análogo al que siente por su familia y es también una suerte de egoísmo lo que le hace interesarse por el Estado" TOCQUEVILLE, A., *La democracia en América*, Madrid, 2010. páginas 53-54

²⁸ SCHMITT, C., *Teoría de la Constitución (Verfassungslehre, 1928)*, Madrid, 2001.

poblacional con diferentes orígenes y de espacios enormes, fomentaron la soledad del individuo, surgiendo reacciones íntimas e introspectivas de conducta²⁹. De este individualismo se pasó a lo largo del siglo XIX a un *colectivismo*. ORTEGA Y GASSET trató este fenómeno en su obra ³⁰. Ortega fue ante todo íntimo, solitario, pues la soledad “*hace a la persona compacta y la repuja*”. Afirmó que en el aislamiento se produce una criba y discriminación de las ideas, afanes y fervores de la persona, que aprende cuáles son los suyos y cuáles son anónimos, “*ambientes caídos del camino como una polvareda*”. Según Ortega, vivir es “*haberse quedado solo*” Es a principios de siglo XX, cuando en América se produjeron las primeras apreciaciones respecto al derecho a la privacidad.

1.2. La civilización y los datos personales.

Durante la anterior exposición temporal y forzosamente sintética, se tuvo como referencia la intimidad, respetando las líneas de la doctrina sobre la evolución y desarrollo del derecho autónomo a la protección de datos personales, sobre el que se centra el presente estudio. La vida en sociedad genera la necesidad de recabar datos sobre la población para planificar diversos aspectos de la vida en común. En otras palabras, fue la convivencia en sociedad y el querer o necesitar conocer al otro, al vecino, a los otros que ocupan el poblado o la ciudad; conocimiento que se almacenó en diferentes tipos de soportes para *confiar*, para intercambiar productos, servicios o culturas, religión, lenguajes. Conocimiento que en manos del mal y de la falta de respeto al seme-

²⁹ RÚIZ MIGUEL, C., *La configuración Constitucional del Derecho a la Intimidad*, Madrid, 1995. En el sentido de desarrollo histórico del derecho a la protección de datos se menciona una de las primeras obras que lo trata, la tesis doctoral de la autora GARRIGA DOMÍNGUEZ, A., *La protección de datos personales en el Derecho español*, Madrid, 1999.

³⁰ ORTEGA Y GASSET, J., *El Espectador*, Madrid, 2007. “Socialización del hombre” que se encuadra dentro de “El espectador” y que el autor desarrolló en la “Rebelión de las masas” ORTEGA Y GASSET, J., *La Rebelión de las masas*, Madrid, 2009. . Se referencia esta edición de 2009, existiendo otras ediciones, de las que se conservan anotaciones.

jante de todas las épocas codujo a situaciones conflictivas, penosas o terroríficas, dependiendo de la época y los poderes ejercientes. Lo tiránico no respeta al otro semejante, afirmación que sirve de base a todo el sistema jurídico. Lo ilegítimo quiere siempre el sometimiento a la voluntad arbitraria del tirano, sea un régimen personificado en un solo líder o sea Estado conformado por leyes teóricamente respetuosas con los derechos de las personas, desde donde se promueva la imposición de conductas en contra de los derechos inalienables del ser humano. Los denominados *derechos de la personalidad* (honor, imagen, intimidad, domicilio, familia) tardaron en la historia de la humanidad en ser reconocidos como tal para todos los ciudadanos³¹. Los citados derechos se considera que evolucionaron desde el Derecho Civil al Derecho Constitucional a lo largo del siglo XIX, pues los derechos de la personalidad, siendo en un principio considerados derechos del ámbito individual y en una sociedad dominada por el Liberalismo, necesitaron de la intervención del Estado para asegurarse la efectividad de su ejercicio. Se podría hablar de una doble protección para los derechos de la personalidad por parte del Derecho Privado hacia el Derecho Público constitucionalista, situándose la evolución de los conceptos jurídicos que solamente formaban parte de los Códigos civiles de la sociedad liberal del siglo XIX en los DDFF (Derechos Fundamentales) constitucionales del siglo XX. El honor, la intimidad y la propia imagen no se regularon en España hasta la Constitución de 1978³².

2. Normas internacionales y europeas.

El análisis expuesto a continuación vendría a ser un línea temporal y normativa. Primero tratada desde el ámbito exterior al Derecho español, con énfasis en el Derecho Europeo que afecta a la protección de datos, antes de entrar en el análisis de la Cons-

³¹ CORDERO CUTILLAS, I., "Redefiniendo los derechos de la personalidad en el siglo XXI", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, , 2014, pág. 20 y ss..

³² Salvo algunas excepciones de mención en la jurisprudencia, como la STS de 6 de diciembre de 1912 (sin numeración conocida) sobre el derecho al honor, no existe regulación en cuanto a los derechos de la personalidad, conocidos como derechos individuales o del Liberalismo.

titución Española y la Ley de Protección de Datos Personales de 1999. En este primer punto, se traza una línea temporal por medio de Tratados Internacionales, regulación europea, Convenios, y Sentencias especialmente relevantes para la normativa española. Durante el desarrollo del presente estudio se aprobó por las Instituciones Europeas el nuevo Reglamento Europeo y del Consejo 2016/679, de 27 de abril, de protección de datos personales, que se nombrará bajo el acrónimo RGPD. Esta norma europea que también será objeto de análisis, será de directa aplicación en los Estados miembros y entrará en vigor en mayo de 2018.

2.1. Del Derecho a la Intimidad al Derecho a la Protección de Datos.

Como se ha observado en los textos precedentes, el derecho a la intimidad es fruto de una evolución histórica, esto es, no fue un derecho creado o repentino a partir del surgimiento de la sociedad americana; aunque gran parte de la doctrina defiende que el derecho a la intimidad no surge como tal hasta el siglo XIX, como un derecho moderno, sí es cierto que ya anteriormente se defendían posiciones a favor de este derecho, en especial por LOCKE y los pensadores liberales³³. Es mayoritariamente admitido que el sistema jurídico norteamericano protegería la privacidad, que no es exactamente una protección a la intimidad. La palabra privacidad o *privacy* no aparece ni en la Constitución de los EEUU ni tampoco en sus enmiendas. El carácter flexible del texto norteamericano facilitó que la Corte Suprema declarase que la Decimocuarta Enmienda protege el Derecho a la privacidad, pues lo relacionaron con la integridad corporal, la libertad de asociación, la libertad de decisión en cuestiones como la educación, la sexualidad y la vida familiar³⁴. Es un concepto amplísimo dentro de la so-

³³ RUIZ referenció la obra de Alan WESTIN, *Privacy and Freedom*. RÚIZ MIGUEL, C., *La configuración Constitucional del Derecho a la Intimidad*, Madrid, 1995. - WESTIN, A., *Privacy and Freedom*, New York, 1967.

³⁴ ABRIL, P., "La intimidad europea frente a la privacidad americana", *Indret: Revista para el Análisis del Derecho*, nº 1, 2014, pág. 62. Patricia S. Abril y Eugenio Pizarro realizan un aclaratorio artículo,

ciudad americana, con multitud de significados que comprenden intereses y prerrogativas de la esfera personal de los ciudadanos. No existieron polémicas en cuanto al derecho a la protección de datos personales ni nació un nuevo derecho fundamental con la llegada de los medios técnicos de tratamiento de datos personales. Para el sistema de los EEUU la protección de datos de carácter personal no representó ningún derecho fundamental. No existió debate alguno en torno al objeto de protección, pues el concepto de *privacy* se amplió con los nuevos tiempos a través de las resoluciones jurisprudenciales, con la casuística de las controversias que llegaban a los Tribunales³⁵.

El derecho a la privacidad, desde la perspectiva norteamericana, protege también frente a los ataques realizados por un particular. El perjudicado puede activar acciones indemnizatorias de contenido extracontractual³⁶. La privacidad, por tanto, podría

muy actual. El derecho a la privacidad desde un punto de vista norteamericano es un *pack* de Derechos protegidos ante la injerencia del Estado, un “derecho a lo físico, a la información, a decidir libremente, a la propiedad y a la libre asociación”, dentro de un marco de interpretación de “la libertad como valor fundamental en la sociedad estadounidense” ... “privacidad y libertad son términos entremezclados y a la vez cobran vida propia” (...) “Pese a la ausencia literal del término *privacidad* en la Constitución, ciertos derechos a la privacidad son doctrina sentada a través del precedente judicial”. Este resumen comenta la doctrina legal norteamericana, afirmando que ésta “conciben la autonomía como el valor central de la privacidad”

³⁵ SERRANO PÉREZ, M., “El derecho Fundamental a la protección de datos. Su contenido esencial.”, *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, nº 1, 2005, pág. 245-265, pág. 29-33. Véase también SERRANO PÉREZ, M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, 2003, pág. 33. La autora consideró errónea la recepción del concepto de *privacy* norteamericano en el sistema doctrinal continental una perspectiva errónea. Fue un intento de adecuación de los ordenamientos europeos frente al ordenamiento norteamericano en cuanto a la protección de datos y las nuevas tecnologías. Citando a AMADEO FRANCO, la autora consideró que de la ubicación constitucional del derecho a la protección de datos y del derecho a la *privacy* norteamericana dependería el rango de la fuente que intervendría para su disciplina y los límites que se le pudieran adjudicar.

³⁶ SERRANO PÉREZ, M., “El derecho Fundamental a la protección de datos. Su contenido esencial.”, *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, nº 1, 2005, pág. 245-265.

ser considerada, en primer lugar, el ámbito de construcción de la personalidad, en ese ámbito personal se desarrolla lo que se denomina por la doctrina el espacio de ensayo del yo, el espacio donde el individuo se prepara para afrontar el mundo exterior, un ámbito de la libertad personal. Por último, la privacidad es una condición para la intimidad, como “*relaciones excepcionales en su intensidad, fundadas en el deseo de compartir un proyecto común en un mutuo cuidado de las personas que participan en esa relación, o también puede ese espacio no ser compartido con nadie, ser sólo del individuo*”³⁷. La intimidad no es lo mismo que la privacidad, pero necesita de la privacidad para desarrollarse.

El ordenamiento jurídico dio forma a la protección de lo *privado* y de lo *íntimo* a través de los DDFF. Hasta llegar a ese punto, es cierto que, no se ha realizado una *Historia del Derecho a la Intimidad* en la que basar una línea decisiva de estudio y análisis. Hay regulaciones civiles, eclesiásticas y penales, que trazaron líneas de defensa y reconocimiento a la intimidad y sus manifestaciones, lo que, en un principio, tomando las palabras del Profesor ALBADALEJO, se definió como *intimidad en el Derecho civil*. La intimidad como Derecho Fundamental llegará a lo largo del siglo XX.

2.1.1 La declaración de Thomas Coole, de 1888 en relación al “*derecho a no ser molestado*”.

La mayoría de la doctrina suele citar como origen de la protección de la *privacy* la declaración del juez Thomas Coole en 1888. Fue la primera vez que el Derecho a la privacidad se defendió como un derecho constitucional³⁸.

³⁷ BEJAR MERINO, H., *El ámbito íntimo. Privacidad, individualismo y modernidad*, Madrid, 1990, pág. 154-155.

³⁸ SALDAÑA, N., "El Derecho a la Privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego.", *Teoría y realidad Constitucional* , nº 28, 2011. Y véase también SALDAÑA, N., "The Right to Privacy" La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el Centenario legado de Warren y Brandeis", *Revista de Derecho*

A finales del siglo XIX existía una motivada necesidad de protección a la privacidad desde una perspectiva constitucional y judicial. En el Derecho heredado de Inglaterra, llamado *Derecho Colonial*, dentro de la expresión *a man's house as his castle* (la casa de un hombre es su castillo) confirió al hogar de cada persona una protección individual. En 1647 el *Código de Rhode Island* estableció que “la casa de un hombre es para sí mismo, su familia y sus bienes como un castillo”³⁹. La tradición tuvo reconocimiento en 1791 con las garantías de la Tercera enmienda de la Constitución norteamericana, que prohibió requisar los domicilios de los particulares por los soldados sin el consentimiento de sus propietarios en tiempos de paz. También se garantizó la inviolabilidad del domicilio privado en la garantía de la Cuarta Enmienda, que prohibió los registros y requisas de forma arbitraria o injustificada. La Quinta Enmienda protegió a la persona frente a la incriminación contra uno mismo, al igual que impidió al Gobierno obligar a un ciudadano a revelar información personal, con lo cual se protege también con esta Quinta enmienda zonas privadas y reservadas de la personalidad.

El juez Thomas M. Cooley consideró en su “*Tratado de Derecho Constitucional*” de 1868 que los Derechos promulgados en la Tercera, Cuarta y Quinta Enmienda son considerados *vehículos de protección de la privacidad individual*⁴⁰.

En 1873, Sir James Fitz Stephen en su análisis “*Liberty, Equality, Fraternity*” realizó las siguientes afirmaciones: “La legislación y la opinión pública deben respetar escrupulosamente la privacidad en todos los casos. Definir claramente el ámbito de la privacidad es imposible, pero puede ser descrito en términos generales”. Especialmente se resalta la siguiente cita: “Todas las relaciones más íntimas y delicadas de la vida son de tal naturaleza que someterlas a observación (...) inflige un gran dolor y puede causar un daño moral duradero (...) Tratar de regular los asuntos internos de una fami-

político, nº 85, 2012. Nieves Saldaña ha realizado dos estudios en los que enfoca la interpretación del trabajo de Warren y Brandeis. La autora analiza en ambos el Derecho Norteamericano a la privacidad.

³⁹ El principio fue formulado por William Pitt en 1763 oponiendo esa máxima al poder del monarca en una intervención parlamentaria. En 1774 John Adams invocaba este derecho ante un tribunal.

⁴⁰ SALDAÑA cita la obra de Cooley de 1868 “*A Treatise in the Constitutional Limitations Which Rest upon the legislative Power of the States of the American Union.*”

lia, las relaciones de amor o amistad, o muchas otras cosas del mismo tipo, por ley o por la coerción de la opinión pública, es como tratar de sacar una pestaña del ojo de un hombre con un par de tenazas. Puedes sacar el ojo, pero nunca podrán asir la pestaña”

En 1879, Thomas Cooley acuñó la famosa expresión, muy utilizada por muchos analistas de protección de datos *“The right to be let alone”* en su obra *“Treatise on the Law of Torts”*⁴¹. En esta obra el juez analizó casos de supuestas violaciones de la Cuarta y Quinta Enmiendas (registros y requisas ilegales en domicilios particulares para obtener suficientes pruebas de cara a un procedimiento contra el acusado). Cooley afirmó que el derecho de la persona a protegerse de las intromisiones en su privacidad negaba la legalidad de la intromisión del gobierno y de la curiosidad lasciva del público en general⁴². Será en 1886 cuando el Tribunal Supremo de los Estados Unidos de América utilizó la expresión y doctrina de Cooley en el caso *Boyd vs. United States*, admitiendo que la aprensión de documentación privada y su utilización como evidencia en su contra, eran violaciones de la Cuarta y Quinta Enmienda, conectando estas garantías constitucionales con la privacidad. En concreto el TS de los Estados Unidos de América afirmó que:

“La esencia misma de la libertad y seguridad constitucional se ve afectada ante cualquier invasión por parte del gobierno y de sus agentes de la santidad del hogar de la persona y de la privacidad de su vida. No es la rotura de sus puertas, o el registro de sus cajones lo que constituye la esencia del delito, sino la invasión de su inderogable derecho a la libertad y seguridad personal y a la propiedad privada”

A partir de este momento, la jurisprudencia norteamericana se desarrolló a favor de proteger el Derecho Fundamental a la Privacidad, incluyendo también la intimidad de los ciudadanos.

⁴¹ Como señala SALDAÑA, esta expresión la utilizó Cooley para definir el derecho individual a la inmunidad personal frente a agresiones físicas, y la profesora lo cita así: “el derecho de la persona se dice que es el derecho a la completa inmunidad; a ser dejado solo”.

⁴² SALDAÑA, N., obra citada.

2.1.2 La fundamentación de Samuel Warren y Louis Brandeis en 1890 sobre el *Derecho a la privacidad*.

Fueron WARREN Y BRANDEIS quienes sentaron las bases técnico-jurídicas del Derecho a la privacidad en su obra clásica "*The rights to Privacy*" de 1890 ⁴³. En la citada obra influyó el aumento de la difusión de la información por medio de las técnicas de publicación a través de la fotografía y la reproducción de la imagen. Estas circunstancias permitieron la exposición de aspectos privados de personas que eran objeto de interés de la sociedad. No podía ser ejercitada, teóricamente, ninguna acción legal para evitar la violación de la privacidad, por lo que resultaba necesaria la creación de un recurso legal que fuera efectivo para la defensa de la vida privada de los individuos frente a los abusos de las publicaciones ⁴⁴. La obra de WARREN y BRANDEIS supuso una continuación de la doctrina creada por el juez Thomas Cooley. Con su artículo "*The right to Privacy*", denunciaron la divulgación de información privada en la prensa indiscriminadamente, defendiendo la tesis de que impedir la publicación de esa información personal y privada era una manifestación del derecho del individuo a ser de-

⁴³Véase PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010. Páginas 323-350, entre otros autores, pues es tratada por gran parte de la doctrina. La obra de Warren y Brandeis tiene una traducción al castellano editada por Civitas WARREN, SAMUEL; BRANDEIS, LOUIS, *El derecho a la intimidad*, Madrid, 1995.

⁴⁴ SALDAÑA, N., "The Right to Privacy" La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el Centenario legado de Warren y Brandeis", *Revista de Derecho Político*, nº 85, 2012. Se añadió otro aspecto a tener en cuenta que motivaría el análisis de Warren y Brandeis, antiguos compañeros de estudios (cursaron juntos los estudios de Derecho en la Harvard Law School entre 1875 y 1877. Brandeis procedía de una familia judía de Kentucky mientras que Warren pertenecía a la élite económica y social de Boston). Warren iba a contraer matrimonio con la hija de un importante senador (senador Bayard) y no quería que su vida anterior, un tanto desordenada, fuera objeto de publicación en la prensa. Pudo influir, siguiendo publicaciones norteamericanas, que la alta burguesía de este país deseaba no ser objeto de conocimiento público. Reformularon la expresión de Cooley "*The right to be alone*" y realizaron un estudio que se publicó el 15 de diciembre de 1890 en la revista "*Harvard Law Review*".

*jado sólo.*⁴⁵ Los autores dieron una gran importancia a este concepto y estaban muy sensibilizados por las publicaciones en la prensa sensacionalista. Los avances tecnológicos, teléfono, telégrafo, fotógrafo, impresiones en papel, mejores medios de transporte y más rápidos, eran una primigenia amenaza para un sector de la sociedad, que no deseaba la curiosidad del público. En concreto, los citados autores afirmaron que:

*“Los recientes inventos y los nuevos métodos de hacer negocios fueron los focos de atención en el siguiente paso que hubo de darse para amparar a la persona, y garantizar al individuo lo que el juez Cooley denomina el Derecho “a no ser molestado”. Las instantáneas fotográficas y las empresas periodísticas han invadido los sagrados recintos de la vida privada y hogareña y los numerosos ingenios mecánicos amenazan con hacer realidad la profecía que reza: “lo que se susurre en la intimidad, será proclamado a los cuatro vientos” (...) La intensidad y la complejidad de la vida, que acompañan a los avances de la civilización, han hecho necesario un cierto distanciamiento del mundo, y el hombre, bajo la refinada influencia de la cultura, se ha hecho más vulnerable a la publicidad, de modo que la soledad y la intimidad se han convertido en algo esencial para la persona; por ello, los nuevos modos e inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una angustia mucho mayor que la que le pueden causar los daños personales”*⁴⁶

⁴⁵ William PROSSER sugiere en su obra “Privacy” de 1960 que las motivaciones de Warren para escribir ese monográfico eran evitar publicaciones sensacionalistas sobre su familia, especialmente sobre el enlace de la hija de Warren, ante lo que SALDAÑA discrepa, pues (se cita textual) “la tesis de Prosser no se sostiene dada la corta edad de la hija de Warren cuando aparece el artículo en 1890”

La tesis de PÉREZ LUÑO parece también cuestionada por SALDAÑA. Parece ser que el biógrafo de Brandeis, Alfred Lief, señala que la causa que motivó el monográfico es la expuesta por Pérez Luño. Pero no se tiene en cuenta otro estudio de Paper de 1983 en el que se señala que el nombre de Warren sólo se menciona dos veces en la publicación “The Saturday Evening” entre los años 1883 y 1890.

⁴⁶ WARREN, SAMUEL; BRANDEIS, LOUIS, *El derecho a la intimidad*, Madrid, 1995, pág. 25-27. Este párrafo se podría escribir ahora mismo, más de un siglo después. La diferencia, como se verá en otros epígrafes, será que no muchos ciudadanos sentirían un *sufrimiento espiritual* tal y como lo describen los autores. Muchos ciudadanos disfrutaban y se enorgullecían de la publicidad de su privacidad. Fomentan esa forma de divulgación ellos mismos. El problema surge cuando, junto a los interesados o por los

WARREN Y BRANDEIS dieron un carácter general a su reclamación de protección ante la invasión de la privacidad. Quisieron la materialización del Derecho a la privacidad y no lo restringieron a un ámbito social o económico. Deseaban que el Derecho a la privacidad se le otorgue a toda persona “*para decidir en qué medida pueden ser comunicados a otros sus pensamientos, sentimientos y emociones*”. Esta atribución igualitaria del Derecho a la Privacidad generó que la doctrina de WARREN Y BRANDEIS tuviera un indiscutible carácter democrático, poco frecuente en la época⁴⁷. Para ambos autores, el Derecho a la Privacidad es un derecho básico de toda persona. Lo diferenciaron también de los Derechos a la Libertad y del Derecho a la Propiedad, clásicos de la época. Argumentaron con que la base para el Derecho a la Privacidad es el Derecho a la *Inviolabilidad de la Persona*. Los autores dieron un contenido psicológico al Derecho a la Privacidad, demandando el *control sobre la información que afecta a la personalidad individual*. Es lo que llamarón “*The right to one’s personality*”.

La aludida obra influyó en los pronunciamientos de diversos Tribunales que reconocían, de diferentes formas, el Derecho a la Privacidad. En 1939, el *American Law Institute*, codifica, el denominado *Right to Privacy* en el primer *Restatement of Torts*, tipificado en el artículo 867 el supuesto de publicación de asuntos de la vida privada o la utilización de imágenes personales. Se estaría frente a lo que modernamente se denomina un tratamiento de datos no autorizado por su titular⁴⁸.

interesados, se añaden informaciones que son de terceros, que pueden estar protegidos por ley, pueden no querer estar junto a esa persona o bien no desean de ningún modo esa publicidad.

47 SALDAÑA cita al periodista Tire Godkin, el cual defendía en 1891 que el Derecho a la Privacidad tenía un significado distinto en función de las personas y las clases sociales.

48 Otros autores revisaron a WARREN Y BRANDEIS en la década de los años 60 del pasado siglo XX. Por citar en relevancia a William PROSSER en *California Law Review*, 1960. Prosser revisó la doctrina de WARREN Y BRANDEIS y la introducción de este Derecho en el sistema constitucional. En España, el autor MARC CARRILLO realizó un monográfico titulado “El Derecho a no ser molestado” con el subtítulo: “Información y vida Privada”. No es una revisión de la obra del juez Cooley ni tampoco de la obra de Warren y Brandeis, aunque toma prestado el título y el subtítulo de tan comentados autores. Analiza la situación actual del uso de la información privada, aportando sentencias y casos. Es una obra citada en

2.1.3 El artículo 12 y el artículo 19 de la *Declaración Universal de Derechos Humanos* en 1948.

Hasta llegar a la Declaración Universal de Derechos Humanos (DDHH), toda la Humanidad pasó por unas etapas históricas cargadas de controversias y de dudosos resultados. No es objeto de este análisis ese devenir histórico, pero los apuntes a los cambios sufridos en las civilizaciones durante la primera mitad del siglo XX, aunque en pinceladas, introducen la exposición de la evolución del Derecho Fundamental a la privacidad, y, por tanto, al desarrollo de la intimidad como Derecho Fundamental igualmente. Esta primera mitad del siglo XX se caracteriza por el totalitarismo⁴⁹, palabra de muchas acepciones entre las que se distingue una especialmente: “*régimen político que ejerce fuerte intervención en todos los órdenes de la vida nacional, concentrando la totalidad de los poderes estatales en manos de un grupo o partido que no permite la actuación de otros partidos*”⁵⁰. El totalitarismo es un concepto que aspira a la generación de un sistema cerrado que se apodera del poder y de la política. No utiliza la política para la defensa de la colectividad contra el desorden en el interior y las amenazas exteriores. Muy al contrario, su objetivo es forjar un ser humano distinto, *El Hombre Total*. Es un fenómeno de despolitización y de despersonalización, destruyendo la economía, la moral, el derecho, el arte, o cualquier manifestación de la personalidad. Este fenómeno se instrumenta desde el Estado. El Estado controla

la mayor parte de la bibliografía sobre protección de datos, por lo que estas menciones se pueden ampliar a muchas otras obras, prácticamente todos los autores lo tienen como referencia.

⁴⁹ RÚIZ MIGUEL, C., *La configuración Constitucional del Derecho a la Intimidad*, Madrid, 1995. El autor analizó esta forma de hacer política citando a Julien Freund en su obra “*L’essence du politique*” de 1961.

⁵⁰ REAL ACADEMIA ESPAÑOLA, ., *Diccionario de la Real Academia Española*, España, 2012. Como un comentario se apunta la definición aportada por el autor de literatura Javier Marías para un artículo del periódico El País: “Hay una peste que comparten todas las tiranías. Es la que emiten la intolerancia, el odio a la crítica y el deseo de aniquilar a los “desobedientes”. http://elpaissemanal.elpais.com/columna/javier-marias-atribulados/?id_externo_rsoc=FB_CM

todo acto y toda manifestación de cada individuo o grupo, sea educativo, laboral, económico, intelectual, de ocio, de vida familiar o incluso la más individual intimidad. Se excluye lo civil, lo privado, la privacidad. La intimidad no existe o no tiene posibilidades. El totalitarismo, visto desde la protección de datos, se nutre del conocimiento de datos personales, a los que trata para formar una discriminación informativa contra los que considera enemigos del Estado, o de Dios, o de la Patria, o de lo que atañe a sus intereses de poder y de control. La Historia muestra que no triunfaron estas consideraciones en gran parte de Europa. Ante el afán controlador y organizador, surgió lo inevitable: una *contrafuerza del callar y del silencio*⁵¹, el cual muestra la intimidad individual como fuerza de la libertad que se opone al totalitarismo.

Una de las manifestaciones del totalitarismo es su intervención en la esfera más personal, por ejemplo, en la procreación y en el matrimonio, dos aspectos completamente íntimos de la persona, retrocediendo en el tiempo hacia civilizaciones anteriores que se basaban en la eugenesia para generar sus normas⁵². No sólo son las manifestaciones del totalitarismo en forma de nazismo o de fascismo las que produjeron semejantes ideas y realidades. También las interpretaciones del marxismo, tanto soviético como chino se entienden dentro de lo que se denomina totalitarismo. Cualquier creencia o cultura que no respete las diferencias es totalitaria.

La llamada sociedad del bienestar también tiene puntos de crítica hacia su intrusismo en las esferas privadas y en la intimidad. El Estado provee como una *nodriza o padre* de una serie de servicios, pero al mismo tiempo también interviene intensamente en áreas consideradas como privadas o de la libertad individual y, sobre todo, trata datos personales. Los ciudadanos se ven obligados a entregar toda una serie de informaciones sobre diferentes cuestiones que pueden rozar el control por parte del Estado de aspectos privados e íntimos. Las exigencias de información y de control no son ajenas

⁵¹ SCHMITT, C., *Teoría de la Constitución (Verfassungslehre, 1928)*, Madrid, 2001.

⁵² Retroceso en el tiempo para nuestra civilización y nuestro sistema normativo europeo, no tanto para otros sistemas de gobierno que en estos puntos se siguen rigiendo en 2017 por normativas totalitarias.

tampoco al llamado capitalismo de consumo o de producción⁵³, pues los consumidores proveen a las empresas de multitud de datos personales, algunos para la misma función de consumo (compra de bienes y/o servicios); otros datos son de personalidad o de preferencias. Todos ellos conforman en la actualidad lo que se ha denominado *big data*.

En todo este entramado social que se desarrolla antes y después de las Guerras Mundiales, nació tímidamente la Declaración Universal de Derechos Humanos⁵⁴. En su entorno histórico, se consolidó progresivamente la obligación jurídica de los Estados respecto a Derechos esenciales y básicos para todos los seres humanos. Las Naciones Unidas inician un camino de convicciones de los distintos gobiernos, al mismo tiempo que se crearon instrumentos jurídicos para explicar, promover y legislar en los distintos países tomando como Derechos Fundamentales de toda persona los pronunciamientos de la Declaración Universal de Derechos Humanos (a partir de este momento, la Declaración)⁵⁵. Dos son los artículos relacionados con el tema de esta tesis. El ar-

⁵³ Según RÚIZ, analizando a diferentes autores, el conocimiento del consumidor hace que el sistema capitalista de consumo no tenga barreras para conocer cuáles son los deseos de su objetivo, el consumidor. El ciudadano está cada vez más controlado en su vida privada e íntima. Actualmente las empresas que conforman el sistema económico demandan más conocimiento de datos personales para mejor proveer de servicios, lo que puede resultar en un momento dado, una violación de derechos.

⁵⁴ PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010. Definición de Derechos Humanos en la página 50. “*Conjunto de Facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, la libertad y la igualdad humanas, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional e internacional*”. El autor realiza un exhaustivo análisis de los derechos humanos bajo diferentes perspectivas de la filosofía del Derecho. Véase también CARRILLO SALCEDO, J., *Soberanía de los Estados y Derechos Humanos en Derecho internacional contemporáneo.*, Madrid, 2001, pág. 49-72. En opinión del autor Carrillo Salcedo, es la convicción de los Estados miembros de Naciones Unidas la que genera obligaciones jurídicas respecto a los Derechos Humanos, manifestando la existencia en Derecho Internacional de “principios jurídicos relativos a los Derechos Fundamentales de todo ser humano, principios de los que se derivan obligaciones jurídicas para todos los Estados.”

título 12 y el 19 de la Declaración⁵⁶, que consagran el Derecho a la privacidad (artículo 12) y el Derecho a la información (artículo 19). Entre ambos Derechos se producen continuamente situaciones conflictivas, que los Tribunales frecuentemente tienen que atender, valorando en cada ocasión los derechos en conflicto y resolviendo mediante el principio de ponderación. El Derecho de comunicación y de información, de libre opinión y de investigación, entra en colisión frecuente con el Derecho a la privacidad y a la intimidad, con el Derecho a la propia imagen y al honor y con el Derecho a la protección de datos personales.

2.1.4 El *Pacto Internacional de los Derechos Civiles y políticos* de 1966.

El proceso de positivación de los Derechos Humanos para convertirlos en Derechos Fundamentales (DDFF), pasó por aclarar en qué consiste el concepto de positivación. Este concepto tiene dos interpretaciones principales. Una es entender la positivación desde un punto de vista doctrinal, la cual genera diferentes posiciones ideológicas. Otra es entender esta positivación de los DDFF desde un punto de vista institucional, como un problema técnico-jurídico⁵⁷.

⁵⁶ Artículo 12 de la Declaración Universal de Derechos Humanos:

“Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.” Con este artículo se protege el Derecho a la Privacidad, teniendo las leyes la obligación de defenderla en caso de que sufra *injerencias o ataques*. Los Estados tienen la obligación de proteger la privacidad en su faceta interna (intimidad personal) y externa (honor y reputación) generando un Derecho Positivo, leyes que hagan efectiva la protección. El artículo 19 establece el límite al Derecho a la Privacidad: “Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.”

⁵⁷ PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010. Desde este punto de vista, la positivación es una generación de reglas, una “formulación normativa a través de unos preceptos emanados según los cauces formales establecidos por el principio de validez de un determinado ordenamiento jurídico” añadiendo dentro de su visión filosófica que el entramado histórico

En el plano del Derecho a la privacidad se encuentran también estas realidades. Los DDHH se quieren positivizar en los diferentes ordenamientos de los países, con todas sus diferencias, tradiciones, doctrina, instituciones, historia normativa. Una de esas manifestaciones fue el *Pacto Internacional de los Derechos civiles y políticos* de 1966⁵⁸. Después de la *Declaración de Naciones Unidas sobre Derechos Humanos*, este Tratado multilateral reconoció y estableció mecanismos para la protección y garantía de lo que denomina *Derechos Civiles y Políticos*, entre los que encontramos a lo largo de todo su articulado manifestaciones de derechos muy próximos a la privacidad⁵⁹.

conlleve en sí mismo una evolución continuada de estos puntos de vista, los cuales se “entrelazan” continuamente en el tiempo. La tendencia a convertir en norma escrita y de obligado cumplimiento los preceptos considerados “naturales” por el mero hecho de nacer, es una afirmación. Otra cosa es pensar y analizar que no siempre el éxito de la norma se desarrolla en su práctica mundana. No siempre la norma alcanza su objetivo con éxito. La práctica de la realidad, fuera de la Doctrina y de las Instituciones, es la verdad real.

⁵⁸ El Pacto Internacional de Derechos Civiles y Políticos se aprueba junto con el Pacto Internacional de Derechos Económicos, Sociales y Culturales. Son los llamados Pactos de Nueva York de 1966-

⁵⁹ Por ejemplo, el artículo 10.1 reconoce una *amplia protección y asistencia a la familia*, con el siguiente texto: “Se debe conceder a la familia, que es el elemento natural y fundamental de la sociedad, la más amplia protección y asistencia posibles, especialmente para su constitución y mientras sea responsable del cuidado y la educación de los hijos a su cargo. El matrimonio debe contraerse con el libre consentimiento de los futuros cónyuges.” En este artículo se aprecian claras referencias a aspectos de la privacidad, como es la libertad para el matrimonio, libertad para consentir en su generación, o la educación de los hijos a cargo de la familia.

Otro ejemplo es el artículo 13: “Los Estados Partes en el presente Pacto reconocen el derecho de toda persona a la educación. Convienen en que la educación debe orientarse hacia el pleno desarrollo de la personalidad humana y del sentido de su dignidad, y debe fortalecer el respeto por los derechos humanos y las libertades fundamentales. Convienen asimismo en que la educación debe capacitar a todas las personas para participar efectivamente en una sociedad libre, favorecer la comprensión, la tolerancia y la amistad, entre todas las naciones y entre todos los grupos raciales, étnicos o religiosos y promover las actividades de las Naciones Unidas en pro del mantenimiento de la paz.” Al presentar estos rasgos de lo que debe ser un Derecho a la Educación, el Pacto genera un perfil de Derechos incluidos dentro, no ya de la privacidad humana, sino también dentro de su ámbito íntimo, como son el desarrollo de la personalidad y el sentido de su dignidad, junto con sentidos de respeto, tolerancia, comprensión y amistad.

El *Pacto Internacional de Derechos Civiles y Políticos* se considera como un referente importante por la Agencia Española de Protección de Datos Personales (AEPD), que lo incluye en su Documentación, por lo que se debe tener también presente en materia de Protección de Datos, pues a través del artículo 10 CE se incorporó a la legislación española.

2.1.5 El artículo 8 del *Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales*, Roma 1950.

Los Estados Europeos consolidaron la convicción jurídica de la obligatoriedad en materia de Derechos Humanos al generar el *Convenio Europeo de Derechos Humanos*, para la protección de los Derechos y Libertades Fundamentales (se nombra como Convenio). El Convenio se firmó en Roma el 4 de noviembre de 1950. Es un tratado multilateral de carácter restringido a los Estados miembros del Consejo de Europa. El Congreso de Europa en La Haya, 1948, aprobó a propuesta de la Comisión Política una resolución en la que se contemplaba la creación de un Tribunal de Justicia para que, ante él, cualquier ciudadano de los Estados miembros pudiera presentar un recurso en caso de que sus derechos no fueran respetados. Es el Tribunal Europeo de Derechos Humanos (TEDH), cuya jurisprudencia reafirma los derechos reconocidos en el Convenio.

Entre otra serie de Derechos Humanos a considerar, el Convenio reflejó en su artículo 8 el Derecho al respeto a la Vida Privada y Familiar⁶⁰. Además, El Convenio realizó en

El Pacto sigue añadiendo direcciones normativas para los Estados que lo ratifiquen, valgan por ahora estos ejemplos.

⁶⁰Con el siguiente texto: “*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*” Es clara la alusión a la privacidad, concretando aún más en el respeto al domicilio y a la correspondencia. En el artículo 9 del Convenio se establece que: “*Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión. Este derecho implica la libertad de cambiar de religión o de convicciones, así como la libertad de manifestar su religión o sus con-*

1950 dos importantes contribuciones⁶¹: Por una parte, la definición jurídica de los DDHH inderogables en cualquier situación, como en caso de guerra y de cualquier otra circunstancia que amenace la nación. Por otra parte, se incluyó de forma implícita en su párrafo primero “*obligaciones jurídicas derivadas directamente del Derecho Internacional y no de un Tratado del que sean partes, por lo que las medidas que los Estados miembros puedan decidir para situaciones de excepción o de emergencia serán acordes con las obligaciones que adoptaron en las cuestiones de Derechos Humanos, impuestas por el Derecho Internacional*”.

2.2. La Informática y el cambio en los sistemas de información a partir de 1960.

En el Diccionario de la RAE el término informática se define como: “*Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores*”⁶². En Alemania se dio como origen de este término la unión de dos palabras: *Information* y *automatik*: *Informatik*, Información automática. Según la tradición, más tenida como cierta que contrastada, la expresión se creó por un ingeniero eléctrico, *Karl Steinbuch*, en 1957, al escribir un documento con ese título: “*Informatik, automatische Informationsverarbeitung*” (“Informática, tratamiento automático de información”). Pero existen otras versiones, rusa, inglesa, francesa o norteamericana que se adjudican con el mismo procedimiento la palabra informática.

vicciones individual o colectivamente, en público o en privado, por medio del culto, la enseñanza, las prácticas y la observancia de los ritos”.

⁶¹ CARRILLO SALCEDO, J., *Soberanía de los Estados y Derechos Humanos en Derecho internacional contemporáneo*, Madrid, 2001.

⁶² Diccionario de la Real Academia de la Lengua Española REAL ACADEMIA ESPAÑOLA, ., *Diccionario de la Real Academia Española*, España, 2012. No se va a entrar a considerar una historia de la informática porque no procede. Se apunta, eso sí, la definición de la RAE.

Fue a partir de los años 50 del pasado siglo XX cuando la información de todo tipo y carácter comienza a tener una relevancia de dimensiones nunca pensadas hasta entonces. Algunos autores destacan la importancia de la situación geopolítica del momento (Guerra Fría, regímenes políticos diversos en el mundo (parlamentario, presidencialista, monárquico, entre otros), capacidad de expansión por medio de la información, control de los gobiernos, sistemas financieros, sistemas de defensa. Lo más relevante de todo ello fue la creación de unas máquinas que son capaces de almacenar y tratar a gran velocidad importantísimas cantidades de datos. ¿Y qué es un dato? La RAE vuelve a definir, de forma muy interesante, el término dato como antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho. En otra acepción es un documento, testimonio, o fundamento. En su relación con la informática, dato es información dispuesta de manera adecuada para su tratamiento por un ordenador. En la terminología de la ingeniería informática, un dato es la unidad indivisible y con significado de información.

Los datos muchas veces de forma individual no tienen relevancia, pero todos juntos en referencia a un individuo, como un mosaico o *puzle*, marcan lo que se denominó *perfil* de información referente a una persona, lo que estará en completa conexión con el Derecho, y junto con el Derecho, los regímenes políticos, los Derechos Fundamentales y la Constitución de cada país.

Por ejemplo, el nombre de una persona (Antonio) por sí mismo, no tiene mucha relevancia para el Derecho. Pero unido a sus dos apellidos, ya tiene un peso legal, un significado para el Derecho: la información sobre una persona (individual y única, como es siempre la persona). Si añadimos algún dato más, la raza, blanca, negra o asiática, el sexo, hombre o mujer, la profesión, el domicilio, el estado civil, la relevancia cobra más fuerza: no vemos al individuo, pero podemos diferenciar más sobre él. Si seguimos añadiendo más datos sobre este individuo, sobre todo datos visuales, tenemos información suficiente para identificarle e incluso localizarle reduciendo la dificultad a la ejecución de la búsqueda física, porque todo lo demás, muy posiblemente se puede saber sin su presencia, sin conocerle físicamente.

Todo este cambio de formas de proceder (el *procedimiento o tratamiento* de datos personales) llamó la atención rápidamente de la doctrina y motivó diversa jurisprudencia. Se generó un vacío legal en Europa que los gobiernos quisieron subsanar mediante las normas. Las regulaciones normativas fueron muy por detrás de los cambios y las consecuencias de los avances tecnológicos. Hasta entonces los datos personales se habían buscado, tratado y almacenado, pero sin conciencia de su determinación e influencia en los DDFF. A partir de la llegada de los medios automatizados de tratamiento de datos, se comenzó a intuir la posibilidad de la generación de un nuevo derecho fundamental: *la protección de datos personales*.

2.2.1 Resolución 509 de la Asamblea General de Consejo de Europa, sobre *Los Derechos Humanos y los nuevos logros científicos y técnicos* de 1968.

En 1968 IBM produjo el primer sistema de gestión de bases de datos, tanto técnicos (contabilidades, mercantiles, financieros, industriales) como personales. Fue cuando autores norteamericanos como MILLER o WESTIN reaccionaron hacia lo que consideraron un uso de la técnica que podría lesionar los DDHH, al vulnerar aspectos de la privacidad e incluso de la intimidad de las personas⁶³.

En Europa, el Consejo constituyó en 1967 una comisión consultiva para el estudio de las tecnologías de la información y su posible uso lesivo de los derechos personales o individuales. Este trabajo se plasmó en una corta Resolución, la 509 de la Asamblea del Consejo de Europa. La citada Resolución se centra en el derecho a no sufrir injerencias en la vida privada, ante el peligro de violación de los mandatos contenidos en el artículo 8 de la Convención Europea de Derechos Humanos⁶⁴. Es relevante leer expresiones como en su punto 2: “Teniendo en cuenta los graves peligros para los derechos de la persona inherentes a ciertos aspectos del desarrollo científico y tecnológi-

⁶³ REBOLLO DELGADO, L., *Vida privada y protección de datos en la Unión Europea*, Madrid, 2008.

⁶⁴ La aludida Resolución puede ser objeto de consulta en la página web del Consejo de Europa (*Council of Europe*) <http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta68/EREC509.htm>

co moderno” O en su punto 3: “Crear que las técnicas desarrolladas recientemente, como las grabaciones telefónicas, las escuchas, la observación subrepticia, el uso ilegítimo de estudios estadísticos y similares métodos para obtener información privada, la publicidad subliminal y la propaganda son una amenaza para los derechos y libertades de las personas y, en particular, para el Derecho a la Privacidad, que está protegido por el artículo 8 del Convenio Europeo de Derechos Humanos” Cuando se aprobó esta Resolución, avance de otras, estaban en pleno funcionamiento todos los desarrollos tecnológicos que se consideraban dañinos o que atentaban contra la privacidad. El daño ya se había producido, pues el uso indebido de los avances tecnológicos no se presentó como previsible ante las sociedades. El Estado trataba datos con finalidades afines a sus competencias, sin mayor consideración. Junto al Estado, sólo las grandes empresas podían obtener y utilizar la tecnología para el tratamiento automatizado de datos, debido a sus costes.

2.2.2 Resolución del Comité de Ministros de 1973, *sobre la protección de las personas respecto a los bancos de datos electrónicos en el sector privado.*

La Resolución del Comité de Ministros del Consejo de Europa de 1973 trató la protección de los ciudadanos ante el uso de datos personales en el sector privado⁶⁵. Se recomendaba a los Estados miembros la regulación a través de medidas legislativas de protecciones y precauciones para que no se hiciera un uso indebido o se abusara de los datos personales. Esta resolución se basa, como dice su texto, en la Resolución nº 3 adoptada por la Séptima Conferencia Europea de Ministros de Justicia.

La Resolución del 73 recomendaba a los Estados miembros una serie de principios aplicables mediante todas las medidas que se consideren necesarias. Los principios se enunciaban en un Anexo y eran de aplicación a la toda la información relativa a las

⁶⁵ MINISTERIO DE JUSTICIA, ., *Resoluciones del Comité de Ministros del Consejo de Europa*, Madrid, 2014.

personas que se hallara registrada en bancos de datos electrónicos (en soporte electrónico, diríamos hoy) del sector privado (empresas, profesionales, se puede entender)⁶⁶. El texto del Anexo contiene el inicio de lo que después se entenderá como Principios de protección de datos de carácter personal. Por ejemplo, la exactitud de la información registrada, que sea adecuada y pertinente, la definición de la finalidad, el derecho de acceso a la información registrada, la autorización de la cesión de la información, la necesidad de los sistemas de seguridad en los denominados en aquel momento bancos electrónicos para evitar el acceso indebido a la información contenida en ellos o la detección de su desvío, con un acceso limitado, de acuerdo al secreto profesional. Se comenzaron a perfilar las ideas de protección de datos para preservar la privacidad y la intimidad de las personas y se invitó a los Estados para que legislaran en consecuencia a estos principios básicos.

2.2.3 La Resolución del Comité de Ministros de 1974, *sobre la protección de las personas respecto a los bancos de datos electrónicos en el sector público*.

Un año más tarde, en 1974, el Comité de Ministros aprobó otra Resolución, esta vez destinada al sector público (Administración y Autoridades Públicas) La Resolución reconoció que se era *“consciente de que la utilización de los bancos de datos electrónicos por las autoridades públicas ha suscitado en la opinión pública una mayor sensibilización respecto a la necesidad de proteger la vida privada de los individuos.”*

La protección de la vida privada frente a las Administraciones Públicas (AAPP) y las autoridades forma parte de varios episodios comentados en las breves alusiones histó-

⁶⁶ En esta Resolución se dieron las primeras definiciones de lo que después se plasmará en leyes y reglamentos. Por ejemplo, se recomienda lo siguiente: “A efectos de la presente Resolución, se entenderá por “informaciones relativas a las personas” (comillas del texto) la información referente a las personas físicas, y por “banco de datos electrónico” todo sistema de tratamiento electrónico de la información que se utilice para gestionar información relativa a las personas y para difundirla”

ricas anteriores. El enfrentamiento de lo *público* como Administración estatal y lo *privado* como ámbito individual del que sólo la persona controla su gestión fue, ha sido (y es) una constante. En el año 1974 se recomendó, recordando la Resolución de 1973, anteriormente tratada, los principios que esta vez también se plasmaron en un Anexo. Las diferencias no fueron destacables. Una relevante a comentar son las recomendaciones del punto 3 en referencia a la situación en que *los bancos de datos electrónicos traten información relativa a la intimidad de la vida privada de las personas, o cuando el tratamiento de las informaciones pueda dar origen a discriminaciones, La creación de los mismos deberá ser prevista por la ley o por una reglamentación especial, o su existencia deberá hacerse pública en una declaración o en un documento, de conformidad con el sistema jurídico de cada Estado miembro. Dicha ley, reglamentación, declaración o documento deberán precisar la finalidad del registro y de la utilización de la información, así como la condiciones en que ésta podrá ser facilitada dentro del sector público o a personas u organismos privados; en particular, cuando La información registrada no deberá utilizarse para fines distintos de los que se hubieran definido, salvo que la ley autorice expresamente una excepción, que una autoridad competente la conceda o que se modifique las normas por las que se regula la utilización del banco de datos electrónico.* Por este texto, la utilización (tratamiento) de datos personales en *bancos de datos electrónicos* se sometió directa y más concretamente a la ley, a la creación de leyes en los distintos países, de manera expresa y detallada. Fue un indicio claro del futuro reconocimiento como derecho fundamental a la protección de datos, pues como tal derecho fundamental tiene reserva de Ley Orgánica en los países democráticos, bajo el control parlamentario de los representantes de la ciudadanía.

2.2.4 La regulación en leyes nacionales de los Estados Miembros del entonces Mercado Común Europeo a partir de 1970. Visión general.

Tanto el Consejo de Europa como la Unión Europea nacieron con ambiciones de futuras regulaciones en Derecho positivo de los diferentes Estados miembros, no sólo como fuentes de principios enunciados que no tuvieran relevancia efectiva para los ciudadanos de Europa. El tránsito fue lento, pero imparable.

En cuanto a las tecnológicas de la información, en 1973 se produjeron dispositivos nuevos para guardar gran cantidad de información por la empresa estadounidense IBM, al igual que Xerox en 1974, con Bob Metcalfe, crea *Ethernet*, una metodología para conectar computadoras, antecedente de internet.⁶⁷ En estos años las normativas sobre protección de datos se continuaron dirigieron a las Administraciones Públicas más que a los entes privados⁶⁸. La razón, ya comentada, se puede encontrar en el coste de las máquinas que hacían posible el almacenamiento de las bases de datos y su tratamiento, el cual era muy elevado, aparte del coste del personal que podía mantener tales sistemas, que era en aquellos años un número de personas especializadas muy reducido y de alta remuneración económica. Otro punto en común se encontró en la creación de instituciones independientes encargadas del control y del cumplimiento de las normativas sobre protección de datos, las cuales solamente se presentaban a rendir informes ante el Parlamento correspondiente, manteniendo un nivel muy alto de conocimiento sobre la evolución tecnológica y la vigencia de los DDFF. Las primeras normas europeas en relación a la protección de datos se produjeron en el *Land* alemán de Hessen, fue la primera *Datenschutzgesetz* (Ley de Protección de Datos) no sólo de Europa sino también del mundo⁶⁹. Aunque bajo los principios actuales faltaban algunas referencias, fue de gran importancia. Esta ley entró en vigor en octubre de 1970. Regulaba las relaciones entre la Administración (en este caso, el *Land* de *Hessen*, los municipios y entidades locales, así como personas jurídicas de Derecho Público) y los particulares, personas físicas, respecto a los bancos de datos que la misma Administración Pública creaba y administraba de forma automática a través de los mecanismos informáticos. La primera Ley de protección de datos alema-

⁶⁷ NORTON, P., *Introducción a la Computación*, México, 2006, pág. 584-585.

⁶⁸ REBOLLO DELGADO, L., *Vida privada y protección de datos en la Unión Europea*, Madrid, 2008.

⁶⁹ SCHILD, H., *Hessisches Datenschutzgesetz. Kommentar.*, Wiesbaden, 2009.

na con carácter federal se promulgó en 1977. Es la denominada *Bundesdatenschutzgesetz*, Ley Federal de Protección de Datos. Se estableció una normativa general relativa al tratamiento de datos personales, independientemente de que se verificara en el sector público o privado. La norma alemana fue posterior a la ley de otro país europeo, Suecia, el cual en 1973 promulga la *Data Lag 1973/289*, por la cual Suecia reguló un sistema de registro abierto para publicitar los bancos de datos personales relativo a personas físicas realizado por medios automatizados, los que debían ser previamente autorizados para funcionar, asociado a una autoridad de control, la *Datainspektionen*, expresión del *Ombudsman* (Defensor del Pueblo, en España) proyectado al tratamiento de datos que vela por el respeto a la ley, con facultades inspectoras, normativas y procesales para requerir la aplicación judicial de sanciones. Esta ley se considera la primera que regulaba la Protección de Datos a nivel nacional. La primera regulación francesa fue promulgada en 1978⁷⁰. Se denominó *Loi n.º 78-17 du janvier, relative à l'informatique, aux fichiers et aux libertés*, Ley relativa a la informática, los ficheros y las libertades que instituyó una autoridad independiente encargada de su cumplimiento. Se realizó como respuesta a la inquietud de la opinión pública a raíz de la publicación en la prensa francesa de un proyecto gubernamental de interconexión de bases de datos en la Administración Pública (se conoció como *proyecto SAFA-R*) para generar un número de identificación de cada ciudadano. La ley delimitó el ámbito de la administración en esta materia. También creó un órgano de control, la *Commission Nationale de l'Informatique et des Libertés*, que se encargó de la correcta aplicación de la Ley y de recibir las reclamaciones de los afectados con potestad reglamentaria. Se menciona también la Ley de registros privados y Ley de registros públicos de Dinamarca, 1978; la Ley de protección de datos de Austria, 1978; ese mismo año de 1978 nace la Constitución Española, objeto de estudio de esta tesis en

⁷⁰ TÜRK, A., *La ley francesa de protección de datos de carácter personal*, Santander, 2005, Agencia Española de Protección de Datos. Alex Türk, Presidente de la Comisión Nacional de Informática y Libertades (CNIL) Francia

su epígrafe correspondiente; y se nombra la Ley sobre utilización de datos en tratamientos informáticos de Luxemburgo, 1979⁷¹.

2.2.5 Resolución del Parlamento Europeo, de 8 de mayo de 1979, sobre *la tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática*

En esta Resolución⁷² se confirmó la expresión Protección de Datos en su punto 4 expresando en inglés el siguiente texto:

"Calls once again on the Commission to prepare for a Directive on the harmonization of legislation on data protection to provide citizens of the Community with the maximum protection;"

Es curioso el punto 2 del texto el cual expresa su intención de "señalar que las disposiciones nacionales para proteger la privacidad tienen una directa influencia en el establecimiento y funcionamiento del mercado común y, en particular, distorsiona las condiciones de la competencia"⁷³

La influencia de la interrelación entre los Estados miembros del entonces Mercado Común se veía afectada por la legislación de los Estados miembros sobre la privacidad y la protección de datos. Eran diferentes visiones y diferentes legislaciones que impedían una visión y un funcionamiento más en conjunto y más simple de las relaciones

⁷¹ SERRANO PÉREZ, M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, 2003. La autora realizó una tesis doctoral sobre el derecho a la protección de datos desde una perspectiva de derecho comparado, donde se amplían todos estos aspectos. Aquí sólo se han reseñado como antecedentes de la situación actual.

⁷²El texto completo se puede consultar en:

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOC_1979_140_R_0015_01&from=EN a 11 de diciembre de 2014.

⁷³ *"Points out that national provisions to protect privacy have a direct influence on the establishment and operation of the common market and, in particular, distort the conditions of competition"*

comerciales entre los Estados miembros. En ese momento se comenzó a vislumbrar la relación entre datos personales, la economía y la política, cuando los poderes públicos y las empresas en común tratan y analizan gran cantidad de datos con vinculaciones de todo tipo: personales, económicos, de consumo o de finanzas.

3. El derecho a la Protección de Datos Personales como Derecho autónomo respecto al Derecho a la intimidad y a la privacidad.

En los inicios de la década de los años 80, se pusieron en marcha las primeras regulaciones nacionales que positivizaban el derecho de la persona a no sufrir injerencias de terceros en su vida privada y a su intimidad a través de las nuevas tecnologías de la información. El sector tecnológico avanzó a gran velocidad a lo largo de pocos años. La regulación era una necesidad creciente, como consecuencia de la expansión de los llamados PC u ordenadores personales, que abarataron increíblemente el almacenamiento y tratamiento de datos⁷⁴. Se añadió al avance tecnológico las primeras redes de conexión de datos al margen del sector de la Administración Pública (en principio empresas de un volumen apreciable, más tarde, todo tipo de empresas y particulares). Todavía no se había creado *internet*, pero existía una creciente expansión de los medios de comunicación de datos, sin ningún tipo de regulación.

La realidad no era sólo un asunto doctrinal. Se debía configurar un Derecho a la protección de datos personales, independiente del Derecho a la intimidad y al Derecho a la privacidad, los cuales ya estaban regulados en todas las legislaciones occidentales, tanto civil como penalmente e incluso en sus Constituciones. Estas regulaciones, que

⁷⁴ Fue en 1980 cuando IBM eligió a Microsoft como proveedora del sistema operativo de su Personal Computer (PC). En 1981 IBM presentó el IBM-PC. Junto a esta empresa, Xerox presentó la computadora Xerox Star, con el primer mouse. Aunque fue un fracaso comercial, sirvió de base a posteriores diseños de otras compañías, como el PC Lisa de Apple, con el primer sistema operativo gráfico y un mouse (ratón). Su precio de 10.000\$ hizo que no se extendiera su uso en el mercado. El PC con más éxito en 1983 fue el portátil de Compaq, aunque pesaba 13 kg. IBM no generó un portátil hasta 1996. Referencias en NORTON, P., *Introducción a la Computación*, México, 2006, pág. 587-590.

se van a nombrar como clásicas, de la intimidad y de la privacidad, es obvio que no funcionaron con los nuevos hechos provocados por el avance tecnológico; de otra forma, si hubieran funcionado efectivamente, aún con adaptaciones, no hubiera sido necesario un nuevo enfoque de los diferentes conflictos de intereses que se producían más allá de las posibilidades de legisladores y jueces para visionar las consecuencias de tales hechos. La doctrina analizó un nuevo fenómeno social e incluso un nuevo fenómeno de civilización, no previsto inicialmente, que debía categorizarse jurídicamente por legisladores y juristas en el sistema europeo de normas.

Existían nuevos objetos y sujetos de derechos y obligaciones que demandaban estudios sobre lo que realmente se producía al aplicar las avanzadas tecnologías, de continuo, cambiantes. A principios de la década de los ochenta el hardware y el software sufren tan extremo ritmo cambiante que las innovaciones sólo duraban meses antes de que se quedaran obsoletas. Entonces, una gran parte de los ciudadanos todavía había vivido la II Guerra Mundial y no comprendió la transcendencia de los sistemas de información ni por supuesto vieron sus consecuencias. El legislador estaba atento a otras cuestiones, como la Guerra Fría, la salida de la crisis de los años setenta, los cambios sociales en países como España, entre otros fenómenos históricos. Aun así, como se va mostrando, la preocupación por la protección de datos fue constante. En ese momento histórico, se entendía como protección de datos la protección que se aplicaba a los datos en sí mismos, a nivel tecnológico, para evitar su pérdida y alteración por procedimientos propios de la técnica. Con el paso de la experiencia, se referían también a la protección de datos para evitar su uso indebido, su mal uso, por terceros con intenciones distintas a las que deben ser originarias en el momento de su almacenamiento en bases de datos. Se trataba de un conjunto de medidas a nivel técnico, que siguieron avanzando según se sofisticaban los sistemas informáticos y de comunicaciones de datos. Ese grupo de medidas son la protección efectiva y real de los datos personales: la seguridad técnica de datos.

El avance tecnológico evidente produjo dos consecuencias en continua relación. Por una parte, los DDFF resultaron afectados negativamente, como un daño colateral no contemplado. Por otra parte, se interpretaron los derechos tradicionales desde otra

perspectiva. La doctrina comienza a debatir sobre el Derecho a la intimidad, el Derecho a la privacidad y la aparición de nuevas expresiones y conceptos jurídicos⁷⁵, llamados autodeterminación informativa, iusinformática, iuritécnica, libertad informática, Intimidad Informática, informática jurídica, entre otras expresiones⁷⁶. Es la positividad del fenómeno social del uso de datos personales en normas nacionales de los Estados lo que condujo a la generación del Derecho a la protección de datos con significado autónomo frente al Derecho a la intimidad y al Derecho a la privacidad. La naturaleza del Derecho a la protección de datos, que reguló una realidad social siempre por delante de las normas jurídicas, junto con la especificidad de los derechos afectados con el hecho del avance de la Informática, hacen que este Derecho a la protección de datos tenga una naturaleza jurídica que MARTÍNEZ MARTINEZ⁷⁷ define como

⁷⁵ LÓPEZ-MÚÑIZ GOÑI, M., *Informática Jurídica Documental*, Madrid, 1984.

⁷⁶ Las expresiones utilizadas por la doctrina jurídica para el nuevo hecho de la protección de datos personales no han sido objeto de análisis. Interés puede tener conocerlas y también nombrar algunos de los autores que han intervenido en su formulación. Entre otros:

LEE LOEVINGER, abogado norteamericano, (1949) emplea el término “*Jurimetrics: the next step forward*” teniendo este concepto como medida del derecho para la información jurídica.

HANS BAADE (1963) utiliza la expresión y los conceptos de la Jurimetría para establecer un sistema acorde con el Derecho anglosajón de precedentes y soluciones. Pronto esto se ve desbordado por los hechos sociales. No era un sistema inteligente, como los conocidos en la actualidad, pero se considera como su antecedente.

MARÍO LOSANO (1966) en Italia, con el estudio “*Giuscibernetica, in Nouvi sviuppi della sociología del diritio*”; Vittorio Frosini (1968) “*Cibernetica, diritio e societa*”. Ambos utilizan los términos “iuscibernética”. Frosini utiliza también el término “Juritecnica”.

El Profesor LÓPEZ-MUÑOZ GOÑI en su obra citada LÓPEZ-MUÑOZ GOÑI, M., *Informática Jurídica Documental*, Madrid, 1984. de los años 80 desarrolla la idea de iusinformática, generando lo que denomina “Informática Jurídica documental”, pues centra su idea en la documentación producida por los poderes públicos, las relaciones interpersonales o de los ciudadanos con el Estado, en variados negocios y obligaciones jurídicas.

El Profesor Miguel DAVARA RODRIGUEZ, con una extensa bibliografía sobre lo que denomina *informática Jurídica* junto con otras expresiones, generó su *Manual de Derecho informático* en 1993.

⁷⁷ MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Madrid, 2004. Ricard Martínez fue responsable del área de estudios de la AEPD.

derecho de la personalidad, connatural e innato, subjetivo, privado, oponible erga omnes, inherente a la persona, intrasmisible, indisponible, imprescriptible, inembargable, irrenunciable y necesario para el desarrollo de la personalidad. DÍEZ PICAZO⁷⁸ lo considera también un Derecho Fundamental autónomo, independiente de otros Derechos. Otros autores, como REBOLLO DELGADO, tienen una posición más crítica, y para ellos el llamado Derecho a la protección de datos personales no es más que una prolongación del Derecho a la intimidad⁷⁹.

La intimidad, interpretada y sentida de forma diferente según las civilizaciones, se entiende, sin embargo, bajo el concepto común de ámbito interior al ser humano, que genera un respeto ante terceros. Es, como se ha visto, el ámbito de los sentimientos, los pensamientos y acciones que no se desean compartir más que con los más próximos o con nadie. La privacidad, como también se ha distinguido, consiste en un grupo de derechos, considerados fundamentales (libertad de expresión, libertad de asociación, libertad de culto religiosos, de afiliación política o sindical, respeto a la propia residencia, respeto a la familia, entre otros) y dignos igualmente del respeto ante terceros y de una protección adecuada. La protección de datos personales, aunque se inició como protección a la intimidad y a la privacidad, como expresión de derechos más tradicionales, tiene una forma de manifestarse diferente, pues confluyen elementos técnicos que antes no se producían. Son las ilimitadas posibilidades de captar, guardar, relacionar, conservar y transmitir todo tipo de información personal. El tratamiento de datos personales se daba antes por cualquier soporte no automatizado. Lo novedoso del avance técnico es su accesibilidad. Es más, se comienza a considerar que la violación del derecho a la protección de datos afecta a otros ámbitos del Derecho y a otros Derechos Fundamentales, por tanto, al regular y proteger los datos personales se está generando la efectividad de los mandatos implícitos en otros derechos fundamentales y se están protegiendo de su violación.

⁷⁸ DÍEZ PICAZO, L., *Sistema de Derechos Fundamentales*, Madrid, 2003.

⁷⁹ REBOLLO DELGADO, L., *El Derecho Fundamental a la Intimidad*, Madrid, 2000; 2ª Edición 2005.

En Alemania se produjo en 1983 la expresión *Derecho a la autodeterminación informativa*⁸⁰, más encaminado a la diferenciación de este Derecho como opuesto al Derecho a la información. La expresión autodeterminación informativa es una traducción del alemán en la Sentencia del *Bundesverfassungsgericht* o Tribunal Constitucional Federal de Alemania. Las partes recurrentes ante el Tribunal Constitucional alemán concibieron lo que ocurría desde los más remotos tiempos de la sociedad: lo relevante no es proteger la información personal e íntima de un ciudadano, sino proteger con diversas acciones y abstenciones de terceros aquellas informaciones que debidamente relacionadas con otras puedan revelar variados aspectos de la vida, del comportamiento y de las acciones de un ciudadano. No se discute la cualidad del dato, si es íntimo, privado o no lo es, sino que se discute su tratamiento, en el caso de la Sentencia del Tribunal Constitucional alemán, tratamiento automatizado de los datos del censo de población. Es el hecho de la mecanización a gran velocidad del tratamiento de datos lo que motivó a los recurrentes, no la naturaleza de la información, curiosa-

⁸⁰ MURILLO DE LA CUEVA, P., *Derecho a la Autodeterminación informativa*, Madrid, 2009. *Recht auf informationelle Selbstbestimmung*. Esta expresión proviene de la doctrina alemana a través de la Sentencia (*Urteil*) de su Tribunal Constitucional Federal el 15 de diciembre de 1983, sobre un recurso de amparo interpuesto contra la Ley del Censo de Población aprobada por el Parlamento en 1982. El TC alemán expone en la Sentencia que "(...) en las condiciones de la elaboración moderna de datos, la protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitadas de sus datos personales queda englobada en el derecho general de protección de la persona del artículo 2º, párrafo 1º de la Ley Fundamental. El derecho constitucional garantiza en esta medida la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y la utilización de los datos referentes a su persona" (...) "Las limitaciones de este derecho a la "autodeterminación informativa" sólo son admisibles en el marco de un interés general superior y necesitan un fundamento legal basado en la Constitución que debe corresponder al imperativo de claridad normativa inherente al Estado de Derecho." Véase también los breves comentarios de HERRÁN ORTIZ, A., *El derecho a la intimidad en la nueva ley orgánica de protección de datos personales.*, Madrid, 2002, pág. 57-59. En ediciones alemanas existe una gran cantidad de publicaciones sobre el denominado *Recht auf informationelle Selbstbestimmung*, como mencionaba en 2004 BRÖHMER, J., *Transparenz als Verfassungsprinzip*, Tübingen, 2004, pág. 196-199. Sirva decir que Alemania, actualmente, denomina la protección de datos personales con la expresión *Datenschutz* (protección de datos), por lo que también se ha producido una evolución en la definición de 1981 a otra más acorde con los tiempos.

mente, porque en el censo sólo se tratan los datos de nombre y domicilio, junto con quizá otros de estado civil, filiación o profesión. Datos que cualquier persona expone para convivir en sociedad, pues no se consideran íntimos. Al margen del debate doctrinal y del *nomen iuris*, es un hecho que la expresión derecho a la Protección de datos personales se implantó tanto en la legislación como en la jurisprudencia posterior.

3.1. El Convenio 108 del Consejo de *Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981*.

Poco antes de la Sentencia del Tribunal Constitucional alemán mencionada en el epígrafe anterior, el Convenio 108 del Consejo de Europa de 1981 fue la primera norma europea que dirigió claramente el desarrollo posterior de un modelo común de protección de datos. El texto con el que se inicia el Convenio 108 comprometió a los Estados miembros del Consejo de Europa a la aplicación de normas de protección de datos, conforme a lo estipulado en el Convenio Europeo de Derechos Humanos⁸¹. Aña-

⁸¹ Se puede consultar el texto completo en la página web de la AEPD a 20 de diciembre de 2014 http://www.agpd.es/portalwebAGPD/internacional/textosynormas/textos_consejo_europa/common/PDFs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf

En la página del COE también se puede encontrar información sobre este Convenio. http://www.coe.int/t/dghl/standardsetting/DataProtection/Global_standard/D%C3%A9pliant%20Conv108_es.pdf

“Los Estados miembros del Consejo de Europa, signatarios del presente Convenio.

Considerando que el fin del Consejo de Europa es llevar a cabo una unión más íntima entre sus miembros, basada en el respeto, particularmente de la preeminencia del Derecho así como de los Derechos Humanos y de las Libertades Fundamentales; considerando que es deseable ampliar la protección de los Derechos y de las Libertades Fundamentales de cada uno, concretamente el Derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados. Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras. Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre

dió garantías en la cesión de datos transfronterizos entre países, aunque estos no pertenecieran al Consejo de Europa, al estar abierta la adhesión incluso a países no europeos, para asegurar un nivel de protección óptimo y con carácter universal. El Convenio 108 definió claramente el Derecho a la Protección de datos personales como un Derecho que está en conexión directa con otros DDFF, concretamente el Derecho a la vida privada, pero también se afirmó que derechos como la libertad de expresión o la libertad de conciencia, las convicciones políticas o religiosas, o los orígenes de la persona, están fuertemente ligados en su ejercicio con el Derecho a la Protección de Datos personales.

El artículo 5 del Convenio 108 estableció los principios de una adecuada protección de datos, como son la finalidad determinada para su obtención y uso, el almacenamiento de datos sólo para esa finalidad, la exactitud y la actualidad o la conservación de los datos se mantendría solamente durante el tiempo necesario para cumplir esa finalidad.

El artículo 6 del Convenio 108 definió a lo que denominó *categorías particulares de datos*: se trata de datos que podrían revelar el origen racial, las opiniones políticas, las convicciones religiosas, relativos a la salud, a la vida sexual o a información referente a cuestiones penales. En 1981 se reconocía que este tipo de datos no podría tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. Además, el artículo 7 estableció la necesidad y obligatoriedad de medidas de seguridad y alude a ficheros automatizados. El artículo 8 estableció una serie de derechos para el titular de los datos. Concretamente reguló que cualquier persona podría conocer la existencia de un fichero automatizado, la finalidad y la identidad junto con la dirección de lo que el Convenio llama *autoridad controladora del fichero*, la

circulación de la información entre los pueblos, Convienen (...) Artículo 1. Objeto y fin. El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus Derechos y Libertades Fundamentales, concretamente su Derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos).”

actual denominación de esta figura es el responsable del fichero; igualmente los ciudadanos podrían obtener la confirmación de la existencia de datos personales que le conciernan, en forma inteligible, el actual *derecho de acceso*; podría obtener, si procede, la rectificación de esos datos, claramente el *derecho de rectificación* y, por último, disponer de un recurso en caso de no ser atendidas sus peticiones. El capítulo III se tituló *flujos transfronterizos de datos*, iniciando así la regulación de la transmisión de datos personales entre países, dentro de la CEE. El capítulo V estableció la creación de un Comité Consultivo, compuesto por representantes de cada Estado miembro del Consejo de Europa. En caso de no ser miembro del Consejo, se podría designar un observador para las reuniones. El Comité Consultivo sometería la memoria de sus trabajos y funciones al Comité de Ministros del Consejo de Europa después de cada reunión.

3.2. La Recomendación de la Comisión Europea 81/679/CEE, de 29 de julio, relativa al Convenio del Consejo de Europa 108 y la recomendación de su firma y ratificación por los Estados miembros.

La Recomendación de la Comisión Europea en los primeros años de la década de los ochenta recogió la visión de la todavía Comunidad Europea sobre la protección de datos personales⁸². En una sintética redacción de cinco puntos, la Comisión puso de manifiesto que el tratamiento electrónico de datos personales y su uso en la vida privada conllevaría el peligro de su utilización abusiva. La vida privada exigía (el texto utiliza este verbo) que la protección de datos personales se ampliara. Calificó la protección de datos personales en el punto 2 como *elemento necesario de la protección del individuo y constituye uno de sus Derechos Fundamentales*. Como se observa claramente, se estableció en ese momento como fundamental el derecho a la protección de datos personales. Así mismo, calificó de deseable que todos los Estados miembros de la Co-

⁸² El texto completo se puede obtener a 20 de diciembre de 2014 en la dirección <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31981H0679&from=ES>

munidad Europea realizaran una aproximación normativa en cuanto a la protección de datos personales. La Comisión dio un plazo, fin de 1981, para que los Estados Miembros firmaran el Convenio 108 del Consejo de Europa y lo ratificasen antes del fin de 1982. Como indica el final del punto 5, si los Estados Miembros no llegaran a firmar y ratificar este Convenio 108, la Comisión se reserva el derecho de proponer al Consejo que adopte un acto diferente, dentro del Tratado de la CEE⁸³.

La Protección de Datos personales se vuelve a tratar en 1990, muchos años después. Concretamente la Comisión emitió una Comunicación en la que hace notar el obstáculo que supone la divergencia de enfoques en materia de protección de datos personales dentro del mercado interior y expresó el deseo de superarlos. En el mes de julio de 1990 se presentó una propuesta de Directiva del Consejo para aproximar las disposiciones legales de los Estados Miembros en referencia a la protección de datos personales y su tratamiento. Después de estudios y discusiones en el Parlamento Europeo, se aprobó el texto de la Directiva 95/46/CE.

3.3. La Directiva 95/46/CE, de 24 de octubre, *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*.

Como se observa, desde 1973 las autoridades europeas estuvieron interesadas en una normalización, unificación de criterios o armonización de las diferentes legislaciones en materia de protección de datos personales, para poder atender las necesidades de la CEE y la libre circulación de personas y capitales. Las nuevas tecnologías de los primeros años hicieron también posible un transporte electrónico de información (flujo de datos), directamente implicado en la gestión empresarial y personal de todos los sectores económicos afectados: desde la gestión de contratos (mercantiles y labo-

⁸³ Los Estados miembros no lo ratificaron dentro de ese plazo.

rales, sobre todo) hasta sectores como el de seguros o transporte, determinantes en las relaciones empresariales.

El más importante pronunciamiento fue el Tratado de la Unión Europea en Maastricht, firmado el 7 de febrero de 1992. En este Tratado se incorpora la Doctrina elaborada por el Tribunal de Justicia de las Comunidades Europeas (en adelante, TJCE) sobre los Derechos Fundamentales como parte del ordenamiento de la Unión a través de los Principios Fundamentales del Derecho. Interesa la incorporación de los Derechos Fundamentales al Tratado de la Unión Europea. En el Artículo 6 del Tratado de Maastricht se estableció que la Unión se adhiriera al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. La adhesión no modificaría las competencias de la Unión que se definían en los Tratados. Reforzando los DDFF que garantiza el Convenio Europeo para la Protección de los Derechos humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales⁸⁴. Existía, por tanto, la obligación de garantizar los Derechos Fundamentales en todos los países miembros de la Unión, incluido el derecho a la protección de datos personales. Posteriormente a 1995 se realizaron más modificaciones al Tratado de Maastricht, que fueron reconocidas también en el artículo 6 del mismo.

El avance en los medios tecnológicos fue imparable a partir de 1990. Se piensa que es precisamente el auge de *internet* en esos años, junto con una total extensión del ordenador personal, lo que impulsa definitivamente la aprobación de una legislación de mínimos para la protección de datos personales en la Unión Europea⁸⁵. La información

⁸⁴ Texto completo a 3 de enero de 2015 en <http://www.boe.es/doue/2010/083/Z00013-00046.pdf> Es una versión consolidada. Existen otras versiones como la que se puede leer en http://europa.eu/eu-law/decision-making/treaties/pdf/treaty_on_european_union/treaty_on_european_union_es.pdf más cercano al original, pero menos actual.

⁸⁵ Es en 1991 cuando Tim Berners-Lee genera el Hipertexto, creando el *World Wide Web* conocido por todos como *www.*, para interactuar con Internet junto con los protocolos de transmisión *http//*, el concepto de URL y el lenguaje de documentos HTML. En 1995-96 Microsoft, líder en el mercado como compañía proveedora de software, lanza Windows 95 con un navegador web predeterminado, el *Explorer*. NORTON, P., *Introducción a la Computación*, México, 2006, pág. 592-595.

se identificó siempre con el poder, pero con los sistemas informáticos, la información puede ser transmitida e interpretada con suma facilidad y rapidez⁸⁶. La tecnología informática y de las telecomunicaciones fue la causa del progreso económico, cultural y, por tanto, social, de nuestro tiempo. Junto con la posible vulneración de los derechos individuales fundamentales, la humanidad se encontró con un enriquecimiento humano y social sin precedentes, en sentidos impensables después de la II Guerra Mundial⁸⁷.

Así pues, en ese momento temporal, dos intereses contrapuestos se analizaron. Por una parte, el Derecho Fundamental a la Protección de datos personales, para el que los avances tecnológicos supusieron un riesgo o una amenaza efectiva anterior y posteriormente al año 1995. Por otra parte, la Unión Europea en sus inicios promovió la libertad del mercado interior, y, por tanto, los datos personales debían circular sin barreras entre los países miembros, que aceptan la libre circulación de personas y capitales. La solución a este conflicto de intereses se encontró en los límites al denominado *poder de la informática* (uso o tratamiento de datos personales, en especial por medios automatizados) con dos fórmulas apreciables en toda la Directiva 95/46/CEE, de 24 de octubre de 1995: por una parte, generando obligaciones al responsable del tratamiento de los datos personales y por otra, generando derechos expresos al titular de los datos⁸⁸. Ya no se habló únicamente de respeto a la intimidad

⁸⁶ PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010, pág. 361. : “En nuestra época se ha adquirido plena consciencia de que la información es poder y que ese poder se hace decisivo cuando, gracias a la informática, convierte informaciones parciales y dispersas en informaciones en masa y organizadas.”

⁸⁷ Siempre se trataron datos personales, pero nunca se habían unido a un régimen de garantías para asegurar al ciudadano la correcta utilización de la información personal, respetando en todo momento sus derechos fundamentales. Quizá fue también la sensibilidad de los años posteriores a la II Guerra Mundial lo que motivó otra visión de la información que hasta entonces no se había producido. Aun así, como se expone en esta tesis, los Estados se resisten a aplicar la garantía de protección de datos.

⁸⁸ El texto completo de la Directiva se puede leer a 15 de enero de 2015 en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/comun/pdfs/B.4-cp--Directiva-95-46-CE.pdf Toda la doctrina se manifiesta sobre estas dos ideas fundamentales. Véase en su temprana tesis doctoral a GARRIGA DOMÍNGUEZ, A., *La protección de datos*

frente a la informática. Se habló también (y se quiso regular legalmente, hasta ese momento sólo habían sido Recomendaciones y Tratados de voluntario cumplimiento) del valor económico de los datos personales y el necesario respeto a los DDFF de las personas. El mercado interior de la Unión y los intereses de las empresas que lo conformaban optaron por el *respeto* en el tratamiento de los datos personales. La Directiva 95/46/CE nació además con una pretensión de permanencia. No es una recomendación, es una imposición legal con plazo; un plazo de tres años para su transposición a las legislaciones nacionales de los Estados miembros (artículo 32 y disposición final 1 de la Directiva 95/46/CE 95). En un nuevo marco territorial, la Directiva 95/46/CE concretó y detalló el Convenio de 1981, con una serie de conceptos comunes para todo el Espacio Económico Europeo (a partir de este punto EEE), tanto a nivel de protección de datos como de respeto a los DDFF⁸⁹.

El Prólogo fue extenso, con un total de 72 Considerandos muy amplios, en los que se delimitan los principios de aplicación de la normativa reflejada en la Directiva 95/46/CE, e incluso criterios de aplicación. Destacan las definiciones de consentimiento, finalidad, tratamiento y seguridad⁹⁰. La Directiva no fue una norma de mínimos como sí lo fue el Convenio del año 81. En su articulado, el artículo 1 define el objeto de la Directiva 95/46/CE como: *1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva 95/46/CE, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. 2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.* Se marcaron dos de los principios que in-

personales en el Derecho español, Madrid, 1999, pág. 295 y ss. También otros autores, como GUERRERO PICÓ, M., *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Navarra, 2006, pág. 63 y ss. REBOLLO DELGADO, LUCRECIO; SERRANO PÉREZ, M^a MERCEDES, *Introducción a la protección de datos*, Madrid, 2008, pág. 44 y ss. entre otros.

⁸⁹ REBOLLO DELGADO, LUCRECIO; SERRANO PÉREZ, M^a MERCEDES, *Introducción a la protección de datos*, Madrid, 2008, pág. 48-50.

⁹⁰ considerandos 31, 33, 40, 39, 38, 46 y 47, entre otros.

terresaban a la Unión: por una parte, *las garantías para los ciudadanos de sus libertades y derechos fundamentales en conexión con el tratamiento de los datos personales*, punto sumamente importante; *por otra no se podía restringir la libre circulación de datos personales entre los Estados miembros*, no dejando a la libre disposición de los Estados miembros el asunto de la protección de datos personales⁹¹.

El artículo 2 mostró las definiciones de términos que después se impondrá en la legislación española de protección de datos personales. Esos mismos términos y definiciones provenían del Convenio 108, pero se resaltaron más. Se destacan por su importancia la definición de datos personales como toda información sobre una persona física identificada o identificable. Esta expresión, *persona física identificada o identificable* se marcó especialmente en la legislación española y en las Resoluciones de la Agencia de Protección de Datos (AEPD) pues se consideró identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. Se abrió en este punto una serie infinita de combinaciones de posibles datos que pueden llevar a identificar a una persona física, generando una visión informativa que podría complementarse con más datos. Otra expresión definida es la de *tratamiento de datos personales*, como cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, 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. El concepto de tratamiento de datos personales utilizado fue sumamente amplio. Ya no se circunscribía únicamente al tratamiento informático o automatizado, sino que se contemplan los tratamientos de datos personales en otros soportes no automatizados, que hasta ahora no se habían tenido en cuenta por los legisladores de

⁹¹ Véase las referencias continuadas a la Directiva 95/46/CE que realizó SERRANO PÉREZ, M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, 2003. en su análisis.

los países de la Unión Europea, los cuales, prácticamente tradujeron la Directiva 95/46/CE para incorporar sus normas en sus ordenamientos internos. Del resto de artículos se puede destacar que estableció conceptos tan importantes como la calidad de los datos, la legitimación del tratamiento de los datos personales, las categorías especiales, el principio de información a los titulares de datos personales afectados por el tratamiento de sus datos, el derecho de acceso, el derecho de rectificación, supresión y bloqueo de datos. También reguló las excepciones y limitaciones al derecho a la protección de datos personales, el derecho de oposición del interesado, la confidencialidad y seguridad del tratamiento, junto con la notificación del tratamiento de datos personales a la Autoridad de control. Se generaron normas para posibilitar el acceso al recurso judicial para el caso de violación de los derechos que se le reconocen al titular de los datos, se reconocieron y regularon los riesgos en las transferencias internacionales de datos personales a terceros países, fuera del EEE (espacio económico europeo), se creó el Grupo para la protección de las personas en lo que respecta a sus datos personales (el denominado Grupo de trabajo del artículo 29, GT29) y se comienzan a definir y promocionar los Códigos de Conducta.

No se va a analizar el Reglamento 45/2001/CE 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 (Diario Oficial L 8 de 12.01.2001)⁹². Ligeramente se comenta que este Reglamento se propuso garantizar la protección de los datos personales en el marco de las instituciones y organismos de la Unión Europea. El texto contempló una serie de disposiciones que garantizaban un nivel de protección elevado para los datos personales tratados por las instituciones y los organismos comunitarios y la creación de una instancia de vigilancia independiente encargada de controlar la aplicación de dichas disposiciones.

⁹² El texto completo se encuentra a 20 de enero de 2015 en http://www.europarl.europa.eu/tools/disclaimer/documents/I_00820010112es00010022.pdf

3.4. El artículo 8.1 de la Carta de Derechos Fundamentales de la Unión Europea, Niza, 7 de diciembre de 2000. El Reconocimiento del Derecho sustantivo, autónomo y fundamental a la Protección de Datos Personales. El Tratado de Lisboa.

La Carta de Derechos Fundamentales de la Unión Europea del año 2000 se considera actualmente una Declaración y no se incluye en el posterior Tratado de Lisboa⁹³. Proclamada en la Cumbre de Niza del año 2000 e incluyéndose esta Declaración anexa al Tratado de Niza, se mantuvo únicamente en proyecto para establecer una Constitución Europea⁹⁴. Tiene por objeto únicamente proteger los derechos fundamentales de las personas frente a actos adoptados por las Instituciones de la Unión Europea y por los Estados miembros en aplicación de los Tratados de la Unión⁹⁵.

El Tratado de la Unión Europea (TUE) tuvo otra revisión en el año 2003 con el Tratado de Lisboa, el cual se firmó el 13 de diciembre de 2007 y entró en vigor el 1 de diciembre de 2009. El Tratado de Lisboa transformó el Tratado de Maanstricht en Tratado constitutivo de la Unión, siendo el propio Tratado de Lisboa una posible Constitución Europea que no ha llegado a ser nombrada como tal por las dificultades en la ratificación que tuvo en Holanda y en Francia en el año 2005.

El Tratado de Lisboa concretó en el artículo 6 que la Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de 7 de diciembre de 2000, tal como fue adoptada el 12 de diciembre en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados. Por tanto, según este artículo 6 del

93 SÁENZ DE SANTAMARÍA, P., "La Carta de los Derechos Fundamentales de la Unión Europea en la práctica española", *Revista de derecho de la Unión Europea*, nº 15, 2008, pág. 233-255.

94 En el posterior Tratado de Lisboa la oposición de Reino Unido de Gran Bretaña y de Polonia generaron la exclusión de la Carta del resto del texto del Tratado de Lisboa, dándose una curiosa fórmula, llamada "incorporación por referencia" a través del artículo 6.1 del Tratado de la Unión Europea (Tratado de Maastricht), lo cual significaba que la Carta "tendría el mismo valor jurídico que los Tratados".

95 A 19 de marzo de 2015 <http://www.europarl.europa.eu/aboutparliament/es/0003fbe4e5/Carta-de-los-Derechos-Fundamentales-de-la-UE.html>

Tratado de Lisboa o TUE, la Carta de los Derechos Fundamentales (o Tratado de Niza) se convierte en un texto jurídicamente vinculante, de obligado cumplimiento en las Instituciones Europeas y por los Estados Miembros para la aplicación del Derecho Comunitario (o Derecho Europeo, como ya se comienza a denominar) en la aplicación de su normativa: Directivas, Decisiones, Reglamentos, Dictámenes o Recomendaciones. Los Tribunales, tanto europeos (Tribunal de Justicia de la Unión Europea -TJUE- Tribunal de Primera Instancia, Tribunal Europeo de Derechos Humanos -TEDH) como nacionales de los Estados Miembros pueden referirse a La Carta (Tratado de Niza) en la protección de los DDHH. El Tratado de Lisboa y su remisión a La Carta en el artículo 6 TUE convirtieron los derechos declarados en el Tratado de Niza en derecho positivo, siendo algo más que normas de interpretación, se considera por la doctrina como norma de tutela de DDFF y de seguridad jurídica para todos los ciudadanos. Esta interpretación se enfrentó con las que consideran que La Carta no es vinculante para los Estados Miembros, teniendo sólo un carácter limitado de interpretación.

La consideración de la doctrina se fundamentó en la ampliación y mejor denominación de derechos ya reconocidos en el año 92. La Carta se mostró igualmente avalada por jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. Lo más interesante a considerar por la doctrina fue la definición de DDFF denominados de nueva generación, entre los que se encuentra en su Capítulo II, de las Libertades, artículo 8, el derecho fundamental a la protección de datos de carácter personal, existiendo en el texto de La Carta una distinción entre vida privada, intimidad y protección de datos⁹⁶.

⁹⁶ El artículo 7 se refiere al respeto de la vida privada y familiar: “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones”. El artículo 8 menciona únicamente la protección de datos de carácter personal, consagrando definitivamente este derecho como autónomo: “1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.”

Existe unanimidad en la doctrina de que la Carta de Niza tiene lo que se ha llamado un *carácter programático*. El Parlamento Europeo considera que, con el Tratado de Lisboa, la Carta de los Derechos Fundamentales adquiere fuerza jurídica vinculante para 25 Estados miembros, mientras que el Reino Unido y Polonia disfrutan de una excepción a su aplicación. La Agencia Española de Protección de Datos (AEPD) menciona la Carta de Niza frecuentemente en su documentación⁹⁷.

El Tratado de Lisboa tiene otras particularidades en las Declaraciones adicionales 20 y 21. En la Declaración Adicional 20 del TUE se refiere a las normas del Tratado de Funcionamiento de la Unión Europea (TFUE) para normas que deban adoptarse con arreglo al artículo 16B del TFUE. Para estos casos, se deben tener en cuenta las *características específicas de la cuestión* en cuanto a Seguridad Nacional de los Estados Miembros, según la Directiva 95/46/CE. El TFUE es el texto más antiguo dentro de la UE. Constituye la configuración material de la UE, junto con el Tratado de la Unión Europea (actual Tratado de Lisboa), la Carta de DDFF de la Unión Europea (Tratado de Niza) y el Tratado Constitutivo de la Comunidad Europea de la Energía Atómica (Tratado Euratom). Se firmó en Roma, en el año 1957 (como Tratado constitutivo de la Comunidad Económica Europea) y sigue en vigor, con modificaciones, bajo la denominación de Tratado de Funcionamiento de la Unión Europea. Tiene una indudable presencia práctica en la UE, pues su contenido es muy pormenorizado. El artículo 16 B del TFUE dispone que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan, por lo cual, el Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

⁹⁷ Como ejemplo, el informe 0261/2012 (Interés legítimo antipiratería) o el procedimiento sancionador nº: PS/00028/2002 (Publicidad con datos de ficheros telefónicos).

La Declaración adicional 21 del TUE se refiere a la protección de datos de carácter personal en el ámbito de la cooperación judicial en materia penal y de la cooperación policial. Establece que podrían requerirse normas específicas para la protección de datos de carácter personal y la libre circulación de dichos datos en los ámbitos de la cooperación judicial en materia penal y de la cooperación policial que se basen en el artículo 16 B TFUE, ya reflejado en el párrafo anterior, en razón de la naturaleza de dichos ámbitos. El punto positivo de este asunto se encuentra en la unidad de la norma comunitaria en cuanto a la política de protección de datos, generando una seguridad jurídica y una cohesión imposible de tener en 27 acuerdos bilaterales diferentes sobre esta materia. El punto de controversia deja abierta la posibilidad de que se generen normas específicas. Se puede tener una base jurídica común para toda la UE, pero queda por generar un sistema jurídico único. Este sistema de excepciones y de regímenes especiales para las normas que afectan a los DDFF dentro de la Unión es una forma de cohesionar políticamente. Sin embargo, jurídicamente, queda mucho por hacer, como lo demuestra las últimas regulaciones que en materia de protección de datos se han producido en Europa⁹⁸.

3.5. El Supervisor Europeo de Protección de Datos y el Grupo de Trabajo del Artículo 29

El Supervisor Europeo de Protección de Datos (SEPD) es una autoridad de control independiente encargada de garantizar que las instituciones y los órganos de la Unión cumplen sus obligaciones en materia de protección de datos, establecidas en el Reglamento (CE) Nº 45/2001 relativo a la protección de datos. Los cometidos principales del SEPD son el control, la consulta y la cooperación.

El Grupo de Trabajo del Artículo 29 (GT29) es un órgano consultivo independiente en materia de protección de datos y vida privada, establecido en virtud del artículo 29

⁹⁸ BLASI CASAGRAN, C., *La protección de los Derechos Fundamentales en el Tratado de Lisboa*, Barcelona, 2010.

de la Directiva 95/46/CE relativa a la protección de datos. Está compuesto por representantes de las autoridades nacionales de protección de datos de los Estados miembros, el SEPD y la Comisión. El GT29 elige a su presidente por un periodo de dos años. Realiza las funciones que establece el artículo 30 de la Directiva 95/46/CE. Asimismo, elabora recomendaciones, dictámenes y documentos de trabajo⁹⁹. El Consejo Europeo de Protección de Datos (CEPD) sustituirá al Grupo de Trabajo del Artículo 29 en el marco del nuevo Reglamento general de protección de datos (RGPD).

4. Anexo orientativo: las regulaciones europeas en materia de protección de datos

La UE siempre ha visualizado la necesidad de equilibrio entre las comunicaciones, la seguridad y la protección de datos personales vinculados a los DDFF, como se ha visto en el análisis que antecede. Así, ha aprobado varias resoluciones sobre estas cuestiones sensibles, relativas en concreto a la elaboración de perfiles en función de la etnia o la raza, la decisión del Consejo de Prüm sobre la cooperación transfronteriza en la lucha contra el terrorismo y la delincuencia transfronteriza, el uso de escáneres corporales para mejorar la seguridad de la aviación, los datos biométricos en los pasaportes y las instrucciones consulares comunes, la gestión de las fronteras, internet y la extracción de datos, entre otras.

Se van a mencionar las regulaciones que la UE ha desarrollado como más relevantes, para delimitar la visión temporal de la normativa europea¹⁰⁰. Se irán referenciando

⁹⁹ REBOLLO DELGADO, L., *Vida privada y protección de datos en la Unión Europea*, Madrid, 2008, pág. 156 y ss..

¹⁰⁰ Esta documentación se encuentra referenciada junto con las STJUE, que no se mencionan en el texto de tesis, en la página web de la Comisión con la URL http://ec.europa.eu/justice/data-protection/law/index_en.htm a 07 de julio de 2016. La AEPD también referencia estos textos legales de la UE en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/index-ides-idphp.php

algunas de estas normativas en la exposición de tesis, por ello es interesante su expresión temporal y a título de orientación.

4.1. Reglamentos.

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.

REGLAMENTO (UE) Nº 611/2013 DE LA COMISION, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)¹⁰¹.

4.2. Directivas.

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 97/66/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. (Derogada por la Directiva 2002/58/CE).

¹⁰¹ El nuevo Reglamento de 2016 se expondrá en el contenido de esta tesis, con un límite lógico de reciente conocimiento y falta de doctrina al respecto.

DIRECTIVA 1999/93/CE, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

DIRECTIVA 2000/31/CE, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

DIRECTIVA 2002/19/CE, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva de acceso).

DIRECTIVA 2002/20/CE, DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva de autorización).

DIRECTIVA 2002/21/CE, DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

DIRECTIVA 2002/22/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal).

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).

DIRECTIVA 2004/82/CE, DEL CONSEJO de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.

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 de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

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 (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

DIRECTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

4.3. Decisiones de la Comisión.

REGLAMENTO (CE) No 831/2002 DE LA COMISIÓN de 17 de mayo de 2002 por el que se aplica el Reglamento (CE) no 322/97 del Consejo sobre la estadística comunitaria en lo relativo al acceso con fines científicos a datos confidenciales.

DECISIÓN 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 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.

DECISIÓN DE LA COMISIÓN de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección adecuada de los datos personales en Hungría.

DECISIÓN DE LA COMISIÓN de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza.

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.

DECISIÓN 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 and Electronic Documents Act.

DECISIÓN 2002/16/CE DE LA COMISIÓN, de 27 de diciembre de 2001, relativa a '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. (queda derogada a partir de 15 de mayo de 2010)..

Corrección de errores de la Decisión 2002/16/CE de la Comisión, de 27 de diciembre de 2001, 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.

DECISIÓN reguladora de la Unidad de Cooperación Judicial Eurojust.

DECISIÓN DE LA COMISIÓN de 30 de junio de 2003, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina.

DECISIÓN DE LA COMISIÓN de noviembre de 2003, relativa al carácter adecuado de la protección de datos personales en Guernsey.

DECISIÓN DE LA COMISIÓN de 28 de abril de 2004 relativa al carácter adecuado de la protección de datos personales en la Isla de Man.

DECISIÓN DE LA COMISIÓN de 29 de abril de 2004 por la que se establece una lista de organismos cuyos investigadores pueden acceder, con fines científicos, a datos confidenciales.

DECISIÓN DE LA COMISIÓN de 14 de mayo de 2004 relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (Bureau of Customs and Border Protection).

DECISIÓN 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.

DECISIÓN DE LA COMISIÓN de 6 de septiembre de 2005, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros (PNR) que se transfieren a la Agencia de Servicios de Fronteras de Canadá.

DECISIÓN DE LA COMISIÓN de 8 de mayo de 2008 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Jersey

DECISIÓN DE LA COMISIÓN (2010/87/UE), 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.

DECISIÓN DE LA COMISIÓN de 5 de marzo de 2010 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre el tratamiento de datos personales

DECISIÓN DE LA COMISIÓN de 19 de octubre de 2010 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuada protección de los datos personales en Andorra

DECISIÓN DE LA COMISIÓN de 31 de enero de 2011 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de

los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales

CAPÍTULO SEGUNDO. EL FUTURO DE LA PROTECCIÓN A LOS DERECHOS FUNDAMENTALES A TRAVÉS DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES.

1. Los denominados Nuevos Derechos Fundamentales generados por la Sociedad de la Comunicación y el Conocimiento.

La evolución de los DDFF (se engloba en esta expresión también la evolución de las libertades públicas y los Derechos Humanos) junto con el avance de las tecnologías de la información y la comunicación es evidente y no se pueden admitir dudas ni cuestiones sobre ese aspecto. Sí admiten más análisis las cuestiones de definición de los nuevos DDFF, en caso de que realmente nos encontremos como civilización ante una nueva forma de derechos o, en otro caso, si solamente es una novedosa manifestación de los mismos DDFF con otras herramientas.

Puede ser que a la evolución de las generaciones por los avances tecnológicos le corresponda una evolución de las libertades. Esta misma afirmación se podría plantear a la inversa: a un mayor avance de libertades le correspondería un mayor avance tecnológico. Para una parte de la doctrina, se habla de *mutación histórica de los derechos humanos* que deriva en nuevas generaciones de derechos, hasta ahora no contemplados¹⁰², con un sentido histórico, vinculado a los acontecimientos del siglo XVIII, donde la burguesía creciente con el mercantilismo avanzó en su propuesta de libertades. Este primer movimiento o primera fase de derechos se consideraría individualista. Es

¹⁰² PÉREZ LUÑO, A., "La tutela de la libertad informática en la sociedad globalizada", *Isegoría: Revista de filosofía moral y política*, nº 22, 2000, pág. 59-68, pág. 64-65. En el año 2000, el profesor Pérez Luño plasma la evolución creciente de los DDFF (él utilizó la expresión Derechos Humanos en el texto, pero se va a englobar DDFF, libertades públicas y DDHH) dentro del ámbito del avance de las tecnologías. Para el profesor de Sevilla, a la "evolución generacional de los avances tecnológicos le ha correspondido una evolución también generacional de las libertades" pues la "mutación histórica de los derechos humanos ha determinado la aparición de sucesivas *generaciones* de derechos". Vinculó los DDHH como "categorías históricas que tan sólo pueden predicarse con sentido en contextos temporalmente determinados, y que nacen con la modernidad en el seno de la atmósfera iluminista que inspiró las revoluciones burguesas del siglo XVIII".

el Estado Liberal. Un segundo movimiento dentro de los derechos y libertades fundamentales se enmarcaría en el siglo XIX y a lo largo del siglo XX, generado por movimientos reivindicativos de derechos sociales, económicos y culturales, ampliando el avance del ser humano hacia contenidos más amplios que conformarían una segunda generación de derechos que sustituyen el Estado Liberal por el Estado Social, consagrándose jurídicamente. En el siglo XXI se percibiría sin lugar a dudas la visión de los DDFF dentro de una amplia y mundial apreciación. Ya la territorialidad no sería determinante ni limitativa ante la presencia de hechos mundiales. Se requiere políticamente un derecho a la paz, un derecho al consumo abierto y justo, un derecho a la calidad de vida y un derecho a la libertad informática y a las comunicaciones, entre otras percepciones sociales. Serían los denominados nuevos derechos, una tercera generación de Derechos Fundamentales que complementa y evoluciona las generaciones anteriores. En cuanto al derecho a la libertad informática (encuentro entre el derecho a la libertad y las nuevas tecnologías de la información y la comunicación) tuvo en los últimos 50 años varias fases de evolución legislativa¹⁰³, desde las llamadas leyes

¹⁰³ En el año 2000, se podía percibir sin dudas una visión más amplia de DDFF, con rasgos muy novedosos, que PÉREZ LUÑO centró en unos ejemplos: “el derecho a la paz, los derechos de los consumidores, el derecho a la calidad de vida o la libertad informática. En base a ello, se abre paso con intensidad creciente, la convicción de que nos hallamos ante una tercera generación de DDHH complementadora de las fases anteriores, referidas a las libertades de signo individual y a los derechos económicos, sociales y culturales.” Es lo que se ha denominado *liberties pollution* o *contaminación de las libertades*, dentro de la teoría social anglosajona, la cual considera que las nuevas tecnologías y su uso erosionan y degradan a los DDFF. El autor manifestó en ese texto su punto de vista generacional para el análisis de la evolución informática y las libertades: “Si la informática y las libertades han evolucionado generacionalmente nada tiene de particular que el punto de encuentro entre ambas categorías, es decir, la libertad informática, responda a su vez, a una decantación generacional. En efecto, la experiencia legislativa de estos últimos años registra una sucesiva decantación desde las leyes de la primera generación, basadas en la autorización previa de los bancos de datos en una etapa en la que los equipos informáticos eran escasos, voluminosos y fácilmente localizables, a las leyes de la segunda generación, cuyo objetivo principal fue la garantía de los datos “sensibles” por su inmediata incidencia en la privacidad o su riesgo para prácticas discriminatorias; y en la actualidad, a las de la “tercera generación”, que se ha hecho cargo de la revolución microinformática con la consiguiente difusión capilar de los bancos de datos. Ello ha hecho prácticamente inviable el control previo de los equipos informáticos,

de primera generación, las cuales se basaban solamente en la autorización previa de los grandes bancos de datos en dispositivos voluminosos, fáciles de localizar, escasos en su número; pasando por las leyes de segunda generación, cuya intención era proteger los llamados datos sensibles, los que tenían una incidencia directa con la intimidad y con las leyes de protección de la persona para no ser discriminada, ignorando la concurrencia de otros datos; y terminando con las leyes de tercera generación o de dispositivos mucho más pequeños y móviles, que agilizan la gestión infinitamente más, pero que deben atender no sólo a criterios de calidad o especie de los datos, sino también a su movilidad, finalidad y función. Este planteamiento es sumamente gráfico y aclarativo. En el término *libertad informática* se englobarían multitud de manifestaciones con incidencia en los derechos y libertades fundamentales y en la realidad individual, social, cultural y de desarrollo del individuo y de las civilizaciones. Se concluye que, en 2017, la globalización de los fenómenos sociales ya no se inscribe bajo unas fronteras, sino que implica a todo el planeta, a toda la humanidad, con una fuerza cada vez mayor, disminuyendo o aumentando, según el caso, el poder de la información. Por tanto, el contexto histórico dio lugar a nuevos DDFF o ha reforzado los existentes por lo menos a nivel de conocimiento de grupos humanos que antes de las tecnologías de la información ni tan siquiera concebían, errónea, falsa o correctamente, el concepto o la idea de los DDFF y las libertades públicas. No se puede asegurar si sería correcto exportar nuestro modelo de DDFF a otras civilizaciones, quizá para otros no fuera lo correcto o lo aplicable o lo conveniente. Pero sí se puede asegurar que el fenómeno trascendió¹⁰⁴. Vivir entre nuevas formas de comunicación y

sobre el que operaron las normas de la primera generación; al tiempo que la tutela de las informaciones ya no puede quedar circunscrita al factor estático de su calidad, según el criterio predominante en la segunda generación de leyes de protección de datos, sino que debe hacerse extensiva a la dinámica de su uso o funcionalidad”

¹⁰⁴ Pasando a los ejemplos, hace unos meses comunicaba con mujeres de La India, que se querían informar sobre la práctica de los DDFF de las mujeres en España, respecto a sus derechos en igualdad con los hombres. No sólo era una pregunta ante el fenómeno machista, era también una forma de saber que sus reivindicaciones son posibles y que para otras mujeres es normal trabajar, salir a la calle sin

nuevas ciencias, implica reflexionar críticamente las innumerables problemáticas en materia de DDFF. Los avances tecnológicos suponen afianzar las libertades como no se hizo nunca antes, repercutiendo en juristas y politólogos para generar análisis sobre la evaluación del impacto de los desarrollos telemáticos e informáticos en la cultura de las civilizaciones y en la filosofía, en nuestra disciplina, filosofía o teoría del Derecho, con la realidad cambiante del siglo XXI.

En el tema del derecho fundamental a la protección de datos personales, la visión global es imprescindible¹⁰⁵. Se produce, lo quieran los Estados (y sus poderes correspondientes) o no lo quieran, una interdependencia, una clara interconexión de los problemas, los riesgos, pero también de las oportunidades, del conocimiento de unos y de otros, de las posibles relaciones humanas (se podría hablar de relaciones afectivas, emocionales incluso, base y motivo más frecuente de las poderosas redes sociales) que solamente a través de una visión internacional puede tener una regulación y una solución a los problemas que se presentan entre las múltiples oportunidades. La AEPD así lo realiza, con sus grupos de trabajo de la EU (GT29, ya mencionado ampliamente) y con diferentes Estados, entre ellos el más vinculado con Europa, EEUU.

escolta masculina o defenderse en los Tribunales, si llega el caso. Cuestiones que las mujeres en España y en nuestro entorno europeo ni tan siquiera se preguntan, pero en La India, siguen cuestionándose.

¹⁰⁵ Véase autor y obra citada: "La tendencia hacia la globalización viene impuesta por el carácter interdependiente, multicéntrico y multicultural de los fenómenos que gravitan sobre la tutela de las libertades" Se cita por el autor un texto de la conferencia del Club de Roma de 1985, que se desarrolló en esta ciudad de Santander: "Comprenderíamos mejor la dinámica de la interdependencia si no imagináramos el mundo como un mapa de naciones, sino como un mapa meteorológico, en el que los frentes climáticos se arremolinan y se desplazan con independencia de las fronteras nacionales y los frentes de bajas y altas presiones crean condiciones meteorológicas a gran distancia." Véase también PÉREZ LUÑO, A., *Nuevas Tecnologías y Derechos Humanos*, Valencia, 2014. En una redacción más reciente el autor junto con otros analizó diversas problemáticas en relación a internet. Resaltan los términos utilizados como *teledemocracia* o *ciberciudadanía*, para expresar la nueva situación en las sociedades democráticas y las que luchan por serlo, en torno a los medios de comunicación y las tecnologías informáticas. El autor se muestra a favor de lo que denomina el reforzamiento de los derechos de participación política, aun asumiendo los riesgos. Se referenciarán sus propuestas más adelante.

El derecho fundamental a la protección de datos es ante todo un derecho con rango constitucional, que puede llegar a ser insuficiente para su eficacia¹⁰⁶. Häberle apuntó en el pasado siglo sus teorías sobre Derecho Constitucional Común Europeo (a partir de ahora, DCCE). El DCCE apareció integrado por un conjunto de principios constitucionales provenientes de cada Estado miembro, pero que son comunes a los diferentes Estados europeos, hayan sido positivados en sus diferentes sistemas jurídicos o no sean más que principios legales. Los principios comunes proceden de diferentes fuentes, como son las diferentes Constituciones de los Estados miembros de la UE y del llamado Derecho Europeo que lo integran las normas de la Unión Europea, del Consejo de Europa y de la Conferencia para la Seguridad y la Cooperación en Europa; todo ello conformaría el llamado *Ius Commune Constitutionale*.

La Constitución Europea es el objetivo de ese DCCE, no sólo para ser una norma de disposición en cuestiones de índole económica, cuya importancia no se pone en duda, sino también como un referente jurídico para los DDFF. Alemania otorga a través de diversos autores mucha importancia a este concepto¹⁰⁷, con la expresión *Das Gemeinsame Europäische Verfassungshaus*, la Casa Constitucional Común Europea¹⁰⁸.

¹⁰⁶ El derecho a la protección de datos personales “posee una dimensión internacional y por ello, su respuesta no puede quedar entorpecida por las limitaciones propias de los ordenamientos jurídicos nacionales” sino que requiere soluciones jurídicas “supranacionales”. El autor incide sobre la idea de un nuevo constitucionalismo, pues las tendencias actuales otorgan al derecho constitucional una “peculiar fisonomía”. El profesor de Sevilla se remite a las teorías de otro eminente jurista, el profesor Peter Häberle, catedrático de Derecho Público en las universidades de Bayreuth y St. Gallen en ese momento de hace 16 años. Häberle acuña la expresión “*Derecho Constitucional Común Europeo*” (DCCE) en sus siglas, cuya inspiración proviene del *ius commune*.

¹⁰⁷ Analiza profusamente conceptos de diversos autores en su obra PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010. La bibliografía en alemán fue también muy extensa, como ejemplo sirva DECKER, F., *Die Verfassung Europas. Perspektiven des Integrationsprojekt.*, Wiesbaden, 2009. Con la salida de Gran Bretaña de la Unión, los denominados populismos en diversos países y las residuales diferencias de la pasada crisis (asunto Grecia, España, Portugal, Irlanda) se revisaron los objetivos de la UE, aunque las perspectivas serían positivas para los europeístas.

¹⁰⁸ “*Con múltiples alcobas hacia el interior y el exterior, pero con autoconsciencia de que sus cimientos son comunes.*”

La LOPD y la Directiva 95/46/CE, junto con la actual regulación del Reglamento Europeo 2016/679, son normas que conforman eslabones del sistema jurídico europeo de las libertades. La eficacia de las normas en cuanto a la tutela y ejercicio de los Derechos y Libertades Fundamentales se haya en dependencia de la calidad de las normas constitucionales y sus leyes de desarrollo, pero también en la sensibilidad y convicción de los legisladores, Tribunales, ciudadanos y otros operadores del sistema jurídico, como son las empresas, para que las normas sobre protección de datos sean tangibles en la sociedad democrática. Porque igualmente viola los DDFF un tratamiento indebido de datos personales como no permitir un acceso a la comunicación y a la gestión por intromisiones del poder político o político-religioso. A las redes de información se accede a través de la voluntad, no se obliga a ningún ser humano. Pero es una flagrante violación de derechos el dominio por cualquier tipo de poder de las comunicaciones y del desarrollo de la libertad informática¹⁰⁹. Polonia, junto con Hungría forman en este momento un conjunto especial y bastante pintoresco de las posibles visiones o políticas dentro de la UE. Tan derecho fundamental es el respeto a las creencias religiosas como lo es la libertad de comunicación y de información, la libertad informática. Las comunicaciones por *internet* serán mucho más valiosas para los ciudadanos que las posibles consecuencias de su uso, que no sabemos si serán negati-

¹⁰⁹Como ejemplos se toman los casos de China y de Polonia, ambos países se encuentran como noticia en el año 2015 debido a la clara violación de DDFF por parte de sus gobiernos. China lo llamó eufemísticamente *libertad y orden*, como una especie de mantra para ocultar una falta de libertad obvia. Como siempre que un régimen político interfiere en la libertad de la ciudadanía, se apela a la seguridad frente al ciberterrorismo y el espionaje enemigo en la Red. Su mandatario pedía respeto a la *cibersoberanía* de su país. A su vez, realizó cinco propuestas: acelerar la construcción de infraestructura; crear plataformas online de intercambios culturales; mejorar la cibereconomía, impulsar la ciberseguridad y crear un sistema de gobernanza global de internet (se entiende que bajo los parámetros chinos) Facebook, Google o Twitter están censurados en China, lo que equivale a decir que son ilegales. China pretende un control global de internet en todo el mundo, tentación para muchos.

La Razón «Libertad y orden»: así quiere China controlar internet <http://www.larazon.es/tecnologia/libertad-y-orden--asi-quiere-china-controlar-internet-ID11478110#Ttt1C6mOZjKV2hUj> a 16 de febrero de 2015.

vas o positivas, sobre lo que consideran una base cristiana¹¹⁰. La pregunta a tener en cuenta es si se han creado o se deben crear nuevos DDFF o lo que existe es una reinterpretación de los existentes, a través de unas nuevas formas de realización de los mismos.

2. El nuevo Reglamento Europeo y del Consejo de 27 de abril de 2016 de protección de datos personales.

2.1. El espacio de libertad, seguridad y justicia, ELSJ.

¹¹⁰ Para el gobierno polaco, en otro ejemplo dentro de la UE, es necesario un control de contenidos y de medios de comunicación, entre otras reformas de corte conservador o más bien, limitador, El partido gobernante tiene suficiente mayoría como para reformar la Constitución. La UE ha pedido explicaciones al Estado polaco, un tanto fuera de los ámbitos comunes del Derecho Europeo, pero parece que tiene un fuerte apoyo social que respalda estas decisiones. Ante este escenario, sobra decir que el pueblo polaco decide su destino, la pregunta es si formando parte de la UE, con una libre circulación de personas y capitales, tales reformas limitativas de DDFF pueden ser o no ser contrarias al Tratado de la Unión. Véase en las noticias “El polaco Kaczynski golpea de nuevo con sus reformas ultraconservadoras”

http://internacional.elpais.com/internacional/2015/12/31/actualidad/1451517883_918125.html a 04 de enero de 2015. Dentro de la prensa alemana, en el diario Die Welt se trató el asunto también, con cierto aire crítico, pues Polonia responsabiliza a Alemania de tantos “desatinos” y ataques a la civilización europea. <http://www.welt.de/politik/ausland/article150583362/Das-polnische-Feindbild-heisst-Deutschland.html> a 04 de enero de 2015. En junio de 2016 volvió a ser noticia la advertencia de Bruselas a Polonia por sus políticas restrictivas en el ejecutivo de Jaroslaw Kaczynski, en especial el control de los medios de comunicación. Si no se resolviera esta situación, Polonia perdería su derecho de voto en la UE, lo cual no ha sucedido a lo largo de la corta historia de la Unión. En 2014 la UE se dotó de poderes ejecutivos para evaluar el cumplimiento del Estado de Derecho en los Estados miembros. http://internacional.elpais.com/internacional/2016/06/01/actualidad/1464782105_752950.html?id_externo_rsoc=TW_CM> Se mencionan las noticias como anécdotas, pues no merecen más consideración en este momento.

Después del TUE (Tratado de Lisboa) se generalizaron los esfuerzos de la UE para priorizar lo que se denominó el Espacio de Libertad, Seguridad y Justicia, conocido por sus siglas ELSJ, para tomar decisiones por un procedimiento más eficaz, democrático, responsable y legítimo, con una mayor competencia de atribuciones para el TJUE (Tribunal de Justicia de la Unión Europea) y relevancia para los Parlamentos nacionales. Es la consecuencia del desarrollo legislativo del artículo 3.2 del TUE, el cual estableció que *la Unión ofrecerá a sus ciudadanos un espacio de libertad, seguridad y justicia sin fronteras interiores, en el que esté garantizada la libre circulación de personas conjuntamente con medidas adecuadas en materia de control de las fronteras exteriores, asilo, inmigración y de prevención y lucha contra la delincuencia*. Es de destacar que el artículo 3.2 TUE figura en el orden de la normativa antes que la realización del mercado interior, dentro de los objetivos del TUE. Además, el Título V del TFUE (artículo 67 a 89) se dedicaron íntegramente al ELSJ.

Después de los programas de *Tampere* en 1999 y *La Haya* en 2004 el Consejo Europeo aprobó en diciembre de 2009 un nuevo programa plurianual en el ámbito del ELSJ para el periodo 2010-2014: el *Programa de Estocolmo*. La Comisión preparó en el año 2012 una serie de normativas para la reforma de la protección de datos, para aumentar el control de los datos personales por los titulares y también reducir el coste de las empresas, junto con un sentido de unificación de normativas, pues los 28 Estados miembros habían desarrollado el derecho a la protección de datos personales con la norma del año 1995, la cual tampoco contemplaba los avances tecnológicos y la comunicación a nivel mundial, la llamada globalización. Se debían eliminar con un único acto legislativo la fragmentación existente y evitar la carga administrativa para los Estados miembros. Se confiaba en generar mayor confianza de los consumidores en la UE, innovación tecnológica, mayor crecimiento y empleo, modernización de los principios consagrados en la Directiva 95/46/CE junto con una propuesta de Directiva específica para el tratamiento de datos personales dentro del marco de cooperación policial y judicial en materia penal. Las negociaciones fueron muy largas y no exentas de dificultades. En el año 2015 el Parlamento y el Consejo consiguieron un acuerdo

tanto para un nuevo Reglamento de Protección de datos como para una nueva Directiva en las materias penales mencionadas.

2.2. El Reglamento 2016/679 de protección de datos de la Unión Europea (RGPD)

Para la modernización de la normativa europea en materia de protección de datos personales se eligió un instrumento jurídico diferente a la anterior regulación. No se elige una Directiva, sino un Reglamento. La razón fue el fracaso en la armonización en el Espacio Económico Europeo (EEE) de las anteriores normas. Un Reglamento es una norma de aplicación directa dentro de los Estados miembros, sin posibilidad de modificación o necesidad de transposición al derecho interno de los Estados miembros (como sí ocurre en las Directivas) lo que permite que las normas sean las mismas para toda la UE. El doble objeto del nuevo Reglamento de la Unión Europea es el mismo que el de la Directiva 95/46/CE: la protección de los derechos y libertades fundamentales de las personas físicas, su derecho a la privacidad en cuanto a sus datos personales, junto con la libre circulación de datos dentro del EEE.

El nuevo Reglamento de la UE (en adelante, RGPD) deroga la Directiva 95/46/CE, supondría para los consumidores un inicio de mayor control y para las empresas mayor claridad, al ser una norma única, reforzando la seguridad jurídica y la confianza en las normas. En el nuevo RGPD se incluye la regulación sobre el *derecho al olvido*, denominado *derecho de supresión*, mediante la rectificación o supresión de datos personales; el derecho a la portabilidad de datos, por el que se pueden trasladar datos personales previa autorización del titular a otro proveedor de servicios; se resalta la importancia innegable de la autorización o consentimiento para el tratamiento de datos personales y se cambia la aplicación de las sanciones a las empresas a un concepto de porcentaje sobre la facturación, que puede ser hasta del 4%. Entre los conceptos novedosos también figura expresamente la normativa sobre transmisión de datos para asuntos policiales y judiciales, unificando con normativa europea lo que ya sucedía en la práctica bajo la justificación de la seguridad y la mejor acción policial. Se han que-

rido tener en cuenta salvaguardias para los riesgos de seguridad y facilitar una mejor cooperación entre las autoridades policiales, respetando todas ellas unas normas comunes en cuanto a protección de datos personales. La entrada en vigor del RGPD se produjo 20 días después de su publicación y serán de aplicación sus normas en todos los Estados Miembros dos años después, en mayo de 2018¹¹¹.

El texto del RGPD es complejo y minucioso en su normativa, incluye conceptos jurídicos muy indeterminados por lo que su interpretación será necesaria. Al ser un Reglamento comunitario su aplicación será directa, sin necesidad de transposición al Derecho español, pero ello genera a su vez problemas frente a la actual regulación de la LOPD. Se destacan algunos principios que se aplicaban desde hace años, pero que en el RGPD tienen su artículo expreso sobre la materia, como es la obligación de establecer la seguridad sobre la protección de datos en el diseño de aplicaciones de software (artículo 25 RGPD); la regulación del consentimiento a través de contratos de adhesión, pues debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. La identidad del responsable del tratamiento se hace imprescindible al igual que los fines del tratamiento a los cuales están destinados los datos personales (considerando 42). El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno (artículo 7 RGPD). Los derechos ARCO (acceso, rectificación, cancelación y oposición) del titular quedan sustituidos por nuevas denominaciones, como son el derecho de transparencia (artículo 12 RGPD), el derecho de información (artículo 13 y 14 RGPD), el derecho de acceso (artículo 15 RGPD), el derecho de rectificación (artículo 16 RGPD), el derecho de supresión o *derecho al ol-*

¹¹¹ Véase el reciente estudio de DAVARA RODRÍGUEZ, M., "El Reglamento Europeo sobre protección de datos.", *El Consultor de los Ayuntamientos*, nº 11, 2016. Uno de los pocos autores que ha publicado en el año 2016. Anteriormente a esta fecha, los apuntes de otros autores sobre el nuevo marco legislativo, como SÁNCHEZ BRAVO, Á., "Nuevo marco europeo de protección de datos personales", *Derechos Humanos y protección de datos personales en el siglo XXI*, , 2013, pág. 258 y ss.

vido (artículo 17 RGPD), el derecho a la limitación del tratamiento (artículo 18 RGPD), el derecho a la portabilidad de datos (artículo 20 RGPD) y el derecho de oposición (artículo 21 RGPD).

Queriendo ser un texto actualizado, se olvidaron cuestiones como *big data*, *cloud computing* o la interconexión de dispositivos y máquinas (el llamado *internet* de las Cosas) lo que lleva a concluir que la normativa nace con cierto carácter obsoleto frente a la realidad actual.

En cuanto al impacto en las empresas de la nueva normativa, se diferencia entre la gran empresa y las PYMES; para la gran empresa será mucho más sencillo su adecuación a la norma, entre otras razones porque colaboró en su desarrollo. Para las PYMES, sin embargo, supondrá un nuevo esfuerzo de adaptación. Muchos de los contenidos son muy complicados e indeterminados, añadiendo que el RGPD permite el recurso al arbitraje en caso de discrepancias y problemas.

Su análisis se realizará en los epígrafes correspondientes a los temas que se quieren abordar, dentro de los DDFF y la práctica de la protección de datos en las empresas y por los ciudadanos.

CAPÍTULO TERCERO. LAS NORMATIVAS ESPAÑOLAS DE PROTECCIÓN DE DATOS PERSONALES.

Antes de la Constitución Española de 1978 (en adelante CE) las pocas normas de protección de la intimidad y de la privacidad se centraban en aspectos lejanos al posterior concepto de protección de datos personales. Se pueden señalar diferentes momentos en una línea temporal para visualizar brevemente la situación anterior a la CE¹¹². Antes del siglo XIX se reflejaban diferentes protecciones a determinados aspectos de la intimidad, en Códigos y Recopilaciones, especialmente centrados en la inviolabilidad del domicilio y la correspondencia, pero también querían proteger el honor o la dignidad. Reduciendo el estudio al constitucionalismo histórico, la inviolabilidad del domicilio se reconoce desde la Constitución de 1812 hasta la vigente CE¹¹³. En cuanto a la inviolabilidad de la correspondencia, la primera Constitución que le dio a este derecho rango constitucional es la del año 1869, artículo 7; en las siguientes Constituciones se continua con ese reconocimiento. Otros aspectos de la intimidad y la privacidad se fueron incorporando a las diferentes Constituciones. En los años anteriores al desarrollo tecnológico, no existe una vinculación entre los derechos mencionados (correspondencia, inviolabilidad del domicilio, intimidad) y los medios de comunicación y tratamiento de la información de carácter personal. Los medios de almacenamiento y tratamiento eran generalmente en papel y sumamente restringidos al uso o tratamiento del sector público y de empresas con amplia gestión que se pudieron desarrollar con el avance de las Revoluciones Industriales. La concienciación sobre la información personal se produjo por el uso que se hizo de ella durante la Segunda Guerra Mundial y los sistemas políticos totalitarios, donde la información per-

¹¹² RÚIZ MIGUEL, C., *La configuración Constitucional del Derecho a la Intimidad*, Madrid, 1995, pág. 78-84.

¹¹³ Concretamente fueron la Constitución de 1808 (Estatuto de Bayona) art. 126; Constitución de 1812, art. 308; Constitución de 1873, artículos 7 y 8; Constitución de 1845, igualmente en los mismos artículos; Constitución de 1856 artículos 8 y 9; Constitución de 1869, artículo 5, con una detallada regulación; Proyecto de Constitución de 1873, artículo 7.1; Constitución de 1876, artículo 6; Constitución de 1931, artículo 31.

sonal de una gran parte de la sociedad comienza a ser tratada con fines políticos y con unas consecuencias nunca antes sospechadas¹¹⁴.

En España, entre los antecedentes normativos de la CE¹¹⁵, se encuentra una Orden ministerial del Ministerio de Justicia de 18 de febrero de 1970, por la que eran convocadas unas jornadas de estudio sobre perfeccionamiento y modernización de los medios y métodos de la Justicia. En las jornadas citadas, se invitaba a considerar como herramientas para el desarrollo de la función judicial las aplicaciones de los primeros ordenadores que posiblemente se comenzaban a implantar en España¹¹⁶. El 9 de abril de 1970, otra Orden ministerial desarrolló las normas para la utilización del télex judicial. El 12 de septiembre de 1970 se creó una Comisión interministerial de Informática y un Servicio Central de Informática. La Comisión tenía como labor supervisar y apoyar la programación informática de los diferentes ministerios, los cuales tenían una Comisión de Informática¹¹⁷. Muy poco antes de la promulgación de la CE, se creó

¹¹⁴ La fotografía y la máquina de escribir, con la producción masiva de papel, generaron un fenómeno de control de masas no visto con anterioridad a través del tratamiento de datos personales. A ello se añaden los medios de comunicación, como telégrafo y posteriormente teléfono o radio. Se sabe que en la Alemania del régimen Nacional Socialista se tenían ya avances tecnológicos de tratamiento de datos, una máquina denominada *Hollerith* que trataba fichas perforadas para elaborar el censo de 1933, innovación en ese momento de IBM. Véase el estudio de GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 26. No se deben olvidar tampoco fenómenos históricos terroríficos como los juicios de religión, tanto católicos como protestantes, judíos o musulmanes, hoy todavía presentes en algunas comunidades religiosas.

¹¹⁵ PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010, pág. 378. Pérez Luño trata los antecedentes normativos de la reglamentación de lo que denomina informática, remontándose hasta el final de los años sesenta para mostrar el interés de investigadores españoles por el derecho de la cibernética o de la informática, cuyos estudios se basaban en las posibles implicaciones y normalizaciones de las tecnologías de la información

¹¹⁶ *Ibíd.*, pág. 380. Véase también como análisis de 1976-1977 a HEREDERO HIGUERAS, M., "Informática y Libertad: la respuesta de los juristas a un problema de nuestro tiempo"].

¹¹⁷ *Ibíd.*, pág. 380. La aportación destacable de esta norma se encuentra en su artículo 1, con una definición legal de informática: "Conjunto de técnicas y métodos necesarios para la utilización de los equipos de proceso de datos"; "Aquellas máquinas y dispositivos capaces de elaborar información de forma digital siempre que la entrada de datos o la salida de los resultados tenga lugar sobre un soporte

una Comisión Interministerial para la elaboración del Plan Informático Nacional, mediante un Decreto de la Presidencia del Gobierno, el 29 de septiembre de 1978. Merece especial atención la alusión expresa en este Decreto al estudio de las concretas aplicaciones de estas tecnologías y a los *problemas que plantea la transmisión de datos dentro y fuera de las fronteras nacionales*.

Posteriormente a 1978 el tema sobre el derecho a la protección de datos personales se centró en el artículo 18 CE¹¹⁸. En la minuta de la ponencia de Constitución en su sesión del día 8 de septiembre de 1977, en el punto 7º se reflejó lo siguiente: “Siguiendo el método de trabajo acordado, se entran a considerar los temas referentes a la intimidad personal y una vez expuestos los criterios de los miembros de la Ponencia, se aprueba un texto como artículo 21. *Los miembros de la Ponencia exponen su preocupación en cuanto a la inclusión, dentro de este artículo, de un apartado que se refiera a la influencia de la técnica, y en especial de la informática, sobre aquel derecho*. Por el representante del grupo Vasco-Catalán¹¹⁹ se propuso aportar una redacción en relación con este asunto, y así se aceptó por los miembros de la Ponencia, posponiéndose la discusión del asunto”¹²⁰. Por tanto, en éste acta se redactó el que se nombra como artículo 21 con el siguiente texto: 1. Se garantiza el honor y la intimidad personal y familiar. 2. El domicilio es inviolable. Ninguna investigación domiciliaria podrá realizarse sin mandato judicial. 3. Se garantiza el secreto de las comunicaciones postales, telegráficas y telefónicas, salvo mandato judicial. 4. (Informática,

creado o aceptado por otras máquinas.” Se consideraban equipos de proceso de datos “las máquinas y dispositivos capaces de aceptar o crear soportes de información o de transmitir ésta a otras unidades”

¹¹⁸ ACTAS DE LA PONENCIA CONSTITUCIONAL DE 1977, “congreso.es”]. A 06 de junio de 2015. Páginas 1 a 5. <http://www.congreso.es/constitucion/ficheros/actas/actas.pdf> Unas notas sobre su creación. La CE de 1978 fue llamada la Constitución de la transición. Las notas de las actas de la ponencia constitucional, marcan el rito, casi frenético, de su creación en tan pocos meses. Se somete al Parlamento el día 31 de octubre de 1978, habiéndose iniciado la “Constitución” (ese es el término que emplea el documento) de la Comisión Constitucional el día 01 de agosto de 1977, según el acta que se referencia.

¹¹⁹ Se piensa que el representante del llamado en el acta “Grupo Vasco-Catalán” era D. Miguel Roca Junquent;

¹²⁰ ACTAS DE LA PONENCIA CONSTITUCIONAL DE 1977, “congreso.es”]. A 06 de junio de 2015. Página 16 del pdf. <http://www.congreso.es/constitucion/ficheros/actas/actas.pdf>

pendiente de redacción)”¹²¹. Los constituyentes tenían como referencia el artículo 35 de la Constitución Portuguesa¹²², el cual sí incluye claramente derechos y limitaciones sobre el uso de información personal¹²³.

En el borrador constitucional y en el anteproyecto se tiene el siguiente enunciado: “La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos”. Este texto se enumeró como artículo 17.4 y pasó a debate en la Comisión Constitucional del Congreso. Dos posiciones se perfilaron en los debates. Una, representada por los miembros del partido UCD, que pretendían la suspensión de la mención a la Informática, por considerar que la garantía del derecho a la intimidad y al honor ya suponía suficiente protección y además porque la alusión expresa a la informática excluía otras técnicas, también invasivas. La otra, de especial importancia: “*consideraba necesario mantener la alusión expresa a la informática, si bien extendiendo la tutela frente a su uso indebido al ejercicio de todos los derechos*, en lugar de restringirla al derecho al honor y a la intimidad”¹²⁴ Esta tesis fue mantenida por el Sr. Gastón Sanz, del Grupo Mixto, el cual proponía el siguiente texto:

¹²¹ ACTAS DE LA PONENCIA CONSTITUCIONAL DE 1977, “congreso.es”]. A 06 de junio de 2015. Página 18 del pdf. <http://www.congreso.es/constitucion/ficheros/actas/actas.pdf>

¹²² Véase PÉREZ LUÑO, páginas 381-385, bajo el epígrafe: “El iter del texto constitucional: elaboración y debates parlamentarios”.

¹²³ DEL PESO NAVARRO, E., *Ley de Protección de Datos, la nueva ley LORTAD*, Madrid, 2000, pág. 9-10. El artículo de la Constitución Portuguesa, poco anterior a la Constitución Española se expresó así: “1. Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanografiados, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización. 2. La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se trate del proceso de datos para fines estadísticos. Queda prohibida la atribución de un número nacional único a los ciudadanos.” Véase también GARRIGA DOMÍNGUEZ, A., *Tratamiento de datos personales y derechos fundamentales*, Madrid, 2009, pág. 33-34. La misma autora escribió su tesis doctoral sobre protección de datos en el año 1999, realizando un análisis sobre todos estos aspectos GARRIGA DOMÍNGUEZ, A., *La protección de datos personales en el Derecho español*, Madrid, 1999.

¹²⁴ PÉREZ LUÑO, obra y epígrafe citados.

“La ley regulará el acopio, uso y difusión de los datos personales contenidos en los archivos o registros, susceptibles de acceso automático, con objeto de garantizar las libertades públicas y el ordenamiento constitucional”

Un texto sensiblemente más amplio de miras y de expresión, sobre el desarrollo de la informática y sus límites en el disfrute de los Derechos Fundamentales. Sin embargo, esta tesis no prosperó. Lo hizo la propuesta del Sr. Roca. Quedó patente, al menos, la inquietud de los constituyentes sobre el uso de la informática de forma abusiva, menoscabando las libertades. La fórmula inicial elegida, “la Ley limitará el uso de la informática” se considera defensiva por amplia doctrina, y negativa respecto a la libertad informática¹²⁵.

El artículo 21 en el borrador, pasó a ser el artículo 18 CE en el texto definitivo y el párrafo de la mención a la informática se incorporó, quedando su redacción así:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna investigación domiciliaria podrá realizarse sin mandamiento judicial, salvo en caso de flagrante delito o con consentimiento expreso del propietario.
3. Se garantiza el secreto de las comunicaciones y en especial de las postales, telegráficas y telefónicas, salvo mandato judicial.
4. La Ley limitará el uso de la informática de manera que quede a salvo el respeto a la intimidad personal y familiar y al honor de los ciudadanos.”¹²⁶

En el Diario de Sesiones de su aprobación en las Cortes Españolas, se destacan varias intervenciones memorables, de las cuales se extraen dos párrafos que miraban al futuro de España. Uno del entonces presidente del Gobierno, D. Adolfo Suárez¹²⁷, y otro

¹²⁵ Ídem.

¹²⁶ ACTAS DE LA PONENCIA CONSTITUCIONAL DE 1977, “congreso.es”]. A 06 de junio de 2015. Página 384 del pdf. <http://www.congreso.es/constitucion/ficheros/actas/actas.pdf>

¹²⁷ DIARIO DE SESIONES DEL CONGRESO DE LOS DIPUTADOS, 3., “congreso.es”]. http://www.congreso.es/public_oficiales/L0/CONG/DS/C_1978_130.PDF a 06 de junio de 2015, página 26 del pdf editado. “La Constitución es, además, instrumento que ordena el futuro, que no pretende

de D. Santiago Carrillo¹²⁸. Su reseña, al margen del tema de esta tesis, quiere ser un humilde homenaje de estas páginas a dos personas excepcionales. La tercera mención es para D. Felipe González, quien fue Presidente del Gobierno cuando se promulgaron la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, que desarrolló parte del artículo 18 CE y la Ley Orgánica de Regulación del Tratamiento de Datos de Carácter Personal, la LORDAT, del año 1992, antecedente de la LOPD actual.

3. El artículo 18.4 de la Constitución Española de 1978.

3.1. Naturaleza jurídica del derecho a la protección de datos personales en la CE 1978

La intención y finalidad de los constituyentes era proteger el uso indebido de los sistemas de tratamiento de datos personales y lo distinguieron del derecho a la intimidad, reconocido en el primer apartado del artículo 18 CE. Por tanto, en un primer momento, no se configura un derecho fundamental a la protección de datos en la CE.

tanto describir la realidad como transformarla. Y por ello la Constitución regula detenidamente las libertades públicas y los derechos y deberes de los españoles; establece garantías, algunas incluso audaces y novedosas, en nuestra latitud y nuestra historia, y consagra lo que es un baluarte de la libertad, la independencia real y efectiva del Poder Judicial, no sólo frente a los restantes poderes del Estado, sino frente a cuáles quiera grupos políticos y sociales.”

¹²⁸ DIARIO DE SESIONES DEL CONGRESO DE LOS DIPUTADOS, 3., "congreso.es"]. A 06 de junio de 2015, página 16 del pdf editado. “Nuestro acuerdo con la Constitución empieza porque la consideramos una Constitución válida para todos los españoles, una Constitución de reconciliación, una Constitución que viene a hacer punto y raya con el pasado de luchas civiles, con el pasado de división que ha conocido nuestro país; una Constitución que refleja las realidades político-sociales y culturales de la España de hoy y que además –y esta es una de las razones por las que la votamos sin vacilar- no cierra el camino al progreso de nuestro país, no cierra el camino a las transformaciones sociales para las cuales nosotros existimos como partido.”

Resulta difícil encontrar teorías sobre los DDFF y la diferente naturaleza que los describe. La mezcla de puntos de vista en los diferentes autores, la interpretación en función de un determinado derecho fundamental o los diversos criterios de los Tribunales Constitucionales, hacen que sea una tarea ardua y no exenta de polémica. Para el desarrollo de este análisis se delimitó lo concerniente al derecho a la protección de datos en una línea clara de actuación y de exposición, más en dirección a la realidad de la eficacia del derecho fundamental a la protección de datos en relación con la empresa y el ciudadano que exponer una serie de teorías, que son fascinantes, pero que no exponen con claridad la práctica material. Aun así, para posicionar la naturaleza jurídica del derecho a la protección de datos dentro del ordenamiento jurídico español, se hace necesario comentar las posiciones de la doctrina en cuanto a las diferentes interpretaciones y aplicaciones de los DDFF en general, para generar un encuadre sistemático correcto, ya que los derechos no se presentan en su estado puro, sino que se interrelacionan, se confrontan, se suplen o complementan, se adormecen por ausencia de atención, se mezclan dentro del sistema social, en especial dentro de los DDFF, los cuales pueden estar en colisión unos con otros en muchas ocasiones¹²⁹.

Un derecho fundamental deriva de la Constitución como doble fuente jurídica; por un lado, como fuente de las demás fuentes y por otro como fuente suprema de eficacia directa. Por una parte, la CE regula la producción de normas cuyos destinatarios son el legislador y los poderes públicos, los cuales no pueden disponer de los derechos que se establecieron en la CE. Por otra parte, la CE crea relaciones jurídicas de forma directa, con eficacia inmediata. Esa eficacia directa de los DDFF los convierte en ejercitables por sus titulares inmediatamente, sin necesidad del legislador, además de proteger frente a las injerencias de los poderes públicos y de los particulares¹³⁰. BAS-

¹²⁹ MAGDALENO ALEGRÍA, A., *Los límites de las libertades de expresión e información en el Estado social y democrático de Derecho.*, Madrid, 2006, pág. 72. El autor cita a BÖCKENFORDEN y a BASTIDA FREIJEDO. Otra intensa relación de diversas posiciones de la doctrina se expone por PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010.

¹³⁰ BASTIDA FREIJEDO, FRANCISCO J.; VILLAVARDE MENÉNDEZ, IGNACIO; REQUEJO RODRÍGUEZ, PALOMA; PRESNO LINERA, MIGUEL ÁNGEL; ALDÁEZ CORRAL, BENITO; FERNANDEZ SARASOLA, IGNACIO, *Teoría*

TIDA considera que *un derecho fundamental es ante todo un derecho subjetivo*; la Constitución atribuye al sujeto, al ciudadano, un apoderamiento jurídico, que es el contenido esencial del derecho en cuestión, lo cual puede exigir a un tercero (poder público o particular) que cumpla un deber. El legislador no puede disponer de los DDFF para negarlos o desnaturalizarlos, puede solamente promover su ejercicio real y efectivo (artículo 9.2 CE). Esta perspectiva se califica de jurídico-positiva. El constituyente realiza una selección de expectativas, tanto a nivel individual como social, e inserta estas en una norma superior a las otras, reguladas de forma indisponible para el legislador; determinados derechos se van a considerar, según esta teoría, como funcionales, ya que serán claves para el funcionamiento de todo el sistema jurídico. Por lógica, el resultado de la regulación de los derechos en la Constitución dependerá de la sociedad que se ordene a través de los mismos. Una sociedad determinada, estructurada alrededor de la propiedad privada como derecho subjetivo, como la sociedad liberal, considerará el derecho a la propiedad como fundamental. Una sociedad organizada desde una Constitución democrática considerará probablemente el derecho a la propiedad como un derecho fundamental con garantía institucional y una Constitución socialista excluirá la propiedad del sistema jurídico¹³¹. La Constitución democrática va a fijar derechos y libertades de los ciudadanos del Estado al que regula en normativas que pueden considerarse iusfundamentales, para satisfacer las expectativas de los sujetos, los individuos que son libre e iguales, con capacidades sociales. Los ciudadanos se identifican con su Constitución; si no fuera así, no podría llamarse norma democrática. Los principios, valores e intereses iusfundamentales de una sociedad deben regularse en normas positivas para no degenerar en una ley natural e inmutable, indisponible. Por todo ello se pueden destacar tres características de una Constitución democrática para la organización social: en primer lugar, la autorreferencialidad individual, como autonomía de la libertad de ciudadanos iguales; en segundo lugar, la autorreferencialidad colectiva, como identificación entre gobernantes

General de los derechos fundamentales en la Constitución Española de 1978, Madrid, 2012, pág. 25 y ss..

¹³¹ BASTIDA FREIJEDO, obra señalada. Los ejemplos se orientan a los del autor.

tes y gobernados, una manifestación de la confianza en la representación colectiva; en tercer lugar, la positividad de la norma, como procedimiento para elegir y cambiar según el procedimiento establecido.

La idea de soberanía popular se manifiesta en la democracia a través de la organización del sistema jurídico como regulación de lo individual y de lo colectivo. Es la base de un Estado Democrático de Derecho: la neutralización de un poder soberano omnipotente que actúa sin reglas y también la falta de total control del Estado sobre el individuo, pues en nombre del pueblo soberano se han cometido demasiadas atrocidades contra la vida, la libertad y la igualdad. El sistema jurídico democrático se basa en una sociedad de individuos libres e iguales que garantiza también las libertades y la autonomía individual. Los DDFF son derechos, pues regulan las expectativas individuales y sociales; también son fundamentales porque la organización democrática de la sociedad los sitúa en la norma superior de todo el ordenamiento constitucional, con una supremacía jurídica única¹³². *El legislador y el individuo se encuentran limitados por el mismo concepto: la función social de los derechos fundamentales*¹³³. No está exenta esta afirmación de matizaciones por HÄBERLE. Existen diferenciaciones en función de las circunstancias y de la interpretación; por lógica, existen también límites para la función social en referencia a prevenir la unilateralidad, en suma, el totalitarismo de lo colectivo, olvidando al individuo, al sujeto, siendo los derechos fundamentales derechos públicos subjetivos; los derechos fundamentales son garantizados no sólo para el logro de un resultado colectivo, sino también se garantizan en los singulares sectores de la vida en favor del desarrollo de la personalidad individual. La libertad que impregna a los DDFF se une a la función social, pues los derechos individuales están interconectados al conjunto social del resto de ciudadanos, no a un solo individuo como tal. La dignidad de la persona es inviolable, aun en contra de los sen-

¹³² Exposición de BASTIDA FREIJEDO, obra citada, p. 28 y ss. Véase también VILLAVARDE MENÉNDEZ, I., "La intangibilidad competencial de los derechos fundamentales. Forma de estado y derechos fundamentales.", *Teoría y realidad constitucional*, nº 20, 2007, págs. 321-357, pág. 323 y ss..

¹³³ HÄBERLE, P., *La Garantía del contenido esencial de los Derechos Fundamentales*, Madrid, 2003, pág. 13 y ss. .

timientos o emociones humanamente admisibles en casos extremos de violencia o de situaciones difíciles de afrontar desde el Derecho. La estima del ser humano como tal, abarca a todos los individuos, eso engrandece al sistema jurídico democrático, generando garantías que protegen a los que considera el individuo sus oponentes, adversarios e incluso enemigos que no respeten los derechos subjetivos inviolables, los DDHH, porque los sujetos antijurídicos son también sujetos de derecho para un Estado democrático.

La redacción del texto del artículo 18.4 de la CE, que se ha analizado en su creación constitucional, no es afortunada, según parte de la doctrina. Y no lo es porque las limitaciones al uso de la informática y de las nuevas tecnologías de la comunicación son imposibles e inaceptables por la sociedad, no tiene sentido oponerse al progreso tecnológico¹³⁴. El constituyente otorgó protección de *rango constitucional* a los DDFF frente a la posibilidad de control que los sistemas informáticos y el advenimiento posterior de la sociedad de la información generaban. El bien jurídico protegido en el artículo 18 CE no es sólo la intimidad y el honor de los ciudadanos, sino también la libertad ante los tratamientos de información personal como consecuencia de la creciente automatización de la información. “Se trata de un derecho de libertad, que algunos llaman autodeterminación informativa”, en palabras de DÍEZ PICAZO¹³⁵. Los datos protegidos por el artículo 18.4 CE no son sólo los que corresponden a la intimidad, sino *cualesquiera otros datos relativos a la persona*¹³⁶. El artículo 18 se encuentra dentro de la Sección 1ª, “De los derechos fundamentales y de las libertades públi-

¹³⁴ DÍEZ PICAZO, L., *Sistema de Derechos Fundamentales*, Madrid, 2003, pág. 276. . Este autor expone una larga lista de textos internacionales sobre la protección de datos, algunos ya comentados. Como *Derecho de libertad* lo califica la autora SERRANO PÉREZ, M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, 2003. Y como libertad informática, en el caso que otros autores.

¹³⁵ DÍEZ PICAZO, obra citada, pág. 277. Se cita la STC 254/1993, de 20 de julio. Para aclarar más esta STC, véase también VILLAVARDE MENÉNDEZ, I., “Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo.”, *Revista española de derecho constitucional.*, nº 14, 1994, pág. 187-224.

¹³⁶ *Ibidem*. Se cita la STC 292/2000.

cas”, Capítulo Segundo, Título Primero de la CE¹³⁷. Su posición en el texto constitucional significa que el derecho a la protección de datos goza del más alto nivel de protección, como reserva de Ley Orgánica para su desarrollo (artículo 81.1 CE); vinculación de todos los poderes públicos y respeto de su contenido esencial por el legislador (artículo 53.1 CE); junto con la tutela de los Tribunales ordinarios bajo los principios de preferencia y sumariedad; en su caso, mediante recurso de amparo ante el TC (artículo 53.2 CE). Se consideraría el derecho a la protección de datos personales un derecho fundamental de configuración legal. La Jurisprudencia del TC distinguió en varias Sentencias una serie de Derechos fundamentales bajo lo que se denominó por el propio Tribunal como *derechos de configuración legal*, derechos con una doble naturaleza: son fundamentales, pero para su eficacia plena, deben contar con una delimitación legislativa¹³⁸.

El TC interpretó el artículo 18.4 como derecho fundamental independiente, estrechamente relacionado con el derecho a la intimidad del artículo 18.1¹³⁹.

¹³⁷ Véase STC 53/1991, de 14 de febrero, FJ5. Los derechos fundamentales se consideran los establecidos en este Capítulo Segundo del Título I CE.

¹³⁸ VILLAVERDE MENÉNDEZ, I., *El legislador de los derechos fundamentales*, Madrid, 2004, pág. 160. “Aparentemente la diferencia estriba en que, mientras unos derechos fundamentales tienen todo su contenido, objeto y límites abstractamente definido en el precepto constitucional que los contiene y el legislador sólo puede concretar lo que ya está en la Constitución, en los de configuración, sin embargo, la Constitución sólo establece un mínimo contenido del derecho a partir del cual, el legislador puede (o debe, según el caso) definir su diseño final.” Entre estos derechos se incluyen el derecho a salir libremente de España (artículo 19.2 CE); el derecho a acceder en condiciones de igualdad a las funciones y cargos públicos (artículo 23.2 CE); el derecho a la tutela efectiva (artículo 24.1 CE); el derecho de petición (artículo 29.1 CE) y el derecho a la protección de datos (artículo 18.4 CE) Véase también HERNÁNDEZ LÓPEZ, J., *El Derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional*, Cizur Menor, 2013, pág. 52-53.

¹³⁹ En este sentido la STC 292/2000, de 30 de noviembre FJ 5 afirma lo siguiente: “Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del artículo 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada, personal y familiar, atribuye a su titular un *haz de facultades* que consisten en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados *comportamientos cuya concreta*

Desde el inicio del siglo XXI, no se cuestiona la existencia del derecho a la protección de datos. Lo que todavía no está completamente unificado, es su concreta denominación. Se han utilizado anglicanismos como *privacidad*, traducciones como *autodeterminación informativa*, expresiones como *libertad informática* y latinismos modernos como *habeas data*¹⁴⁰. Esta multiplicidad de enunciados puede ser consecuencia de la discusión doctrinal que se generó durante años alrededor de la determinación de su fundamento. Una parte de la doctrina entendió que tenía su fundamento en el artículo 10 CE, o canon interpretativo de la CE y en el propio artículo 18.1 CE o derecho a la intimidad, de la cual era una manifestación tecnológica¹⁴¹. Otro sector doctrinal con-

regulación debe establecer la Ley, aquella que conforme al artículo 18.4 CE debe limitar el uso de la informática, bien desarrollando el Derecho fundamental a la protección de datos (artículo 81.1 CE), bien regulando su ejercicio (artículo 53.1 CE)” En su relación con el derecho a la intimidad, la STC 94/1998, de 4 de mayo, STC 254/1993, de 20 de julio y STC 290/2000, de 30 de noviembre.

¹⁴⁰ Véase el interesante análisis sobre las diferentes expresiones doctrinales en SERRANO PÉREZ, M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, 2003, pág. 171 y ss..

¹⁴¹ El artículo 10 CE declara en su punto 1 que los derechos inviolables de la persona, su dignidad, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás, como fundamentos incuestionables del orden político y la paz social. En su punto 2 establece que las normas relativas a los derechos fundamentales y las libertades públicas se interpretaran de acuerdo con lo establecido en la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre estas materias que se ratifique por España. Véase CUENCA GÓMEZ, P., "La incidencia del derecho internacional de los derechos humanos en el derecho interno: la interpretación del artículo 10.2 de la Constitución Española.", *Revista de Estudios Jurídicos. Versión electrónica.*, nº 12, 2012, pág. 1-24. También LEÓN BASTOS, C., *La interpretación de los derechos fundamentales según los tratados internacionales sobre derechos humanos*-, Madrid, 2010, pág. 120 y ss.. también BASTIDA FREIJEDO en BASTIDA FREIJEDO, FRANCISCO J.; VILLAYERDE MENÉNDEZ, IGNACIO; REQUEJO RODRÍGUEZ, PALOMA; PRESNO LINERA, MIGUEL ÁNGEL; ALDÁEZ CORRAL, BENITO; FERNANDEZ SARASOLA, IGNACIO, *Teoría General de los derechos fundamentales en la Constitución Española de 1978*, Madrid, 2012, pág. 30 y ss.. : “Si la CE no estableciese qué derechos o libertades son inherentes a la persona, qué derecho implica el reconocimiento constitucional de la dignidad humana, habría que deducirlos de esta referencia genérica del art. 10 CE.” Y también SÁIZ ARNAIZ, A., *La apertura constitucional al derecho internacional y europeo de los derechos humanos. El artículo 10.2 de la Constitución Española.*, Madrid, 1999, pág. 266 y ss.

sideró que tenía su fundamento en el artículo 18.4. CE¹⁴² Actualmente la mayoría de la doctrina considera que existe una clara distinción entre el derecho a la intimidad y

¹⁴² Posición que se mantuvo en las SSTC 290/2000 y 292/2000. El voto particular del magistrado JIMÉNEZ DE PARGA es un ejemplo de esta dualidad doctrina; por una parte, mantiene que el artículo 18.4 CE es un mandato al legislador para que limite el uso de la informática, es más, adopta el término libertad informática, frente al término empleado en la STC 292/2000 que es protección de datos personales. El magistrado considera el derecho a la libertad informática como una manifestación del artículo 10.1 CE, en cuanto derecho inherente a la libertad de las personas. Autores en esta misma tesis se encontraron RÚIZ MIGUEL, REBOLLO DELGADO, DEL CASTILLO VÁZQUEZ, en cuanto al tema de protección de datos. Existen otra serie de autores que entran en controversia sobre la consideración del artículo 10 CE como canon interpretativo de todo el sistema jurídico o sólo de los derechos fundamentales del Capítulo Segundo, Título I CE, como son SAIZ ARNAIZ o el autor PONCE MARTÍNEZ; las obras de referencia son generales sobre derechos fundamentales. Volviendo a la protección de datos, en la otra posición, que considera el derecho que se fundamenta en el artículo 18.4 como un derecho autónomo, destaca MURILLO DE LA CUEVA, TRONCOSO REIGADA y PÉREZ LUÑO. Véase también STC 36/1991, de 14 de febrero, El TC, delimitó el texto del artículo 10.2, en la Sentencia 36/1991, de 14 de febrero, con el siguiente mandato: "Esta norma se limita a establecer una conexión entre nuestro propio sistema de derechos fundamentales y libertades, de un lado, y los Convenios y Tratados internacionales sobre las mismas materias en los que sea parte España, de otro. No da rango constitucional a los derechos y libertades internacionalmente proclamados en cuanto no estén también consagrados por nuestra propia Constitución, pero obliga a interpretar los correspondientes preceptos de ésta de acuerdo con el contenido de dichos Tratados o Convenios, de modo que en la práctica este contenido se convierte en cierto modo en el contenido constitucionalmente declarado de los derechos y libertades que enuncia el capítulo segundo del título I de nuestra Constitución"(FJ 5). De este modo, en palabras del Tribunal Constitucional "aunque los textos y acuerdos internacionales del artículo 10.2 constituyen una fuente interpretativa que contribuye a la mejor identificación del contenido de los derechos cuya tutela se pide a este Tribunal Constitucional, la interpretación a que alude el citado artículo 10.2 del texto constitucional no los convierte en canon autónomo de validez de las normas y actos de los poderes públicos desde la perspectiva de los derechos fundamentales, es decir, no los convierte en canon autónomo de constitucionalidad". "Si así fuera, sobraría la proclamación constitucional de tales derechos, bastando con que el constituyente hubiera efectuado una remisión a las Declaraciones internacionales de Derechos Humanos o, en general, a los tratados que suscriba el Estado español sobre derechos fundamentales y libertades públicas". El Tribunal se remite a otras sentencias del mismo: SSTC 64/1991, de 22 de marzo (FJ4), 372/1993, de 13 de diciembre, (FJ7), 41/2002, de 25 de febrero (FJ2) y STC 236/2007 de 7 noviembre FJ5.

el derecho a la protección de datos, siendo éste último considerado como derecho fundamental autónomo. En este sentido puede darse el caso de que se pueda alterar o conculcar el derecho a la protección de datos personales y no cometer ningún acto contra el derecho a la intimidad, por ejemplo, publicando una foto en *internet* de los participantes a una actividad deportiva sin autorización expresa de los titulares de los datos, las personas reflejadas en la fotografía. Sin lugar a dudas, ambos derechos están relacionados, pero no protegen los mismos aspectos; tienen diferente objeto y bien jurídico protegido y no tienen los mismos contenidos. El objeto del derecho a la intimidad es la garantía a los ciudadanos de su ámbito íntimo, reservado, aquello que no desean que sea público puesto que sólo interesa a la persona y a su dignidad. Para ello el legislador limita el acceso a determinada información por parte de los otros sujetos jurídicos, sean estos poderes públicos u otros ciudadanos, generando un bien jurídico protegido como es el respeto que los demás deben ejercer ante el ámbito íntimo personal. Los otros desconocen esa información y respetan la falta de conocimiento. Cualquier intento de conocer es una agresión al derecho a la intimidad personal¹⁴³. El contenido del derecho a la intimidad lo integran las facultades de exclusión de conocimiento. El derecho a la protección de datos tiene por objeto la garantía de control sobre los datos personales, todos ellos, no sólo los de ámbito íntimo; control sobre cualquier dato o grupo de datos que pueda identificar o hacer identificable a un ciudadano. Los bienes jurídicos protegidos en el caso del derecho a la protección de datos son la información personal y junto a esta, las libertades públicas y los derechos fundamentales de las personas físicas. El contenido del derecho a la protección de datos es el conocimiento por parte del ciudadano de los tratamientos y usos posibles, otorgando o no su consentimiento para estas finalidades, teniendo a su vez una serie

¹⁴³ La exposición de REBOLLO DELGADO es muy aclaratoria: “cabe entender el derecho a la intimidad como la protección de la autorrealización del individuo. Es el derecho que toda persona tiene a que permanezcan desconocidos determinados aspectos de su vida, así como a controlar el conocimiento que terceros tiene de él. La intimidad es el elemento de desconexión social.” Es un derecho de libertad en la disposición de información personal que el ciudadano tiene inherente a su condición. Véase REBOLLO DELGADO, LUCRECIO; SERRANO PÉREZ, M^a MERCEDES, *Introducción a la protección de datos*, Madrid, 2008, pág. 34-40.

de facultades sobre la disposición de información personal, como es el acceso, la cancelación, la rectificación y la oposición al tratamiento de datos personales, destacando el conocimiento y control sobre la cesión de datos a terceros¹⁴⁴. La transcendencia de la dignidad humana se extiende por todo el texto constitucional y por la totalidad del ordenamiento jurídico. Cualquier ataque a la dignidad humana, sea cual sea la forma, debe tener una respuesta de protección por la Ley y los Tribunales. Si el medio para esa forma de ataque es un sistema mecanizado de proceso de datos, una forma de comunicación rápida o unas imágenes televisadas, siguen rigiendo la misma ley y los mismos principios. Por ello, las interpretaciones jurisprudenciales y de las Autoridades encargadas de la protección de datos personales deben definir y adaptar al rápido avance de las tecnologías la reacción de todo el sistema jurídico ante los nuevos casos de protección. Esta protección se materializó en multitud de ocasiones después de una agresión o violación del derecho a la protección de datos. Siendo un derecho de protección, su eficacia legal es muchas veces sólo reactiva.

El mandato del artículo 9 CE tiene relación con el artículo 10 CE, pues en su apartado 2 se determina que los poderes públicos promoverán las condiciones para que la libertad y la igualdad del individuo y de la sociedad sean reales y efectivas. El mandato incluye remover los obstáculos que impidan la plenitud de la libertad y de la igualdad hacia la participación de todos los ciudadanos en la vida política, económica, cultural y social. Es el artículo constitucional que consagra la eficacia del Derecho. El legislador tiene una tarea sumamente importante para ofrecer una respuesta adecuada a las cuestiones que las tecnologías plantean en el ámbito de los derechos fundamentales. El desarrollo pleno de la personalidad de cada ciudadano exige remover los obstáculos que se presentan en la utilización indebida de los medios tecnológicos, como son el monopolio de grupos limitados de unas tecnologías que no están al alcance de toda la sociedad o condicionar el ejercicio de la libertad y la igualdad de los ciudadanos. No basta para esta misión legislativa con establecer planteamientos puramente defensivos ante el progreso tecnológico, puesto que éste es también una forma de expansión

¹⁴⁴ GUERRERO PICÓ, M., *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Navarra, 2006, pág. 232-237.

de los derechos fundamentales, los cuales son todos interdependientes y están interrelacionados materialmente¹⁴⁵. El derecho a la protección de datos es un *instituto de garantía* a otros derechos, con una forma limitativa difícil de aplicar en la actualidad dentro de todo su rigor y eficacia¹⁴⁶.

El legislador dilató su labor de configuración legal del derecho a la protección de datos hasta 1992 con la LORDAT. Mientras tanto, los datos personales fueron objeto de usos abusivos y contradictorios con cualquier lógica de protección de derechos fundamentales. Desde transferencias de datos masivas a otros sistemas de gobierno, sin control ninguno, hasta usos invasivos de la intimidad y de la personalidad, como puede ser publicidad de todo tipo, uso de información privada (datos médicos, académicos) para sugerir servicios o prestaciones empresariales y profesionales, información laboral tratada para fines de selección de personal, entre otros tratamientos, tanto en soporte digital (entonces menos avanzado que en la actualidad, más lento pero efectivo en su entorno) como en soportes de papel, documentación en general que

¹⁴⁵ Véase a este respecto las ideas de PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010, pág. 347-350. Este autor considera el artículo 105 b) dentro de la dualidad intimidad e informática, y la separación de textos en la CE como un error del constituyente, pues los archivos y registros de la Administración del Estado son de vital importancia para los derechos fundamentales, al igual que es importantísimo dejar aspectos que afecten a la intimidad y a la tecnología en manos de lo que denomina juego de partidos, desconstitucionalizando su contenido. Señala también las repercusiones negativas de la dualidad de legislaciones, ordinaria para el artículo 105 CE y orgánica para el artículo 18 CE. Esta cuestión la resuelve, según el autor, la STC 18/1981 de 8 de junio FJ 5: “debe señalarse que la reserva de Ley que efectúa en este punto el art. 105 de la Norma Fundamental no tiene el significado de diferir la aplicación de los derechos fundamentales y libertades públicas hasta el momento en que se dicte una Ley posterior a la Constitución, ya que en todo caso sus principios son de aplicación inmediata.”

¹⁴⁶ TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio.*, Valencia, 2010, pág. 69 y ss.. El autor remarca dentro de la teoría de la norma que el artículo 18.4 CE es “un ejemplo de cláusula abierta, no de cláusula cerrada; de valor, no de regla constitucional. Es un precepto con muy poca densidad normativa. Por tanto, el contenido necesario y positivo de este derecho fundamental -las facultades que conforman su contenido esencial- se tiene que dibujar con una construcción indirecta: las garantías de este derecho fundamental se alcanzan limitando el fenómeno de la informática.”

era tratada sin las debidas consideraciones, sin conocimiento del afectado, sin su consentimiento, y sobre todo, sin medidas de seguridad. El artículo 18.4 CE estableció una limitación en cuanto al uso de la informática, pero no sólo frente a ella. Se establece un límite para garantizar el honor, la intimidad y el pleno ejercicio de los derechos, en general, de los ciudadanos, reconocidos en todo el sistema jurídico. El objeto del artículo 18.4 CE, de la LORDAT y de la LOPD (ambas expresamente en su artículo 1) es *garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas*. Se deduciría de estas afirmaciones que sólo se puede garantizar el ordenamiento constitucional y la garantía de otros derechos fundamentales si se protegen los datos personales¹⁴⁷. La protección no puede significar impedir el uso de la informática, lo cual fue y es imposible, sino compatibilizar con el respeto de los DDFF el tratamiento de datos personales, eliminando, a ser posible, la mayor parte de los riesgos que una utilización abusiva de datos personales podría provocar en los ciudadanos¹⁴⁸

3.2. Novedad y avance respecto a su tiempo. La nueva dimensión espacio-temporal de los derechos fundamentales. Sociedad e individuo.

El fenómeno de los sistemas automatizados de información fue (y es ahora mismo, con su constante avance) indudablemente una revolución porque supone una forma completamente nueva de organización, registro y utilización de la información personal¹⁴⁹. El citado cambio cuantitativo, fue de tal envergadura que obligó a considerar la problemática entre información e intimidad con un enfoque jurídico distinto. Porque en el inicio de toda la controversia, la posible amenaza de los sistemas automati-

¹⁴⁷ TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio.*, Valencia, 2010, pág. 74-75.

¹⁴⁸ SERRANO PÉREZ, M., "El derecho Fundamental a la protección de datos. Su contenido esencial.", *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, nº 1, 2005, pág. 245-265, pág. 124. La autora cita a MURILLO DE LA CUEVA.

¹⁴⁹ PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010, pág. 343.

zados de procesos de datos se visualizaba sólo en dirección a la intimidad, no en cuanto a otros aspectos del desarrollo personal, en cuanto a derechos y libertades fundamentales, como es en la actualidad¹⁵⁰. El artículo 18.4 CE representó un gran avance respecto a la situación anterior, pero también resultó un avance respecto a su tiempo, aunque, el texto constitucional español no sea tan explícito como el portugués. Se puede además añadir la crítica expuesta por la doctrina de la restricción del alcance a los ámbitos personal y familiar no sean propios del encuadre del derecho a la protección de datos dentro de las libertades públicas y sean consideradas como fragmentarias e individualistas¹⁵¹. En la actualidad, el ciberespacio permite ser más individual que nunca, pues un ciudadano puede crear su mundo y vivir sólo de él, llevando las nuevas tecnologías al extremo, generando una nueva intimidad. Por el contrario, ser ciudadano es ser parte de la sociedad que nos rodea, donde se participa y se toman decisiones que a todos afectan, formando parte de nuestro Estado social, democrático y de Derecho, base de la democracia y al que deben servir los DDFF. La democracia se sirve de los contrastes ideológicos, de la tolerancia y respeto hacia los otros ciudadanos. Los derechos fundamentales garantizan la libertad de los individuos (una autonomía privada, que constituye a la persona) y la participación de todos en la vida político-social de un pueblo soberano (una autonomía pública, que constituye al ciudadano) Pudiera ocurrir que el ciberespacio sea un espacio cerrado, de exclusión, en vez de un espacio público, abierto. Un espacio democrático es tal si todo el que quiere tener acceso a él puede hacerlo, es más una posibilidad que una decisión. El

¹⁵⁰ MURILLO DE LA CUEVA, P., *Derecho a la Autodeterminación informativa*, Madrid, 2009, pág. 1.

¹⁵¹ PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010, pág. 344-345. Para este autor existe un peligro de exegesis literal del artículo 18.4, dejando fuera los aspectos sociales y colectivos, que tienden a posibilitar el acceso de personas y grupos a la información que les afecte directamente. El equilibrio socio-político exige, a su vez, que se garantice la participación de los grupos sociales a los bancos de datos. Pérez Luño piensa que el problema no reside en impedir el proceso electrónico de información, lo cual considera necesario para el funcionamiento del estado moderno, sino que el problema estriba en asegurar un uso democrático de la información. Considera que “urge evitar que el desarrollo tecnológico produzca una modificación del poder en una sola dirección, para ser monopolio de unos grupos y no patrimonio de toda la población”

ciudadano puede acceder o no hacerlo. Eso no es lo determinante en cuanto a los DDFF. Lo más importante sería la posible participación libre de la persona, del ciudadano. Si pensamos, además, que en el ciberespacio actual las delimitaciones espaciales y temporales presentes en el mundo real no son tales, el objeto de los DDFF, aquello que se regula con su definición, queda en cuestión. ¿El tiempo, modo y lugar para regular el ejercicio de los derechos fundamentales establecidos en la CE, desarrollados por una forma jurídica adecuada según los artículos 53 y 81 CE es también viable constitucionalmente? La nueva forma de realidad permite que no exista una interacción social entre personas físicamente en un tiempo determinado y de modo tangible¹⁵². Se puede considerar que la aportación de las tecnologías a los derechos fundamentales es una nueva forma para su ejercicio según la materia, lo cual puede ser base para regularlos en esta manifestación. El ciberespacio existe, es un espacio, diferente al físico, pero real, con un lugar inexistente y sin límites temporales. En ese espacio virtual (pero real) una persona física no es tal, es *datos e información* que circula en ese sistema. La ausencia de límites físico-temporales añade un riesgo evidente al individuo, a la persona física: la falta de control en el ejercicio de los derechos fundamentales en cuanto a responsabilidad tangible de forma patrimonial o económica e incluso penal. Se puede incluso hablar de irresponsabilidad en caso de un ejercicio indebido, dañoso, vejatorio o simplemente inconsciente de los DDFF, sin la debida limitación. Ante esta visión individualista y liberal de los derechos fundamentales, se puede encontrar otra visión más social y estatal. Es la pregunta frecuente en los últimos años sobre si el Estado debe fomentar y facilitar los medios para acceder al ciberespacio, con el fin de garantizar la igualdad de oportunidades en cuanto al ejercicio de los derechos fundamentales, incluso a cargo del propio Estado, que lo forman los ciudadanos. Al no ser la única forma ni ser indispensable para el ejercicio

¹⁵² REBOLLO DELGADO, LUCRECIO; SERRANO PÉREZ, M^a MERCEDES, *Introducción a la protección de datos*, Madrid, 2008, pág. 34 y ss.. El autor considera que el uso de las telecomunicaciones y los sistemas automatizados permiten romper las barreras de espacio y de tiempo como hasta ese momento habían sido interpretadas.

de los derechos fundamentales, la respuesta puede ser negativa¹⁵³. O puede que un Estado moderno, donde la Administración Pública es electrónica, y gran parte de la economía también, con oportunidades de información, empleo, cultura, en un entorno digital, deba fomentar, incluso costear el acceso al espacio informático y tecnológico, pues puede ser que los ciudadanos que no puedan costearse los accesos de comunicaciones, el equipamiento informático o los programas, por no hablar de la formación en su utilización, estén siendo directa o indirectamente discriminados dentro de una nueva expansión de la sociedad, como es el ciberespacio.

Las preguntas son ¿dónde queda la protección a la información personal en un enfoque social?; ¿hasta dónde existe un derecho social a la información individual-y personal?; ¿qué tipos de datos son los que sólo el individuo debe poseer y controlar? no se trata de vivir, en la expresión de MURILLO DE LA CUEVA en una *casa de cristal* (¿totalmente democrática?)¹⁵⁴. La libertad nos es propia como seres humanos, no sólo por mandato y desarrollo constitucional. El Estado, como tal, va a tener derecho de acceso a una importante cantidad de datos personales, para cumplir con su actividad de organización como tal, como Estado. Pero el individuo, la persona, el ciudadano, al que corresponde toda esa información, debe mantener el poder de disposición y control sobre ellos. En palabras de FROSINE, “la libertad informativa representa una nueva forma de desarrollo de la libertad personal; no consiste únicamente en la libertad negativa del *right of privacy*, (...) consiste, también, en la libertad de informarse, es decir, de ejercer un control autónomo sobre los datos propios, sobre la propia *identidad informática*”¹⁵⁵.

¹⁵³ VILLAYERDE MENÉNDEZ, I., "Ciberconstitucionalismo. Las TIC y los espacios virtuales de los derechos fundamentales", *Revista Catalana de dret públic*, nº , 2007, pág. 19-42.

¹⁵⁴ MURILLO DE LA CUEVA, P., *Derecho a la Autodeterminación informativa*, Madrid, 2009, pág. 4. “veríamos así, en juego, no ya nuestra intimidad, sino, también, la identidad que nos es propia y, por tanto, la libertad que nos pertenece constitutivamente”

¹⁵⁵ GARRIGA DOMÍNGUEZ, A., "Una nueva exigencia de la libertad: La protección de los datos personales "sensibles"", *Dereito. Revista jurídica de la Universidad de Santiago de Compostela*, nº 2, 2000, pág. 54.

3.3. Consideración del derecho a la protección de datos como Derecho Fundamental de configuración legal. Su contenido esencial.

Como se expone en este texto, el derecho a la protección de datos de carácter personal se fue separando, en función de los hechos producidos por el desarrollo de las tecnologías de gestión de información y de la evolución de lo que se considera control sobre la propia información, del derecho a la intimidad, tanto en su concepto como en su regulación. En un primer momento, después de la CE, se reguló la protección al honor, a la intimidad personal y familiar. Muy posteriormente se regularon los aspectos de protección de datos. Una primera ley en 1992 y la actual de 1999. Existen serias dudas sobre la causa que produjo esa dilación en el tiempo, pues en Europa se había regulado la protección de datos personales en Constituciones y leyes de los diferentes Estados, como se muestra en el análisis que precede a estos epígrafes. Sólo cabe una respuesta: la falta de interés del legislador en regular la protección de datos en España. En los análisis que se aportan a continuación se aprecia con claridad que el desarrollo legislativo del derecho a la protección de datos personales, siendo un derecho fundamental de configuración legal, no fue afortunado, supliéndose tales insuficiencias con Sentencias del TC y con Informes, Resoluciones y Estudios de la AEPD, lo cual ante un derecho fundamental es claramente insuficiente. No se discute la categoría de derecho fundamental al derecho a la protección de datos, pero la necesidad legal de su definición y conceptualización promueve que su contenido esencial se presente afectado. Según la más remota jurisprudencia del TC, en la STC 11/1981, de 8 de abril, FJ 10, se establecía la definición de contenido esencial de los DDFF: “es aquella parte del contenido de un derecho sin la cual éste pierde su peculiaridad o, dicho de otro modo, lo que hace que sea reconocible como derecho perteneciente a un determinado tipo. Es también aquella parte del contenido que es ineludiblemente necesaria para que el derecho permita a su titular la satisfacción de aquellos intereses para cuya consecución el derecho se otorga.” Es el *límite de los límites, el límite*

*al legislador*¹⁵⁶, que no puede desvirtuar en el desarrollo legal del derecho fundamental, según el artículo 53 CE, las garantías que la CE otorga a los DDFF y es la garantía de su contenido esencial. El derecho a la protección de datos personales no es ilimitado, como no lo es ningún derecho fundamental, cede ante otros derechos cuando es necesario para preservar, por ejemplo, la seguridad nacional. La STC 292/2000, de 30 de noviembre, así lo reflejó en su FJ 11. Debe ser la ley, por acción del propio legislador, por lo que se denomina doctrinalmente *habilitación constitucional*, el acto que limite el derecho a la protección de datos, al mismo tiempo que lo desarrolla, tal y

¹⁵⁶ MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, Madrid, 1996, pág. 145 y ss. La garantía del contenido esencial es el "único límite de los límites que recibe expresa sanción constitucional. Su función es, por tanto, proporcionar un parámetro conforme al cual apreciar si el legislador que restringe el contenido constitucionalmente protegido *prima facie* de un derecho fundamental para preservar otros derechos o bienes constitucionales comprime, o no, tan acusadamente dicho contenido que, en la práctica equivale a su total desvirtuación." Las diferencias entre la concepción o teoría absoluta y la concepción o teoría relativa de los DDFF ocupan las páginas del autor, con referencia al principio de proporcionalidad, a la doctrina alemana, a las Sentencias del *Bundesgerichtshof* o Tribunal Federal Alemán (el equivalente al TC español), y las SSTC más interesantes en este punto. Destaca la STC que el autor transcribe literalmente, la STC 11/1981, la cual sostiene que estas dos teorías o vertientes de interpretación para la definición de los DDFF no son antitéticas, sino complementarias, pudiéndose utilizar conjuntamente (p. 150-151, obra señalada) El momento histórico y la situación se tiene en cuenta también para valorar tanto el contenido esencial como las interpretaciones del mismo. Distinción entre teoría absoluta y teoría relativa del contenido esencial que extiende MAGDALENO ALEGRÍA, A., *Los límites de las libertades de expresión e información en el Estado social y democrático de Derecho.*, Madrid, 2006, pág. 271.277. El autor se decanta por la teoría absoluta del contenido esencia de los DDFF, afirmando que existe un núcleo duro o resistente de contenido en los DDFF, el cual permanece inalterable y que debe ser preservado sin excepción, aun en casos en que existan justificaciones proporcionales a su restricción. Es una interpretación que el autor considera material, frente a la interpretación o teoría relativa que realiza una interpretación formal. En otro escrito el autor opta también por esta teoría absoluta de los DDFF: MAGDALENO ALEGRÍA, ANTONIO;, "Libertad de expresión y partidos políticos en la jurisprudencia del Tribunal Europeo de los Derechos Humanos.", *Anuario de la Facultad de Derecho de la Universidad de La Coruña.*, nº 11, 2007, pág. 431-450. En cuanto a los límites de los DDFF véase la clarificadora exposición de ABA CATOIRA, A., *La limitación de los Derechos en la Jurisprudencia del Tribunal Constitucional español*, Valencia, 1999, pág. 193 y ss.

como afirma la STC 292/2000, de 30 de noviembre. El contenido esencial del derecho a la protección de datos se encontró definido en las normas que lo configuran, generando derechos al titular y obligaciones al responsable del tratamiento de los datos personales, reconocidos en las leyes de protección de datos, en especial en la LOPD y su Reglamento, que son la transposición de normas europeas comentadas, a la espera de las precisiones sobre la nueva normativa del RGPD que nuestros legisladores realicen en un futuro próximo. En cualquiera de los casos, los derechos de acceso, rectificación, cancelación, supresión, oposición, información sobre el tratamiento de los datos, exigencia de la seguridad adecuada, junto con los denominados principios de protección de datos, entre los que destaca el principio del consentimiento del titular, generan un reconocimiento del derecho a la protección de datos personales por su contenido esencial, por tanto, aunque los datos no formen parte de su ámbito privado (o íntimo, como pueden ser datos de salud) por cualquier causa, el titular tiene derecho al control de los mismos, porque de lo contrario, como afirmó la STC 292/2000, de 30 de noviembre (FJ 10), “privada la persona de aquellas facultades de disposición y control sobre sus datos de carácter personal, lo estará también de su derecho fundamental a la protección de datos, puesto que, como concluyo en esta punto la STC 11/1981, de 8 de abril, (FJ 8) *“se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección”*. Esta última frase se debe tener muy en cuenta en este momento, donde se puede observar una creciente incertidumbre sobre el derecho a la protección de datos en la sociedad, la económica y la política global. Existen postulados críticos, indefiniciones y realidades que rebasan a la doctrina y a los legisladores¹⁵⁷.

¹⁵⁷ Algunos autores criticaron el modelo actual por su patente ineficacia en muchos casos. Como pequeña obra crítica a la antecesora de la LOPD, la LORDAT de 1992, véase RUIZ CARRILLO, A., *Los datos de carácter personal*, Barcelona, 1999. Véase OLIVER-LALANA, A., "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*, Madrid, 2013. Se volverá a esta referencia en epígrafes posteriores. Antes de este estudio, GUERRERO PICÓ, M., *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter*

Otro asunto controvertido doctrinalmente es la opción del legislador por el Derecho Público Administrativo. Este aspecto se presentó con el paso de los años como una fuente de normas rígidas y de dudosa eficacia, muy al contrario de lo que ocurría con el derecho a la intimidad, al honor y a la propia imagen, los cuales se regularon en leyes civiles y penales alrededor del concepto de intromisiones ilegítimas en caso de que no existiera el consentimiento del afectado o un mandato legal, cuya regulación en España no se modificó prácticamente desde 1982. La rigidez de la configuración del derecho fundamental a la protección de datos por ese carácter administrativo contribuiría a la problemática con sus reglas formales (formularios de solicitud de consentimiento, documentos de seguridad, por ejemplo), más que a la solución por la incorporación de usos efectivos, tanto tecnológicos como organizativos, como pudiera ser la privacidad desde el diseño y por defecto (en inglés *privacy by design and by default*), que forman parte integrada de cualquier sistema de seguridad de datos en general¹⁵⁸.

Centrando el punto de exposición, se analizarán las normas sobre intimidad y la anterior ley de protección de datos de 1992 muy resumidamente; y más extensamente toda la normativa actual sobre protección de datos.

4. La Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar

Personal, Navarra, 2006, pág. 329 y ss.. La autora proponía ya en ese momento una solución global para un problema global, como era el nuevo ciberespacio provocado a raíz de la implantación de internet, para no dejar sin contenido al derecho a la protección de datos personales. Otro autor muy crítico con el ejercicio de los derechos fundamentales y su protección a través de la AEPD es BOIX PALOP, A., "¿Una red donde todos somos menores de edad?", *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*, Valencia, 2010, pág. 419 y ss. En especial el texto en pág. 426, "el ejercicio de los derechos fundamentales y su expresión".

¹⁵⁸ Véase la línea crítica de ÁLVAREZ RIGAUDIAS, C., "El poder del usuario digital", *Hacia un nuevo Derecho Europeo de protección de datos*, Valencia, 2015, pág. 279.

Durante el tiempo previo a la entrada en vigor de la CE, fue aprobada la ley 62/78 de, 26 de diciembre, de Protección Jurisdiccional de los Derechos Fundamentales, como una fase previa y una forma de canalizar procesalmente los derechos fundamentales. El artículo 18 CE no resultaba protegido en su totalidad con esta norma. Fue el Real Decreto-Ley de 20 de febrero de 1979, la norma que amplió los derechos y libertades aludidos en el anterior artículo 1.2 de la Ley 62/1978, incluyendo la protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen. No incluyó, de nuevo, ninguna referencia a la protección de datos personales. Cuatro años después, en 1982, se desarrolla la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del Derecho al Honor, la Intimidad Personal y familiar y de la propia imagen¹⁵⁹.

La ley se consideró por la mayoría de la doctrina como defectuosa y precipitada¹⁶⁰. Fueron el TC y la jurisdicción ordinaria, con una afortunada labor delimitadora, quienes aportaron soluciones interpretativas, sin modificar esta ley, pero aplicando directamente el artículo 18 CE en los casos que se consideró necesaria la protección constitucional¹⁶¹.

¹⁵⁹ En su artículo 1 se dice que:

“1. El derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, garantizado en el artículo 18 de la CE, será protegido civilmente frente a todo género de intromisiones ilegítimas, de acuerdo con lo establecido en la presente Ley Orgánica. 2. El carácter delictivo de la intromisión no impedirá el recurso al procedimiento de tutela previsto en el artículo 9 de esta Ley. En cualquier caso, serán aplicables los criterios de esta Ley para la determinación de la responsabilidad civil derivada de delito. 3. El derecho al honor, a la intimidad personal y familiar y a la propia imagen es irrenunciable, inalienable e imprescriptible. La renuncia a la protección prevista en esta ley será nula, sin perjuicio de los supuestos de autorización o consentimiento a que se refiere el artículo segundo de esta Ley. El artículo 2 afirma que la tutela civil “del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales, atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia.”.

¹⁶⁰ PÉREZ LUÑO y MURILLO DE LA CUEVA, entre otros

¹⁶¹ FAYOS GARDÓ, A., "Los derechos a la intimidad y a la propia imagen: Un análisis de la jurisprudencia española, británica y del Tribunal Europeo de Derechos Humanos. 25º Aniversario de la LO 1/1982", *Indret. Revista para el Análisis del Derecho*, nº 4, 2007. Este autor analiza diferentes sentencias del TC

Los pronunciamientos del TC se basan en diferentes fundamentos para argumentar y delimitar conceptos del derecho a la intimidad. Actualmente, ¿no serían más asuntos a tratar bajo el concepto de protección de datos, a tenor del cambio en los medios de comunicación que actúan mucho más intensamente en las redes sociales, a través de *internet*? Tampoco explicó la Ley de 1982 la diferencia entre el derecho a la propia imagen y el derecho a la intimidad. Con esta Ley se alargó el tiempo de desarrollo de una norma que tratara ese asunto de la protección de datos hasta 1992, poco antes de la Directiva 95/46/CE, de 24 de octubre.

5. La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORDAT).

La LORTAD se consideró insuficiente para corresponder con una respuesta normativa a los tiempos en que fue promulgada. Tuvo una vigencia muy efímera, pues estuvo en vigor sólo desde 1992 a 1999, año en que se promulgó la actual vigente Ley de Protección de Datos de Carácter personal (en adelante LOPD) por tanto sólo tuvo siete años de aplicación. Llegó tarde en muchos sentidos, pues tanto en el ámbito internacional como en el ámbito español se estaban produciendo numerosos avances tecnológicos. Una parte de la doctrina no lo disculpa, pero lo justifica¹⁶². La LORTAD puso limitaciones a los abusos de la época de los años 80 y principios de los 90 del pasado siglo

en referencia a la Ley de 1982, como por ejemplo el asunto Paquirri (STC 231/1988); el asunto Tous-Montiel (STC 197/1991); Intimidad de un enfermo de SIDA (STC 20/1992)

¹⁶² MURILLO DE LA CUEVA, P., "La construcción del derecho a la Autodeterminación informativa", *Revista de Estudios Políticos*, nº 104, 1999, págs. 35-60, págs. 41-42. "...la LORTAD, básicamente una norma de carácter general que no ha sido complementada por otras de alcance sectorial, no ha previsto -ni podría haberlo hecho, aunque lo hubiera pretendido- soluciones para muchos de los problemas que afloran en (aquella ya lejana, paréntesis nota de esta tesis) la realidad. Porque lo cierto es que hemos llegado a una situación en la que se hace una utilización masiva de la informática en todas las relaciones sociales y surgen cada día nuevos supuestos de conflicto entre las exigencias que impone el progreso social y económico y las que derivan de la defensa de los derechos fundamentales del individuo"

XX, que sacudieron a la opinión pública con escándalos de tráfico organizado de datos de carácter personal.¹⁶³ Era imposible para los juristas considerar lícito lo que ocurría, o para politólogos o tecnólogos, alegar sorpresa o desconocimiento. Todos estaban al corriente de los posibles peligros que se materializaron en más de una ocasión, y, por supuesto, en más de las que fueron conocidas por la opinión pública, pues los casos comentados por la doctrina no dejan de ser los que se dieron a conocer a la prensa, en su mayoría relacionados en mayor o menor medida con actividades públicas o del sector público. Se piensa que otras muchas violaciones de seguridad se daban en empresas privadas sin que se conociera por la ciudadanía¹⁶⁴. En España se sucedieron los casos de riesgo de contaminación informática de las libertades, en los archivos informatizados de la policía¹⁶⁵.

¹⁶³ PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010, pág. 386. “Los veintiún millones de ciudadanos españoles, inmediata o potencialmente, agredidos en su intimidad y otros derechos fundamentales abrieron una brecha en la inconsciencia cívica y política sobre los peligros que entrañan determinadas manipulaciones de las nuevas tecnologías. Fue preciso llegar a esta situación para que el conformismo cotidiano de quienes tienen como misión velar por la tutela de las libertades, y quienes tienen como principal tarea cívica el ejercerlas, se viese agitado por la gravedad del riesgo y la urgencia que revestía su respuesta”

¹⁶⁴ El autor pone como ejemplos los bancos de datos del FBI, el Pentágono o de la CIA que en los años 70 almacenaban informes de ciudadanos sobre actitudes individuales para control político e ideológico, como parece ser que ocurrió con la comunidad académica; en este caso se almacenaban para la policía las consultas bibliográficas de alumnos y profesores a través de los archivos informatizados. Otro ejemplo es el caso del Instituto Nacional de Estadística de Francia y el sistema llamado SAFARI, cuyo proyecto fue suspendido, para evitar el cruce de ficheros. El caso con más incidencia doctrinal fue la Sentencia del TC de Alemania en el asunto de la Ley del Censo de Población, en 1983, sentencia que sienta la terminología muy ampliamente aceptada por la doctrina anterior a la misma de “autodeterminación informativa” y que posteriormente a la citada sentencia se transforma en término general para alegar el derecho a una serie de protecciones y acciones a favor del control de datos personales (quién, qué, cuándo y con qué motivo se pueden tratar datos de ciudadanos en una sociedad democrática)

¹⁶⁵ Como ejemplo se pone el caso “Curiel” ECHEBARRÍA, J., “elpais.es”]. El Diputado comunista fue detenido en el aeropuerto de Barajas cuando la cámara de una terminal del control de aduanas en conexión con el sistema informático del Ministerio del Interior, entonces denominado Berta, informó al agente de turno de sus antecedentes. Con esta misma referencia del diario El País se comentan otros

Una breve referencia a su articulado presenta influencias de los textos internacionales ya analizados en este estudio y que tenían algunos años de vigencia cuando la LORTAD fue creada. Como recordatorio, se menciona el Convenio 108 de protección de datos personales de 1981 del Consejo de Europa (ratificado por España en 1984) que establecía en su artículo 4 la obligación de los países firmantes de generar en su derecho interno las normas necesarias para garantizar el Convenio. También el Acuerdo de *Schengen* de 1985 para la supresión de fronteras entre los países firmantes supuso la creación de una base de datos personales para uso policial en Estrasburgo y por tanto se debían aplicar los principios de protección de datos personales.

El ámbito de aplicación de la LORTAD se estableció en el artículo 2.1: "La presente ley será de aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado". A continuación, se estableció un largo listado de excepciones, que parece ser el sistema general de la LORTAD. El párrafo 2.2 excluyó la aplicación de la LORTAD para los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general; también para los ficheros mantenidos por personas físicas con fines exclusivamente personales; los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales, cuestión que no quedó excesivamente clarificada, al igual que los denominados ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales; se consideraron también excluidos los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto

aspectos del funcionamiento de los archivos informatizados de aquellos años. El artículo informa de que D. José Barrionuevo, Ministro del Interior, entregó a Javier Solana, Ministro de Cultural, los 808 primeros expedientes de carácter político, entre los que se encontraban las fichas policiales realizadas en el régimen anterior de D. Felipe González, Presidente del Gobierno en esa fecha, y de D. Alfonso Guerra. Estas fichas fueron enviadas al Archivo Histórico Nacional.

http://elpais.com/diario/1989/07/23/espana/617148001_850215.html a 27 de julio de 2015

los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos.

El párrafo 3 del mismo artículo remitía a la legislación especial la regulación de los siguientes ficheros: los ficheros regulados por la legislación de régimen electoral; los sometidos a la normativa sobre protección de materias clasificadas; los derivados del Registro Civil y del Registro Central de Penados y Rebeldes; los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo, de la función estadística pública; los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio, Reguladora del Régimen del Personal Militar Profesional.

Es muy importante señalar que la LORDAT solamente se aplicó a los datos personales que se trataban por sistemas automatizados que, en realidad, era el mandato constitucional del artículo 18.4. Otros tipos de soportes no eran ni tan siquiera sugeridos, con independencia del tipo de datos que contuvieran. Otra curiosidad es la utilización en el texto por el legislador de 1992 del término privacidad, para definir el espacio protegido por la protección de datos frente a las definiciones de intimidad, ampliando la tutela a un sentido más abierto, utilizando el anglicanismo proveniente de EEUU y el mundo angloparlante.

El artículo 1 de la LORTAD definía su objeto, en desarrollo del artículo 18.4 de la Constitución Española. Quedó excluido de esta ley la protección del derecho a la propia imagen. En caso de una vulneración del mismo por medios informáticos, se aplicó la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y a la propia Constitución, a falta de una regulación más específica, ya que la Ley del 82 sigue en vigor.

La LORTAD tenía en el artículo 3 una serie de definiciones dentro de su articulado, traduciendo lo estipulado en las Directivas comunitarias. Como ejemplo, la definición

de dato de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables; o también la definición de fichero automatizado: todo conjunto de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

En el Título II, artículos 4 a 11, se establecieron los principios de la protección de datos de carácter personal: calidad de datos, almacenamiento, licitud, finalidad, información al afectado, consentimiento del afectado, protección especial de datos en relación al artículo 16 CE (ideología, religión, creencias, origen racial, salud, vida sexual)

En el Título III se regularon los derechos del titular de datos personales y su ejercicio. Son los derechos de información, acceso, rectificación y cancelación, impugnación e indemnización.

Los reglamentos de desarrollo de la LORTAD fueron dos. De una parte, el Real Decreto 428/1993, de 26 de marzo, mediante el que se aprobó el estatuto de la Agencia de Protección de Datos, la cual comenzó a funcionar en 1994. De otra parte, el Real Decreto 1332/1994, de 20 de junio, que desarrolló aspectos de la LORDAT. El Código Penal de 1995 tipificó por primera vez en España delitos contra la intimidad a través de tecnologías informáticas (artículos 197 y siguientes)

Las primeras Sentencias del TC resolvieron cuestiones en base a la utilización por parte de empresas de datos personales relativos a afiliación sindical de sus trabajadores y a la problemática del número de identificación fiscal, junto con el alcance del artículo 18.4 de la CE¹⁶⁶. Resumiendo, la STC 254/1993, de 20 de julio, estimó un recurso de amparo ante la negación de acceso a un ciudadano a sus datos en ficheros de la Administración Pública. Los argumentos de la Administración eran la falta de desarro-

¹⁶⁶ MURILLO DE LA CUEVA, P., "La construcción del derecho a la Autodeterminación informativa", *Revista de Estudios Políticos*, nº 104, 1999, pág. 35-60. El autor realizó un artículo en referencia a la LORTAD casi al final de su vigencia, analizando sentencias del TC sobre lo que denominó derecho a la autodeterminación informativa.

llo del artículo 18.4 CE. El TC consideró que se podía aplicar el Convenio 108 del Consejo de Europa sobre la Protección de Datos Personales, ratificado en ese momento por España, relacionando el artículo 18.4 con el 10.2 de la CE. El TC manifestó que: “... nuestra Constitución ha incorporado una nueva garantía constitucional con forma de respuesta a una forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los derechos fundamentales. En el presente caso estamos ante un instituto que es, en sí mismo, un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática” Mediante el aludido pronunciamiento se produjeron dos efectos a destacar. De un lado, se afirmó que el artículo 18.4 reconoce un derecho fundamental, el derecho a la protección de datos personales, que protege frente a las agresiones potenciales a la libertad (y a otros derechos fundamentales). De otro, por delimitar el contenido del derecho a la protección de datos acudiendo a la vía interpretativa del artículo 10.2 CE, en concreto, el Convenio 108.

La STC 143/1994, de 9 de mayo. tuvo como base la admisión de la constitucionalidad del número de identificación fiscal, conocido por NIF, que fue establecido por el Real Decreto 338/1990, de 9 de marzo, como un código numérico de obligada utilización en las relaciones entre las Haciendas Públicas y en las relaciones patrimoniales de cualquier tipo, incluso entre particulares. El TC, en este caso, no tuvo en cuenta otros ejemplos en los que se prohibió el NIF, como es el caso de Portugal, que lo prohíbe en su Constitución del 76; tampoco apreció los debates doctrinales de ese momento en Europa, ya que eran los momentos previos a la Directiva 95/46/CE. La asignación de números personales de identificación es uno de los temas más controvertidos en la Protección de Datos personales, debido a los riesgos inherentes a su utilización por ficheros públicos y privados. A través de la identificación numérica de una persona se registran con mucha más rapidez los datos referentes a ella. Es por eso que muchas legislaciones lo prohíben.

Las dos sentencias más significativas para la doctrina fueron la STC 11/1998, de 13 de enero y la STC 94/1998, de 4 de mayo. La primera porque el TC argumenta la existencia de un nuevo derecho fundamental: el control de los datos de una persona por ella misma. Alega el Tribunal¹⁶⁷, el derecho (entre otros) de oposición de un ciudadano a que “determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención”, lo que se denomina *Habeas Data*. El TC reafirmó la doctrina de la autodeterminación informativa o libertad informática, marcando la importancia de la finalidad en la utilización de los datos junto con el consentimiento libre e informado del titular de los mismos. Los hechos que se analizaron fueron considerados muy graves desde la perspectiva de la protección de datos¹⁶⁸. La Sentencia tuvo otra lectura significativa para el desarrollo posterior del derecho fundamental a la protección de datos personales. Se trata de la dimensión instrumental del derecho a la protección de datos en la medida en que sirve para garantizar otros derechos, fundamentales o no. En ese caso, el derecho a la protección de datos sería considerado instrumental respecto al derecho fundamental de libertad sindical reconocido en el artículo 28.1 de la CE¹⁶⁹.

6. La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

¹⁶⁷ MURILLO DE LA CUEVA, Obra citada. Página 46-48.

¹⁶⁸ La empresa (RENFE) responsable del fichero de afiliación sindical, cuya finalidad consistía en la deducción en el salario de los trabajadores de la cuota de afiliación sindical al que pertenezcan cada uno (si se daba el caso) e ingresarla en la cuenta del sindicato, utilizó esos datos para una finalidad diferente, detraer el importe del salario que autoriza la legislación laboral sobre el derecho de huelga.

¹⁶⁹ La STC 94/1998, de 4 de mayo, estableció la siguiente doctrina respecto al artículo 18.4 CE: “... no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona a la privacidad, según el neologismo que reza en la exposición de motivos de la LORTAD-pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la información de los datos personales propicie comportamientos discriminatorios.”

Lo que en un principio se presentó como un proyecto de ley de reforma de la PRODAT en alguno de sus artículos, sobre la base de un anteproyecto elaborado por el Gobierno con intervención de la Agencia Española de Protección de Datos (AEPD), terminó siendo una nueva ley Orgánica que la doctrina consideró completamente innecesaria e insuficiente. El Proyecto de Ley de reforma tenía como objetivos incluir la protección de los tratamientos de datos no automatizados y la regulación del acceso a los datos por terceros, ambas exigencias de la nueva Directiva 95/46/CE. Es cierto que quizá sólo se necesitaban algunos ajustes en la ley de 1992, en función de la Directiva 95/46/CE, pero la nueva configuración política pidió una nueva ley, y eso fue lo que ocurrió. Los recursos de inconstitucionalidad presentados a la ley del 92 se resolvieron con la nueva LOPD ya promulgada, en el año 2000, por lo cual, fue el TC quien aportó más luz a este asunto¹⁷⁰.

La LOPD no tuvo Exposición de Motivos, lo que no es habitual en nuestro sistema jurídico. No se adujo la causa para la nueva promulgación de la LOPD: La obligación de incorporar al Derecho Español la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de julio de 1995, relativa a la protección de las personas físicas en lo que respecta a sus datos personales y a la libre circulación de los mismos. La Directiva 95/46/CE tuvo como objetivo procurar el flujo de datos efectivo entre los distintos países de la Unión Europea, protegiendo los datos personales sin restar eficacia a las AAPP de los países miembros y de la propia Unión, además de potenciar el desarrollo del sector privado empresarial y profesional. La Directiva 95/46/CE generó, además, la obligación de la existencia en cada país miembro de una Autoridad independiente que supervise su aplicación (artículo 28) También se creó una autoridad comunitaria, el *Grupo de Protección de las Personas*, integrada por representantes de las autoridades de protección de datos de cada país miembro y un representante de la Comisión. Esta Autoridad a nivel comunitario informaría a la Comisión de los conflictos que su-

¹⁷⁰ Las divergencias de opinión están presentes en las sesiones del Congreso de los Diputados, por nombrar alguna, la de 25 de noviembre de 1999, reflejada en el Diario de Sesiones del Congreso (VI Legislatura, Nº 277)

gieran en la aplicación de la Directiva 95/46/CE entre los Estados Miembros y contribuiría en la interpretación homogénea de las diferentes normas nacionales (artículos 30 y 31) En el artículo 32 se estableció la obligación de los Estados Miembros de adaptar las disposiciones legales internas a la Directiva 95/46/CE.

la LOPD fue, para la doctrina, una continuación de la LORTAD, puesto que reproducía casi literalmente los preceptos de su predecesora, añadiendo artículos de la Directiva 95/46/CE, incluso los artículos que eran la base para los diferentes recursos de inconstitucionalidad se incluyen, curiosamente, en la (supuesta) nueva ley. La LOPD mantuvo la opción de su antecesora, facilitando la creación de ficheros y actuando a posteriori, una vez que han sido inscritos en el Registro General de Protección de Datos (art. 39 LOPD) En el art. 7 establecía expresamente la prohibición de creación de ficheros con la finalidad exclusiva de almacenar datos de carácter personal sobre afiliación sindical, ideología, religión, creencias, origen racial o vida sexual (recordemos, datos especialmente protegidos); además establecía mecanismos de control sobre tratamientos de datos que puedan presentar riesgo para los derechos de las personas. La LOPD no subsanó el defecto de su antecesora de pretender ser una ley general de protección de datos llena de excepciones, con una gran cantidad de referencias a leyes externas a la LOPD. Mantuvo también una fuerte referencia a la normativa sectorial precedente. En el art. 2 se apreciaba con claridad, sin embargo, que, aun existiendo exclusiones para su aplicación en el art. 2.2, mantenía su carácter supletorio, pero además en el punto 2.3 del mismo art. se establecía que los ficheros que se mencionaban se regirían por sus disposiciones específicas y por lo especialmente previsto, en su caso, por la LOPD, por lo que se estableció que dichos ficheros debían respetar los criterios generales establecidos en la LOPD¹⁷¹. La LOPD no estuvo exenta

¹⁷¹ TRONCOSO REIGADA opinó que la LOPD “se convierte así en una norma general del sistema que respeta la existencia de regulaciones específicas, pero trata de someter todos los tratamientos a la disciplina general de la Ley, por lo que se sitúa en el centro del sistema de protección de datos”. El autor dió un contrapunto a su opinión, mencionando en pie de página a Mercedes Serrano, la cual cita marcando que para SERRANO la aplicación de la LOPD no es automática a los sectores con legislación específica, sino que requiere de interpretación, como inspecciones sectoriales llevadas a cabo en Hospitales

de polémica doctrinal¹⁷². Fue el TC quien aportó más claridad a la definición del contenido del derecho fundamental a la protección de datos personales por medio de las Resoluciones a los diferentes recursos de amparo planteados¹⁷³. Entre esas Sentencias destaca la que conforma el epígrafe siguiente, que es, según la doctrina, el eje central de toda la posterior interpretación de la LOPD.

o entidades de crédito. TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio.*, Valencia, 2010, pág. 90-91.

¹⁷² PÉREZ LUÑO, A., "Sobre el arte legislativo del birlibirloque. La LOPRODA y la tutela de la libertad informática en España", *Anuario de Filosofía del Derecho*, nº 18, 2001, pág. 321-326. Dos años después de la entrada en vigor de la LOPD (que el autor mencionó como LOPRODA), Pérez Luño analiza esta ley desde un punto de vista crítico. Los datos aportados por Pérez Luño pueden ser interesantes, desde una perspectiva de 18 años. Véase también como interesante PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, 2010, pág. 389-392. Aquí el epígrafe se enuncia como "la LOPRODA: ¿Un ejemplo del arte legislativo de birlibirloque?" Otros contenidos del libro de 2010 están en el artículo de PÉREZ LUÑO, A., "La tutela de la libertad informática en la sociedad globalizada", *Isegoría: Revista de filosofía moral y política*, nº 22, 2000, pág. 59-68. La LOPD es calificada por el autor como una obra del "arte legislativo del birlibirloque" o "el arte de poner y quitar", tomando palabras de José Bergamín. El legislador del año 1999 reproduce en la nueva ley, bajo el gobierno del Partido Popular, la mayoría de limitaciones y excepciones *injustificadas* a las garantías de libertad informática que se daban en la anterior ley de 1992, con un comentario llamativo: el Grupo Parlamentario Popular había impugnado ante el TC esos contenidos en anteriores legislaturas donde no era partido gobernante, pero en esa legislatura apoyó esos contenidos recurridos.

¹⁷³ Cosa la cual al ya citado Profesor PÉREZ LUÑO le parece tan deplorable: "Hay que deplorar en cualquier caso que deba confiarse a nuestra, cada vez más atareada e hipertrofiada, magistratura, la corrección de las numerosas imperfecciones técnico-legislativas y materiales de la LOPRODA" PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010, pág. 420. Véase también ORTÍ VALLEJO, A., "El nuevo derecho fundamental (y de la personalidad) a la libertad informática. A propósito de la STC 254/1993, de 20 de julio.", *Derecho Privado y Constitución*, nº 2, 1994, pág. 305-332. También del mismo autor ORTÍ VALLEJO, A., *Derecho a la intimidad e informática*, Madrid, 1994. Es comentario de esta tesis añadir que después de 40 años de experiencia democrática comienza a ser clara la tendencia de los legisladores, poco interesados en establecerse en una posición, de posponer la eficacia de la ley a la jurisprudencia del TC. La jurisprudencia se respeta por todos, tiene el símbolo de la neutralidad y permite a la política liberarse de un trabajo arduo y poco entendido, por la falta de consenso. Al menos, eso se puede deducir, ante la falta de definición de tantas leyes y la posterior definición por mecanismos jurisprudenciales, tanto del TC como del TS.

7. La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre: Independencia y autonomía del Derecho Fundamental a la Protección de Datos personales respecto al Derecho a la Intimidad.

El Defensor del Pueblo presentó en marzo del año 2000 un recurso de inconstitucionalidad contra los arts. 21.1 ("Comunicación de datos entre Administraciones Públicas") y 24.1 y 2 ("Otras excepciones a los derechos de los afectados") de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal por vulneración de los artículos 18.1 y 4 CE y 53.1 CE. Estos preceptos reproducían el mismo texto contenido en la LORTAD y habían igualmente sido recurridos ante el TC, pero la derogación de la LORDAT hizo que el TC no dictara sentencia¹⁷⁴. La interpretación conjunta de los dos preceptos legales que fueron recurridos posibilitaba, en primer lugar, que pudieran hacerse cesiones de datos entre Administraciones Públicas para fines distintos a los que motivaron su recogida; en segundo lugar, que el titular de esos datos no fuera informado, cuando se recababan, de la posibilidad de dicha cesión, al no estar prevista en la norma que creaba y regulaba el fichero; en tercer lugar, que la propia cesión se efectuaba sin el consentimiento del afectado; y en cuarto y último lugar, que la autorización para efectuar esas cesiones pudiera contenerse en

¹⁷⁴ El Defensor del Pueblo recurre dichos artículos de la LOPD que tenían el siguiente contenido:

Art. 21.1 LOPD: Comunicación de datos entre Administraciones Públicas" Este artículo permitía la comunicación de datos entre Administraciones cuando "la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso"

Art. 24.1 LOPD: "Otras excepciones a los derechos de los afectados" el cual excepciona el principio de información en la recogida de los datos cuando ésta "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas" o "afecte a la persecución de las infracciones administrativas"

Art. 24.2 LOPD: los derechos de acceso, rectificación y cancelación (art. 15 y 16.1) "no serán de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección".

una norma de rango inferior a la Ley. Todo ello vulneraba lo dispuesto en el art. 53.1 CE al permitir que una norma de rango inferior a la Ley autorizara la cesión de datos entre Administraciones Públicas sin el consentimiento ni el conocimiento del afectado, incluso para fines diversos para los que fueron recogidos y automatizados. De este modo, la LOPD permitía que reglamentariamente se impusiera un límite al derecho fundamental a la protección de datos reconocido en el art. 18.4 CE, pues se permitía la cesión de datos personales sin previo consentimiento del afectado; limitación que tan sólo y de forma muy restringida podría establecer una Ley. Por otra parte, esa remisión al reglamento esconde una remisión en blanco al Ejecutivo para que fije a su arbitrio, justamente, esos límites, lo que contraría la reserva de ley que a tal efecto establece el art. 53.1 CE.

La Doctrina conviene que la analizada Sentencia del TC fue la más clara de todas las anteriores que trata sobre la existencia de un Derecho Fundamental a la protección de datos personales, con completa autonomía respecto al derecho a la intimidad, aunque ambos se encuentren regulados en el art. 18 de la CE¹⁷⁵. El contenido esencial del derecho a la protección de datos personales apareció claramente diferenciado. La Sentencia argumentó de tal modo que no muestra un nuevo derecho, sino una deducción lógica conforme a los tiempos y su evolución¹⁷⁶. El TC dedicó una buena parte de la STC 292/2000 a este cometido: diferenciar el derecho específico a la protección de

¹⁷⁵ Así autores como TRONCOSO REIGADA, MURILLO DE LA CUEVA, CANALES GIL o HEREDERO HIGUERAS ya intuía la misma teoría en el año 1996. Véase también MARTÍNEZ MARTÍNEZ, SERRANO PÉREZ, VILLAS-VERDE MENÉNDEZ, o DÍEZ PICAZO, en la misma línea. Como existieron varias denominaciones del nuevo fenómeno objeto de regulación, los autores aportaron también diferentes visiones, hasta que el TC unificó las definiciones.

¹⁷⁶ SERRANO PÉREZ, M., "El derecho Fundamental a la protección de datos. Su contenido esencial.", *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, nº 1, 2005, pág. 245-265. Serrano Pérez realiza en el año 2003 un análisis sobre el nuevo derecho fundamental, definido con acierto para la autora por el TC. Esta autora considera que el nuevo derecho no es una nueva creación sino una *deducción*: "a partir del uso de la informática de la existencia de un conjunto de facultades y posibilidades, esto es, de un contenido esencial que sólo pueden encuadrarse bajo esta categoría y que rebasa los límites de la intimidad"

datos del más general a la intimidad. Y lo hace con los siguientes argumentos¹⁷⁷. Por una parte, el diferente objeto de protección, pues el derecho a la intimidad protege los datos íntimos de la persona, los cuales, por su propia definición, deben ser excluidos del conocimiento por parte de las demás personas. El derecho a la protección de datos protege cualquier dato, *sea o no íntimo*. Este criterio facilita la eficacia del derecho y aporta seguridad a la protección de datos. Los datos que se protegen son todos aquellos que identifiquen o puedan identificar a la persona, pudiendo servir para la creación de los perfiles de personalidad. El contenido de este derecho fundamental no es el secreto, sino el control de los datos personales por su titular. El problema más esencial es el uso diferente a la finalidad para la que han sido recabados o su cesión a terceros de forma irregular (FJ 6) Por otra parte, atribuye una serie de facultades positivas (*haz de facultades*) al titular de los datos (FJ 6) para garantizar a la persona el poder de control sobre sus datos personales se hace posible y efectivo *imponiendo a terceros*, los responsables de los ficheros, *unos deberes de hacer*: exigencia de consentimiento del titular, obligación de ser informado sobre la finalidad para la recogida de los datos, derecho de acceso, rectificación, cancelación y oposición. De todo este abanico de facultades, la más resaltada fue la necesidad de consentimiento del afectado, de forma libre y consciente, denominado *consentimiento informado*. Por último, la protección de todos los derechos inherentes a la persona: sean o no constitucionales, y sean o no sean relativos a la intimidad y al honor de la persona. En palabras de TRONCOSO REIGADA, “para el Alto Tribunal, con la previsión del art. 18.4 CE, el constituyente establece un derecho fundamental en sí mismo frente a los riesgos que podría entrañar el uso de la informática, para garantizar no sólo el derecho a

¹⁷⁷ TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio.*, Valencia, 2010, pág. 133-140. Véase también HERNÁNDEZ LÓPEZ, J., *El Derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional*, Cizur Menor, 2013, pág. 98-100. Extenso análisis del autor sobre las SSTC. Para este autor, la STC señalada es el inicio del reconocimiento del derecho a la protección de datos personales como derecho autónomo y se diferencia claramente del derecho a la intimidad.

la intimidad y al honor, sino también el pleno ejercicio de los derechos de la persona.¹⁷⁸”

En el FJ 7 de la Sentencia, el TC definió específicamente el derecho a la protección de datos personales, sin utilizar el término *autodeterminación informativa* de la Sentencia del Tribunal Alemán de 1981, anteriormente mencionada en esta tesis por la doctrina, sino con una redacción propia y la expresión protección de datos, con el siguiente texto: “De todo lo dicho resulta que *el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.*”¹⁷⁹ La disposición y el control del titular sobre sus datos personales constituye el contenido esencial del derecho a la protección de datos.

El TC declaró la nulidad de los aspectos recurridos bajo el argumento de inconstitucionales por vulneración del artículo 53.2 (reserva de ley). Censuró también que la LOPD no fijara expresamente los límites al consentimiento para la cesión de datos entre Administraciones con una finalidad distinta a la autorizada por el titular de los datos personales en su recogida¹⁸⁰. En el ámbito de la doctrina, se puede analizar que

¹⁷⁸ TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio.*, Valencia, 2010, pág. 139.

¹⁷⁹ La definición pudo estar influida por la lectura de los borradores de la Carta de Derechos Fundamentales de la Unión Europea, donde ya se habla de este derecho como derecho autónomo, por parte del ponente de la sentencia, D. Julio Diego Fernández Campos, Magistrado del TC. Nota en página 132, obra citada de TRONCOSO REIGADA.

¹⁸⁰ HERRÁN ORTIZ, A., *El derecho a la protección de datos personales en la sociedad de la información.*, Bilbao, 2003, pág. 90-92. Será este asunto de la cesión de datos un tema muy discutido por su vulneración constante por parte de las empresas y profesionales. Véase también a TRONCOSO REIGADA, que se muestra crítico con la actitud del TC en esta Sentencia, respecto a los ficheros de la Administración Pública en varios de sus textos, entre ellos los que publica en las obras aportadas en la bibliografía. No es objeto de tesis la situación de los datos personales con las AAPP, sólo se apunta

la STC 292/2000, como bien en el mismo texto se refleja, suplió la labor del legislador abiertamente, definiendo el contenido esencial del derecho a la protección de datos para el Derecho español, tarea que debería haber afrontado el legislador de los años noventa del pasado siglo XX y que no realizó con suficiente efectividad¹⁸¹. Se reconoció la protección de cualquier información personal, aunque no sea relevante para otros aspectos o cuando fuera notoria, incluso para datos de acceso público, para cuyo tratamiento se necesita el consentimiento del titular.

7.1. El poder de disposición y de Control del individuo sobre sus datos personales.

La afirmación del TC tiene su antecedente en la doctrina del TC alemán de 1981. Actualmente, en una sociedad donde los datos viajan a la velocidad de la luz por los medios de comunicación, de dispositivo móvil a dispositivo móvil, de servidor a servidor de datos, parece una declaración de buenas intenciones más que una realidad hablar de *poder de disposición* de la persona sobre sus datos. Desde los más básicos (nombre y apellidos, dirección, teléfono) necesarios para que entregue un paquete la agencia de transportes, hasta los más íntimos (vínculos afectivos, tendencias sexuales, ideologías, historial médico), esos, que en un momento determinado la persona

como comentario. Prácticamente todos los autores citaron directa o indirectamente la Sentencia 292/2000 de 30 de noviembre, por su importancia posterior. Destacan GUERRERO PICÓ, M., *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Navarra, 2006, pág. 217 y ss.

¹⁸¹ Es cierta la ineludible influencia de la doctrina alemana en estos aspectos. Los autores doctrinales que se citan utilizan las referencias de la doctrina y la jurisprudencia alemana. El TC se ve en la situación de proveer un elemento de DDFF que la CE no tiene; aun hoy está por definir con rango constitucional el derecho a la protección de datos, dando como referentes el insuficientemente definido artículo 18.4 CE y la STC 292/2000, la cual, suponiendo un avance a su tiempo, en estos momentos de 2017 es ya un documento obsoleto ante los avances de las tecnologías y las nuevas formas de relaciones entre los ciudadanos. Con el nuevo RGPD de 2016, las diferencias serán todavía más notables.

no desea compartir más que con un cierto grupo, en confianza, o ni tan siquiera llegar a comunicar¹⁸². Es también cierto, que anteriormente en la Historia de la Humanidad las personas se informaban entre sí. Los datos personales existían y se almacenaban en la memoria de las personas (que es también un soporte de datos, visto desde esta perspectiva) Los poderes del momento generaron soportes más físicos, desde una piedra inscrita con datos de cualquier tipo, tabillas de arcilla, papiros o papel, en las sociedades evolucionadas. Los censos de población, activos en la más remota Historia de la civilización, eran formas de control de prestaciones económicas o militares, entre otras formas de racionalización del Estado; ejemplos de todo ello se encuentran en las formas de organización del Imperio Romano, basadas en datos personales. En el cristianismo se encuentran los Libros de Inscripción de fieles, con todo tipo de datos personales: nacimiento, filiación, matrimonio, ordenación sacerdotal o monástica, enfermedades, fallecimiento, traslados. Todos ellos eran soportes de datos y ficheros sin lugar a dudas. Como se ha mencionado, entrada la Revolución industrial, el papel y la mecanización de procesos de datos con las máquinas de escribir, los datos personales se hacen cada vez más precisos y densos, más fáciles de procesar y tratar con medios más rápidos. Las comunicaciones facilitaron aún más todos estos procesos. Por tanto, el tratamiento de datos personales en soporte no automatizado era una realidad desde el inicio de la civilización, y de la sociedad. Saber quién es quién interesó

¹⁸² Un ejemplo de la realidad práctica. En un ámbito empresarial se produjo el siguiente comentario: “Una psicóloga que conozco es capaz de conocer las tendencias sexuales de la persona, sus traumas infantiles y una buena parte de su inconsciente sólo con su presencia, por sus ropas, sus gestos y su modo de expresarse.” La sorpresa no se basa en las aptitudes de la psicóloga, que podrían ser ciertas o no, la sorpresa es el desconocimiento de esa profesional del simple respeto a la persona que analiza sin su consentimiento, pero de la que, además, se atreve a almacenar datos, editando, muy profesionalmente, un perfil, sin su conocimiento y sin su consentimiento. El caso se basaba en las capacidades de negociación, y en tener cierto poder sobre el contrario que se sienta a la mesa para llegar a un acuerdo. Ese poder se basaba en una serie de datos, ciertos o no, de estricto carácter personal e íntimo, que eran manejados sin escrúpulo ninguno para obtener una mejor posición. La finalidad es totalmente ilegítima, no se necesita la LOPD para saber que esa actuación violaba derechos básicos de la dignidad de la persona. Pero todo ello se realiza a diario en múltiples ámbitos de la realidad, tanto física como virtual, a través de datos personales.

al poder político, religioso y a la sociedad en general desde siempre, y sigue interesando¹⁸³. La ciudadanía se basa en el conocimiento. Disponer o no disponer de los datos propios, es una disyuntiva que no tiene siempre explicación. Por una parte, el propio interesado puede querer ser conocido en ciertos ámbitos por razones laborales, culturales o personales, todas ellas legítimas. Por otra, la sociedad no puede funcionar correctamente sin ese conocimiento de los otros y sus datos personales, aquellos que le identifican como persona y como ciudadano, que le hacen sujeto de derechos y obligaciones en la sociedad democrática en la que desarrolla sus facultades personales, amparado por los DDFF. La doctrina jurídica mostró en pasados años una resistencia a pensar en la protección de datos como un derecho autónomo que ampara otros derechos, considerándolo una invasión en el ámbito de derechos fundamentales como el secreto de las comunicaciones, el derecho a la intimidad y a la propia imagen o el derecho a la inviolabilidad del domicilio. Lo quisieron considerar como un derecho instrumental, tal y como sostuvo la STC 254/1993, de 20 de julio¹⁸⁴. Parece ser que el futuro se fue creando a favor de incrementar los ámbitos en los que el derecho a la protección de datos es cada vez más amplio, debido, sin lugar a dudas, a la

¹⁸³ Las intervenciones del poder político en las comunicaciones se remontan a sus inicios, en especial las intromisiones en la correspondencia, más adelante telégrafos y teléfonos.

¹⁸⁴ MARTÍNEZ MARTÍNEZ, R., "El Derecho Fundamental a la Protección de Datos: Perspectivas", , nº 5, 2007, pág. 57 y ss . El autor expone en 2007 bajo el epígrafe descriptivo "*El poder de atracción del derecho fundamental a la protección de datos*" que "en la práctica asistimos a un constante crecimiento del ámbito de lo protegido por el derecho fundamental a la protección de datos, y jurídicamente hablando, corremos el riesgo de invadir territorios fronterizos como el del secreto de las comunicaciones, el derecho a la propia imagen y quién sabe si en el futuro, y de la mano de la videovigilancia, el de la inviolabilidad del domicilio. (...) se corre el riesgo de reducir el artículo 18 de la CE a la idea de protección de datos. Es necesario ser conscientes de que, pese a la contundencia del aparato de tutela y sanción que ampara este derecho, ello no supone ni que la protección de datos sea la técnica más eficaz, ni la más adecuada. Sin embargo, la cuestión puede abordarse también desde otra perspectiva, seguramente más productiva, consistente en situar el derecho a la protección de datos en el plano de la función instrumental que la CE y la jurisprudencia del TC desde la STC 254/1993 le han atribuido. Por tanto, aunque en muchos de los casos en los que estén en juego los derechos del artículo 18 CE existieran tratamiento de datos personales, resultará esencial discernir tanto la realidad material de los hechos y los derechos de los afectados, como la técnica de tutela más adecuada."

enorme expansión de los dispositivos electrónicos, de fácil manejo por cualquiera, junto al desarrollo de los medios de comunicación, que convierten a la transmisión de datos en un *hobby* o un juego en manos de toda la población, la cual no es consciente en ese momento de las consecuencias. Los sistemas informáticos, esa combinación entre servidores de todo tipo (desde los decisivos servidores de gestión para las AAPP, como son la Sanidad, la Seguridad nacional o el ejército; hasta los servidores de videojuegos y películas) y programas informáticos orientados al almacenamiento masivo de datos personales y no personales, pero que pueden relacionarse rápidamente unos con otros (*big data*), generaron una situación cuestionable en cuanto al ejercicio de los DDFF. Cerrar el derecho a la protección de datos a un sentido técnico o instrumental ha sido imposible¹⁸⁵. El Derecho fundamental a la protección de datos amplía la protección constitucional a datos que tengan incidencia en el ejercicio de cualquier derecho, sean fundamentales o no. Los datos protegidos son cualquier dato que, junto con otros, pueda identificar a la persona y crear un perfil e incluso una línea de conducta, que sirvan a una u otra utilidad que en circunstancias presentes o futuras puedan suponer un riesgo o amenaza para la persona, ya no solo en sus DDFF, también en sus intereses, en su desarrollo, tenga conocimiento de esa amenaza o riesgo, o simplemente sea una sombra de duda a su alrededor. Ciertamente es que el derecho fundamental a la intimidad está relacionado con la protección de datos, pero no sólo es este derecho custodiado por la protección de datos personales. La intimidad se refiere a determinados datos que la persona desea que permanezcan desconocidos. La protección de datos se refiere al tratamiento de información personal, sea íntima o no, como puede ser el nombre o la dirección, datos imprescindibles para cualquier actuación o interrelación social: Quién eres, dónde vives.

Las dos posturas jurídicas de dos formas de ordenamiento y de Estado se muestran ante los hechos actuales como relevantes: la posición anglosajona de EEUU, en la que todo lo que no está prohibido está permitido en cuanto a tratamiento de datos; en el

¹⁸⁵ REBOLLO DELGADO, L., *Derechos Fundamentales y Protección de Datos*, Madrid, 2004. Véase las interesantes consideraciones de este autor en cuanto a fundamentar el derecho a la protección de datos sin olvidar el derecho a la intimidad.

lado opuesto se encuentra la posición europea-continental, en el caso del derecho a la protección de datos firmemente desarrollado por Alemania, Estado que mantiene una posición de prohibición de cualquier actividad o tratamiento de datos, salvo que esté permitida por el titular o sea obligada para situaciones de intervención estatal. El sistema jurídico europeo y en concreto, el español, optaron por prohibir cualquier tratamiento de datos personales que no esté expresamente permitido por su titular, salvo excepciones generadas por la ley o por situaciones de emergencia, individuales o sociales. La pregunta es ¿dónde queda el poder de la persona para disponer y controlar sus datos? Y en consecuencia, ¿Es real ese poder? o ¿es sólo un enunciado en la sociedad actual?¹⁸⁶

7.2. La obligación de hacer y la obligación de no hacer con carácter previo a cualquier relación.

La LOPD estableció una serie de obligaciones *de hacer* y *de no hacer* para los que fueran a tratar datos personales, denominados como responsable del fichero o del tratamiento de datos personales, sea de forma automatizada (soporte digital o informático) sea no automatizada (generalmente soportes en papel o plásticos, en la actualidad) Es el *haz de facultades* que la LOPD puso a disposición del titular de los datos. La STC 292/2000 en su FJ 6 estableció que el titular tiene como derechos o poderes jurídicos y los responsables de tratamiento de la información personal tienen como obligación determinados deberes jurídicos con carácter previo a su tratamiento, como son el requerimiento previo de consentimiento (informado, se verá) del titular de los datos personales para el tratamiento, la finalidad y la cesión de datos, si la hubiera;

¹⁸⁶ La doctrina se plantea muy seriamente si la legislación intensiva en esta materia tiene eficacia en las situaciones que se han ido plateando en los cambios sociales. Véase las ideas de BOIX PALOP, A., "El equilibrio entre los derechos del artículo 18 de la Constitución, el "derecho al olvido" y las libertades informativas tras la Sentencia Google.", *Revista General de Derecho Administrativo*, nº 38, 2015. Las obras de COTINO HUESO, las mencionadas de GARRIGA DOMÍNGUEZ, también de MARTÍNEZ MARTÍNEZ, entre otras que se aportan.

la información previa al titular de los datos de la finalidad, uso y destino de los datos recabados y la información previa al titular de dónde y cómo ejercer los derechos de acceso, rectificación, cancelación y oposición de sus datos personales (recordemos, derechos ARCO). Estos tres puntos conformaron principalmente *el poder de disposición* del titular sobre los datos personales. Existen otras obligaciones que son tratadas en la LOPD, como son el derecho a indemnización o el deber de secreto, además de proporcionar a los datos personales suficientes medidas de seguridad para su mantenimiento, acceso controlado por terceros o calidad de la información.

Igualmente obligó a esos mismos responsables a no realizar una serie de actos. Son las obligaciones de *no hacer*, que se manifestaron en la absoluta necesidad de cumplimiento de los mandatos contenidos en la LOPD, para no vulnerar la protección de datos. Entre las obligaciones de *no hacer* la más importante es no tratar datos sin consentimiento del titular y sólo tratarlos para la finalidad consentida. Otras obligaciones se podrían considerar la abstención de tratamiento de datos en casos de cancelación de los mismos, que deben mantenerse por razones legales o de otra índole obligatoriamente, pero que no deben ser tratados nunca más; no realizar cesiones de datos que no estuvieran autorizadas por el titular, salvo que sean obligatorias por ley o por mandato judicial; no tratar o ceder datos sin una finalidad conforme al consentimiento recabado; otro ejemplo habitual podría ser no realizar comunicaciones con un titular que no desea ser objeto de informaciones no autorizadas expresamente.

Si estos deberes y derechos *de hacer* y de *no hacer* se cumplieran, la protección de datos sería eficaz, sin lugar a dudas. Dos cuestiones se pueden aportar para que esto no ocurra: En la mayoría de casos el consentimiento no es otorgado por el titular con plena conciencia de las consecuencias. Bien se trata de un servicio que quiere conseguir, bien no tiene inconveniente en ese momento para otorgar el consentimiento, bien simplemente no tiene conciencia. El titular desconoce que es *sujeto* del derecho a la protección de datos personales. Ignora las consecuencias, porque no las conoce. Es un ciudadano sin formación jurídica, aunque en los últimos años se adquirió mayor conciencia sobre el derecho fundamental a la protección de datos, debido principal-

mente a las noticias que se han ido produciendo¹⁸⁷. Por otro lado, tenemos el enorme coste para las empresas que supuso la implementación de la LOPD, en especial las medidas de seguridad y de procedimientos en la gestión empresarial, en especial para PYMES, profesionales y autónomos. No se pueden catalogar las posibles situaciones que las pequeñas empresas pudieron experimentar en esas circunstancias. Las empresas multinacionales con enormes recursos jurídicos y de gestión se vieron muchas veces en situaciones de conflicto, pero pudieron solucionarlo con cierto nivel de acierto, aunque muchas de ellas, en especial las de sectores de telecomunicaciones y de servicios financieros, se vieron inmersas en constantes denuncias ante la AEPD, como muestran sus Resoluciones. Los medios y la influencia de las grandes empresas, en especial las multinacionales, con las implicaciones estatales que por su actividad y recursos tienen, no pueden ser comparables a los medios y recursos de las pequeñas y medianas empresas, que junto con profesionales de todo tipo (desde los oficios más sencillos y comunes, como mensajeros autónomos, fontaneros, peluqueros, autónomos de venta al por menor; hasta las profesiones más exigentes en capacidad y medios, como médicos, ingenieros, arquitectos o abogados) llevan más de 18 años obligados a cumplir la normativa de la LOPD, sin distinción de formación o de capacidad intelectual. El derecho fundamental a la protección de datos debe ser garantizado y facilitado por las empresas y profesionales, que son sujetos de derecho privado¹⁸⁸. Esta cuestión distorsiona mucho su naturaleza de derecho fundamental en la práctica. En otro lado se encuentran los tratamientos de datos que *ex profeso* tienen como finalidad actuaciones ilegítimas, ilegales, que violan expresamente el ordenamiento jurídico y los DDFF. Es un límite de este estudio, no entrar en consideraciones penales o en situaciones de degradación política, anticonstitucionales; sistemas de poder (de gobiernos reconocidos en muchos casos por el Derecho Internacional) que ejercen un tratamiento de datos personales para imponer un sistema de terror, antinatural, anti-

¹⁸⁷ DE LA TORRE OLID, FRANCISCO; CONDE COLMENAREJO, PILAR; , "Consideraciones críticas en torno a la autogestión y preservación de la intimidad en un escenario de riesgo", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, , 2014, pág. 56 y ss..

¹⁸⁸ No se trata el tema del ejercicio del derecho a la protección de datos por las Administraciones Públicas, las cuales sí tienen garantías del Estado a través de las competencias constitucionales.

social y antijurídico. Para este tipo de organizaciones criminales la respuesta no se encuentra en la protección de datos pues ni en mínimos el respeto por los Derechos Humanos más básicos no existe. Son delincuentes de todo tipo que aprovechan los sistemas de información y de comunicación para sus acciones antijurídicas. Los artículos 197 y ss. del Código Penal se encargan de considerar y tipificar como delito determinadas conductas relacionadas, pero no están todos los casos que se pudieran producir, además de un límite imposible de afrontar, como es la no territorialidad en la comisión de las acciones antijurídicas.

Por último, un comentario de reflexión sobre el uso y tratamiento de datos personales por el poder, sea el Estado, sean grupos estratégicos de empresas (pueden considerarse como tal los sectores de telecomunicaciones, financieros, energéticos, de información y se incluyen en este momento la enorme influencia de las redes sociales, sea por religiones, partidos políticos, asociaciones de gran calado social) La antijuridicidad existió siempre, y para sus fines necesitó y necesita información, no le es imprescindible que existan sistemas informáticos para manifestarse. Es cierto que los nuevos sistemas han conseguido una expansión sin precedentes de información personal y unos tratamientos insospechados. También se puede afirmar que los hechos que violan los DDFF son idénticos, aunque con otros medios. Al igual que se puede acabar con la vida de semejantes con las propias manos o con armas primitivas y el ingenio humano ha ido creando armas inimaginables, sofisticadas, basadas en muchos casos en ingenios cuya primera motivación no era la privación de la vida humana, se puede considerar que las mentes que desean lo antijurídico y antisocial van a utilizar elementos en principio inofensivos para cometer todo tipo de actos dañinos, violando, como no puede ser de otra forma y en primer lugar, los DDFF. La evolución humana no es culpable de estas conductas. La modernidad no significa mayor riesgo de vulneraciones. Es culpar, por ejemplo y a título de comentario, a la máquina de escribir manual, a las fábricas de papel, a la radio y al teléfono del Holocausto del régimen nacional-socialista alemán del pasado siglo XX¹⁸⁹. Los archivos que se generaron ante-

¹⁸⁹ Por no entrar en mayores determinaciones históricas, se escoge este hecho tan conocido. La URSS tampoco estuvo exenta de situaciones criminales masivas cuyas fuentes eran listados de ciudadanos

riores a ese momento fueron utilizados para generar un régimen de terror basado en la discriminación por razón de datos personales: raza, religión, familia, ideología política, sindicación, salud. Esos mismos sistemas de soporte en papel, los mismos medios de comunicaciones, la misma máquina de escribir, fueron utilizadas favorablemente para la sociedad del siglo XX en la consecución de derechos importantísimos como puede ser el derecho a la información, tan implantado en la sociedad moderna del pasado XX, fenómeno que no se había producido con esa amplitud anteriormente; derechos sociales como la educación o la asistencia sanitaria, que aportaron calidad de vida a los ciudadanos y un futuro mucho mejor del que somos esta generación la consecuencia, tenían como base listados, censos o expedientes con información personal. *Es el uso y finalidad del tratamiento de datos lo que produce situaciones de riesgo para los derechos fundamentales, no los medios técnicos empleados.*

Por todo ello un análisis se hace necesario: ¿Es eficaz la protección de datos como derecho fundamental que aporta la legislación ahora en vigor?; ¿Las violaciones al derecho a la protección de datos pueden evitarse?; ¿Son las empresas las obligadas a cumplir los mandatos de la LOPD o debería el Estado, como realiza con otros derechos

con datos personales. Las naciones como China o Corea del Norte todavía se encuentran en tesituras no calificables como democráticas y de respeto a los DDFF. Dentro de los países considerados democráticos, EEUU tuvo y tiene sus momentos difíciles en cuanto a tratamiento de datos personales y DDFF, como se expondrá en posteriores epígrafes. Quizá la diferencia estriba en que EEUU es una dinámica sociedad que se adapta rápidamente a sus nuevas conductas sociales, generando un Estado abierto a múltiples realidades, (como puede ser la aceptación del matrimonio homosexual por el Tribunal Supremo de EEUU el pasado mes de junio de 2015, algo impensable hace unos años, basándose en el derecho fundamental a la igualdad de todos los ciudadanos). Ese dinamismo se basa en una sociedad donde el derecho a la información sobre las actividades políticas es un ejemplo de control sobre el poder o poderes que se ejercen dentro de su sistema. En nuestra propia Historia puede decirse que los actos contra las personas y sus derechos fundamentales se produjeron con independencia de la tecnología empleada en los medios de información y soporte de datos. Por aportar un comentario, en el régimen anterior a nuestra democracia no necesitaban ni cámaras ni ordenadores: tenían lo que se denominaba como “portero” o “portera”, la persona que controlaba para el Régimen a todos los vecinos informando sobre sus actividades y su conducta. Eran los delatores, los que se interesan sin respeto por la vida de los otros, fenómeno social de toda sociedad totalitaria, sea cual sea su tipología de Estado.

fundamentales, ser el proveedor y el garante del derecho a la protección de datos? En los próximos epígrafes se tratará de despejar las incógnitas enunciadas.

CAPÍTULO CUARTO. LA PROTECCIÓN DE DATOS PERSONALES COMO GARANTÍA DE OTROS DERECHOS

1. Algunas Ideas previas. Los cambios tecnológicos de la última década (2007-2017)

A partir de este momento, la exposición de esta tesis se orienta hacia el presente y el futuro del derecho a la protección de datos personales. Los acontecimientos a escala mundial y los avances de las tecnologías, ante los que cualquier ámbito de la vida más cotidiana se expone actualmente, en esa dualidad de cambio positivo y riesgo de negativas consecuencias, hacen que se tenga la prudencia de no zanjar las situaciones posibles, pues mañana pueden aparecer otros motivos para entender que no se ha completado la misión del legislador ni del analista. Se van a mencionar brevemente los cambios tecnológicos de la última década (2007-2017) pues son sumamente representativos para las exposiciones que se desarrollan a continuación. Muy resumidamente, fue en el año 2007 cuando Apple lanzó al mercado su creación más espectacular: el iPhone 2G, un teléfono móvil con capacidades de PC, el primer *smart phone* o *teléfono inteligente*. Fueron los innumerables avances en comunicaciones de los últimos 10 años los que permitieron que funcionara en cualquier lugar como un pequeño PC transformándose en un sustituto del mismo, incluso con muchas más opciones. Destacaba entonces su capacidad de conexión a internet con acceso a la información que allí se expande a nivel mundial y algo que pasó en un primer momento desapercibido, pero sumamente importante para el desarrollo posterior de la denominada sociedad de la información: la incorporación de una cámara de captación de imágenes y de audios, como un pequeño dispositivo de videograbación, y una cámara de fotografía. Google generó un sistema operativo muy económico en el año 2008, denominado *Android*. Este nuevo sistema abarató considerablemente los costes de un *smartphone* y propagó los dispositivos en todos los sectores sociales. Otro hecho tecnológico muy importante, pero que pasó desapercibido entre la generalidad de la población en 2008, fue la creación por IBM del supercomputador *Roadrunner*, primer servidor de

datos masivos, ya superado ampliamente en la actualidad, o la fabricación de nuevos equipos para comunicaciones de la empresa *CISCO*. En 2010 *Microsoft* presentó el sistema operativo *Windows 10*, el cual será crucial para extender aún más los sistemas de datos y de comunicaciones. También en 2010 Apple lanzó otro producto muy importante, la tableta o iPad, un dispositivo portátil de pequeño tamaño, muy similar a los lectores de texto anteriores de *Amazon*, pero con la versatilidad de un PC y con pantalla táctil, que incorporó un teclado, táctil igualmente. Otras empresas, como Samsung, también siguieron a la compañía Apple en los desarrollos de dispositivos móviles o tabletas y teléfonos. La generación de programas o *software* para análisis masivos de datos, cada vez más eficientes y rápidos fue una constante durante toda la década. Se comienza a denominar *data mining* o *big data* el fenómeno tecnológico de captación, almacenamiento, procesado, análisis y tratamiento de todo tipo de datos por grandes instalaciones de servidores dispersas por todo el mundo, con programas como el *Hadoop* de la empresa IBM. Aunque las técnicas se realizaban desde los años ochenta del pasado siglo XX, fue en esta década donde alcanzaron una expansión sin precedentes. No se deben olvidar las plataformas de redes sociales, Facebook, Twitter, LinkedIn o Instagram, entre otras. Detrás de todo lo que se usa tan fácilmente, existen sofisticados programas o software de gestión, cada vez más avanzados junto a enormes instalaciones de servidores. A las redes sociales se une el comercio de bienes *on-line*, con *Amazon* o *Alibaba* como líderes mundiales de ventas y distribución, que se amplió a muchísimos pequeños empresarios, también hacia servicios cotidianos. Se debe mencionar el enorme impacto de los videojuegos, sector tecnológico en auge, al ampliar sus versatilidades a juegos en línea, con varios jugadores dispersos en el mundo. Se espera la extensión de las gafas de realidad virtual e incluso habitaciones para reflejar realidades virtuales, cuyo uso puede ser tanto para actividades de ocio como para otras no determinadas todavía, pero que se orientan a la empresa y a las actividades científicas. Otros nuevos avances son el denominado internet de las cosas o *Internet of things*, abreviado IoT. Se utilizan dispositivos totalmente cotidianos comunicados con servidores de almacenamiento y proceso de datos, como pueden ser lectores de consumo de gas y electricidad, electrodomésticos, básculas de peso, pul-

seras de *fitness*, por citar algunas versatilidades del IoT. Sus usos representan un excelente avance para la civilización. Sus riesgos existen también. Se van a diferenciar tres manifestaciones de los avances actuales, por sus extensas implicaciones en los DDFF, en especial en el derecho fundamental a la protección de datos personales, sin olvidar que se encuentran íntimamente relacionadas¹⁹⁰.

1.1. El *clouding* (nube) o almacenamiento y tratamiento de datos en grandes servidores interconectados por una red de comunicaciones.

Clouding, *cloud computing*, *cloud* o *informática en la nube*, son los términos que identifican servicios de programas informáticos y almacenamiento de datos en grandes sistemas de servidores dispersos en el mundo (*granjas de servidores*) o *servidores web*, a través de una red de comunicaciones, que usualmente es *internet*, pero que se abre a una nueva forma de comunicación en rejilla o *grid* (en especial para entornos de investigación y académicos). Se denominó en un principio *Software als a service* (SaaS) o servicios de programas de informática a través de redes de comunicación, de forma que diferentes usuarios ubicados en diversas localizaciones a nivel mundial, accedían a los servicios de gestión simultáneamente, por cualquier dispositivo (móvil o fijo) y en cualquier momento¹⁹¹. El sistema en *cloud* tuvo un espectacular desarrollo por sus enormes ventajas para los proveedores y para los usuarios, pues reduce significativamente los costes de equipos y de programas informáticos, mejora la actividad

¹⁹⁰ Véase por todo lo expuesto un resumido e interesante análisis de FRANZIUS, C., "Das Recht auf informationelle Selbstbestimmung", *Zeitschrift für das Juristische Studium*, nº 61, 2015.

¹⁹¹ Véase BELTRÁN PARDO, M., *Cloudcomputing, tecnología y negocio*, Madrid, 2013, pág. 5. Los autores ofrecen claridad de conceptos y muchos ejemplos. Interesante es la definición de *cloud computing* para la NIST (National Institute of Standard and Technology of US Departament of Commerce): es "un modelo de negocio que permite acceso remoto, según nuestras necesidades y bajo demanda, a través de una red de comunicaciones, a un conjunto compartido de recursos de cómputo configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser reservados y liberados de manera rápida con un mínimo esfuerzo e intervención por parte del proveedor."

pues no depende de horarios laborales o de ritmos planetarios (día-noche), la seguridad se aplica más eficientemente en instalaciones protegidas de forma económicamente asumible, realizando una protección ante ataques, tanto a las instalaciones físicas como a los contenidos almacenados y gestionados. Ofreció otra ventaja políticamente aceptada: los gobiernos que deseaban controlar policialmente a sus ciudadanos y sus contenidos encontraron más difícil su localización. Por otro lado, para diversos países supuso un reto en el control de la información relevante para la Seguridad Nacional.

El *cloud* se convirtió en un nuevo modelo de negocio para las tecnologías de la información. Incluso se ofrecía gratuitamente por algunas empresas (*Dropbox*, por ejemplo), pagando por el consumo de espacio de almacenamiento al llegar a cierto volumen o consumo de servicios efectuado, eliminando a millones de pequeños usuarios los costes de instalación de complicados sistemas para sus actividades profesionales con un precio muy competitivo. Se produjeron toda una serie de ventajas basadas en la automatización de los sistemas y rápida adaptación ante la demanda variable, evitando la temible y propagada *piratería* o uso indebido (sin abono del precio) de programas de software, en parte resultado de la crisis económica mundial. Las empresas proveedoras de servicios en *cloud* ofrecen en la actualidad el ya mencionado software como servicio (SaaS, *Software as a Service*), también la modalidad de plataformas como Servicio (PaaS) e Infraestructuras como Servicio (IaaS). Las empresas *Google*, *Amazon* o *Microsoft* fueron las pioneras en este nuevo modelo de negocio sumamente extendido, que en cierto modo se apuntó a finales de siglo XX a través de los sistemas de comunicaciones por mail gratuitos, las redes sociales y con las instalaciones en red de las grandes corporaciones y gobiernos que accedieron a Internet¹⁹².

¹⁹² Sirva como recuerdo la polémica MSN (Microsoft NetWork). Sobre este asunto de la creación de empresas en *cloud* existe una extensa literatura informática y amplia literatura jurídica, aunque las definiciones en leyes no han existido, quizá por la falta de inquietud para su regulación o porque los usuarios mostraron un evidente entusiasmo en el uso de servicios en *cloud*, que evitaban teóricamente riesgos y no tenían costes excesivos.

Desde el punto de vista de la protección de datos el asunto de gestión de datos en *cloud* no está exento de polémica en los últimos años. En el ámbito europeo, realmente se encuentra sin regular. Por una parte, los servicios que se unen a las infraestructuras de telecomunicaciones se encuentra regulados y definidos. En el lado opuesto, las nuevas actividades de los últimos años a través de internet se han desarrollado orientadas a incentivar la competencia y la economía, obviando la regulación. Con esa realidad, las empresas han optado por fórmulas de adhesión que les aplica las menores responsabilidades posibles y permiten todo tipo de actividades con una supuesta prestación de consentimiento del titular de los datos, poniendo en cuestión los DDFF de los usuarios, como son la protección de datos, la libertad, la privacidad, la transparencia del sistema (tanto en las telecomunicaciones como en la gestión de información); todo ello influye en la política de los gobiernos, como puede ser en la Seguridad Nacional, la protección de la propiedad intelectual, los casos de espionaje internacional y por supuesto los DDHH en general. Las nuevas fuentes de ingresos para las empresas tecnológicas, y también de provisión de bienes y servicios en general, son el acceso a datos a través de vías de telecomunicación. Por otro lado, las empresas tecnológicas se han creado nuevas fuentes de ingresos, apoyándose en la publicidad y en la captación de datos personales, es cierto, pero no es menos cierto que a su vez se ha innovado en servicios personalizados y dirigidos a las necesidades de los usuarios, que aceptan y utilizan, confiando en sus múltiples ventajas. Los problemas estriban en que los titulares de datos no aprecian los límites ni las garantías a sus derechos, a los cuales el prestador de los servicios está irremediabilmente obligado¹⁹³. El *cloud* no contempló en un principio la protección de datos, porque no se planteó fronteras

¹⁹³ Sirva como primeras referencias PÉREZ MARTÍNEZ, J., *Las reglas del juego en el ecosistema digital. Level Playing Field*, Madrid, 2016, pág. 2 y ss. Existen multitud de estudios a favor del *cloud*, por citar algunos en España ERCOLANI, G., "Análisis del potencial del Cloud Computing para las PYMES", *Cuadernos de Gestión de información*, nº 2, 2012. GUASCH PORTAS, V., "Cloud Computing, turismo y protección de datos", *Revista de análisis turístico*, nº 17, 2014, pág. 61-68. BUSTAMANTE DONAS, J., "Ética en la nube: Dilemas éticos y políticos en el modelo de computación en la nube (Cloud Computing)", *Argumentos de razón técnica: Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología*, nº 16, 2013, pág. 37-54.

territoriales y las regulaciones, en especial la europea, se basaba en áreas territoriales de los Estados miembros. Las empresas de todo tipo y actividad (financiera, turística, venta de bienes, por ejemplo) se enfrentarán a múltiples legislaciones, que debían aportar suficiente flexibilidad como para combinar entre sí las diversas normas.

1.2. El *big data*, o tratamiento masivo de datos.

La expresión que se pretende definir se refiere o se utiliza en dos conceptos diferentes. Por una parte, *big data* expresa el tratamiento de una gran cantidad de datos (personales o no personales) a través de sistemas automatizados con finalidades diversas por empresas (grandes corporaciones, pero también en la actualidad pueden ser PYMES), Estados e incluso con fines culturales o de investigación académica. Por otro lado, la expresión *big data* se refiere a las tecnologías que tienen como finalidad el tratamiento de esas enormes cantidades de información, a través del empleo de algoritmos y fórmulas estadísticas; en este caso la finalidad es realizar extracciones de información de los datos para utilizarla en la una mejor gestión. Otro concepto relacionado es *minería de datos (data mining)*, el cual incluye en el análisis de los sistemas automatizados datos de voz o de imagen, datos de relaciones o los *likes* de las redes sociales. Otro elemento relacionado es la inteligencia artificial, denominación que se aplica a una serie de programas informativos que pueden extraer continua información y procesarla a gran velocidad, con un resultado requerido, generando la impresión de inteligencia humana¹⁹⁴. Los ámbitos de influencia del fenómeno tecnológico *big data* abarcan múltiples aspectos, en la economía, la ciencia, la técnica, el derecho y la sociedad. El concepto de *big data* se abre a la asociación de los cambios producidos en los espacios socioculturales, económicos y políticos. El tratamiento masivo de datos no es nuevo, se han tratado siempre datos de forma voluminosa con los

¹⁹⁴ GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 28. Véase también BELTRÁN PARDO, M., *Cloudcomputing, tecnología y negocio*, Madrid, 2013, pág. 16 y ss. En la misma línea véase GIL GONZÁLEZ, E., *Big Data, privacidad y protección de datos.*, Madrid, 2016.

medios que tenían a su alcance en todas las civilizaciones, lo realmente asombroso es el volumen de datos que se llega a tratar en este momento, al contar con los elementos técnicos adecuados. La importancia del *big data* reside en su utilización para almacenar datos del pasado, tratarlos con medios técnicos y proyectar hacia el futuro los resultados de los análisis, influyendo en la toma de decisiones en todos los ámbitos de la existencia. Por ejemplo, en la producción de bienes y servicios se utilizan todo tipo de datos que se asocian o *cruzan* entre sí para conseguir una predicción lo más ajustada posible de la demanda de productos, antes de su fabricación e incluso antes de su diseño, consiguiendo una eficiencia nunca alcanzada para las empresas productoras, modernizando e innovando en sus estrategias empresariales. Otro ejemplo muy importante se visualiza para el sector de salud y prevención, donde el uso de tecnología *big data* proporciona, sin duda, beneficios sin fronteras en la prevención de enfermedades, fabricación de medicamentos, mejora de las condiciones de vida, decisiones políticas y económicas en relación al bienestar de la población. Entre todas estas ventajas, se presentaron en los últimos años nuevos problemas jurídicos ante el tratamiento y finalidad de los datos, que el legislador y la jurisprudencia no han resuelto siempre satisfactoriamente, en especial frente al derecho a la protección de datos personales en relación con otras áreas jurídicas. *Big data* y *cloud* son fenómenos tecnológicos que se encuentran íntimamente unidos en sus consecuencias¹⁹⁵. Los datos que son tratados en los sistemas *big data* proceden de los usuarios de la red, los propios titulares de datos personales, que, a través de sus mails, redes sociales, uso de diversos dispositivos (teléfono móvil, tabletas, televisión) abastecen de datos, personales y no personales a las empresas. Las personas comparten información porque les gusta hacerlo, se expresan en las redes sociales y en los medios de comunicación libremente. Ello no significa que sea negativo, simplemente se apunta su vulnerabilidad al carecer de regulación.

¹⁹⁵ DORSCHER, J., *Praxishandbuch Big Data. Wirtschaft - Recht - Technik.*, Wiesbaden, 2015. Un ejemplo empresarial en España es la exitosa gestión de INDITEX para la fabricación en días de prendas demandadas por sus clientes. La gestión de la demanda se realiza a través de un sofisticado sistema de análisis masivo de datos o *big data*.

1.3. El internet de las cosas o *internet of things* (abreviado IoT)

El internet de las cosas o IoT (a partir de ahora) se compone de un grupo o conjunto de objetos cotidianos que están comunicados por internet, enviando información a servidores que almacenan y tratan la información transferida con diversas finalidades empresariales. Son objetos que envían datos de su uso y funcionamiento a través de la red de comunicación. En esa definición se incluyen pulseras inteligentes que procesan datos de salud (pasos que se realizan, calorías que se consumen, temperatura corporal, horas de sueño, entre otros datos físicos), electrodomésticos, lectores de datos de consumo de energía, domótica, alarmas de seguridad, videocámaras, dispositivos de geolocalización, objetos que incorporen una onda de radiofrecuencia (RFID), para seguir su trayectoria, como una tarjeta de pago de autovías, por ejemplo, o en la identificación de mascotas. Sus grandes ventajas han propiciado que su uso se extienda sin limitaciones, pues permite un seguimiento de actividades que antes no era posible. Los riesgos estriban, como en los casos anteriores, en su falta de regulación, pues transfieren datos personales masivamente para su tratamiento y creación de perfiles. El incremento de este tipo de tecnologías propicia todo tipo de nuevas creaciones en áreas de la salud, por ejemplo, como son los administradores de medicamentos implantados en el cuerpo, marcapasos, prótesis inteligentes que transmiten información a los profesionales de tratamiento del paciente, para la investigación y mejora de las terapias, medicamentos y servicios. En otros sectores, los marcadores de presencia y las videocámaras generan datos para optimizar la seguridad en las instalaciones. Los ejemplos se ampliarán con más análisis, baste en este epígrafe con estos conceptos¹⁹⁶.

¹⁹⁶ Véase el interés que en el año 2011 suscitaba el asunto en LLÁCER MATACÁS, M., "La autodeterminación informativa en la sociedad de la vigilancia: *ubiquitous computing*", *Protección de datos personales en la sociedad de la información y la vigilancia*, Madrid, 2011, pág. 61 y ss.

2. El objeto de regulación en la protección de datos personales.

2.1. El artículo 1 LOPD

El artículo 1 de la LOPD definió el objeto de la norma analizada, que lo forman *la garantía y protección de las libertades públicas y los derechos fundamentales en relación al tratamiento de los datos de las Personas Físicas, en especial los derechos fundamentales al honor e intimidad personal y familiar*. Hasta el año 2007 no gozaron de expansión suficiente las normas respecto a la protección de datos, esperando las actuaciones que el Reglamento de desarrollo suscitó. El texto de la LOPD eludió una mención directa al artículo 18.4 de la CE, y tampoco hizo referencia a los medios por los que se realiza el tratamiento de datos personales para extenderse a los tratamientos automatizados y no automatizados de datos personales. Un detalle es la inversión en la mención de los derechos protegidos, realizando en primer lugar una mención a la salvaguardia de los derechos fundamentales, en general, para después realizar una referencia a los derechos de garantía del honor e intimidad personal. La LOPD dejó claro que pretendía un enfoque positivo, protegiendo derechos en vez de estableciendo limitaciones al uso de la tecnología o de cualquier otro medio de tratamiento de datos personales, por lo que se eludió mencionar la *limitación del uso de la informática* que se exponía en el texto constitucional. Así mismo, tuvo una importantísima vocación expansiva en cuanto a los derechos a los que pretendía proteger y frente a las acciones de tratamiento de datos, sean automatizados o no. El texto expresó el objeto de la ley que debe ser la protección y defensa de los derechos del individuo, del ciudadano del cual se recogen y tratan datos personales. El individuo tiene el derecho de controlar los datos que le pertenecen, aunque la sociedad le requiera datos para interrelacionarse. Sin los datos personales, los objetivos de una sociedad son difícilmente alcanzables, y en la actualidad, el propio titular quiere disfrutar de las ventajas de la interrelación social a través de los medios tecnológicos, por lo que aporta todo tipo de datos personales sin pesar y sin ser advertido de los riesgos. La

regulación de la LOPD estableció ciertos límites a los tratamientos de datos personales, pero también igualmente se fueron estableciendo límites al derecho a la protección de datos, por requerimientos en su mayoría, administrativos y del Estado Social. El fenómeno de la auto-desprotección de los datos personales, por el que el ciudadano expone datos con su consentimiento y permite su tratamiento pudiera ser un auto-límite al derecho a la protección de datos en favor de las ventajas de la sociedad de la información y de la tecnología¹⁹⁷. Se pensó por la doctrina, que la falta de mención del artículo 18 CE y la falta (ya mencionada) de Exposición de Motivos en la LOPD tenían relación, pues parece claro, en el año 2017, que se intentaba evitar en 1999 dar la impresión de que *estábamos ante un nuevo derecho fundamental*, tan impor-

¹⁹⁷ MURILLO DE LA CUEVA, P., "El Objeto de la Ley Orgánica de Protección de Datos de Carácter Personal", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, 2010, pág. 75-96. Véase también en la misma línea doctrinal SERRANO PÉREZ, M., *El derecho fundamental a la protección de datos. Derecho español y comparado*, Madrid, 2003, pág. 254. Otros autores consideraron que la definición del objeto de la LOPD no era preciso como en la LORDAT de 1992, entre ellos REBOLLO DELGADO, LUCRECIO; SERRANO PÉREZ, M^a MERCEDES, *Introducción a la protección de datos*, Madrid, 2008, pág. 55. La anterior ley de protección de datos establecía como objeto "limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos". El autor en su crítica afirmó: "Parece claro que el artículo citado (artículo 1 LOPD) referencia más la pretensión última del legislador que el propio objeto de la ley, que no es otro que la protección de datos. La LORDAT siguió el tenor literal de la CE, mientras que la LOPD aportó las novedades de las regulaciones europeas comentadas, en especial la Directiva 95/46/CE. Otras matizaciones aportó la autora DEL CASTILLO VÁZQUEZ, I., *Protección de datos: Cuestiones constitucionales y administrativas: el derecho a saber y la obligación de callar*, Madrid, 2007, pág. 324. La autora entendió que, si el objeto de la LOPD en su artículo 1 era la garantía y protección de los datos personales, de las libertades públicas y de los derechos fundamentales en cuanto a su tratamiento, la LOPD extendió su tutela a todos los datos de carácter personal registrados en cualquier soporte y a todo tipo de tratamiento o uso, tanto por el sector público como privado. La protección no se reduce a los datos íntimos de las personas sin a cualquier tipo de dato personal. La finalidad de la LOPD no es la protección de los datos personales, sino la protección de la información personal en función del tratamiento que se les aplique, con el objetivo de proteger la libertad de la persona y su desarrollo, como afirma GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 160.

tante como cada día se nos presenta en estos posteriores años trascurridos desde esa fecha¹⁹⁸. Es llamativo que sólo un año después del debate de la LOPD se produjesen casi simultáneamente varios hechos (que aseverarían en su certeza la intuición de la diputada mencionada a pie de página) dando carta de naturaleza al derecho fundamental a la protección de datos de carácter personal, como fueron la STC 292/2000, de 30 de noviembre, y la elaboración de la Carta de los Derechos Fundamentales de la Unión Europea, aprobada como Declaración de Jefes de Estado y de Gobierno de Niza, el 7 de diciembre de 2000. Como se dijo en su epígrafe correspondiente, la Carta goza actualmente del mismo rango normativo que los Tratados. La resistencia del legislador a mencionar un nuevo derecho fundamental no mencionado en la CE se hizo tan evidente, que es imposible no reconocerlo¹⁹⁹. Pudiera ser que el legislador no quisiera invadir los espacios correspondientes a la CE y al poder constituyente. Aun así, fue una solución fácil que tomó el legislador de 1999, el cual no intuyó lo que iba a suponer la creación de nuevos dispositivos, programas y medios de telecomunicaciones, que unidos entre sí, formarían lo que en aquellos momentos algún autor podía pensar que era la *sociedad en red*. Además, la sociedad no se había percatado de los riesgos

¹⁹⁸ La diputada del Congreso, Sra. Uría Echevarría, que fue diputada por el Partido Nacionalista Vasco por la circunscripción de Vizcaya hasta 2008 se situó delante de sus compañeros diputados en la sesión de debate de la LOPD, apuntando que “el proyecto que examinamos es una ley orgánica que pretende regular un derecho fundamental, la protección de los datos personales, que forma parte más que del derecho a la intimidad, como se ha dicho, del derecho a la autodeterminación informativa (...) basada en la combinación entre los artículos 18.4 –que sólo habla de la protección frente a la informática; la ley va más allá-junto con el artículo 10.2 de la CE y las normas del Convenio 108 del Consejo de Europa, sobre las facultades que han de ser reconocidas a las personas en lo que hace a la tutela de sus datos”.

¹⁹⁹ MURILLO DE LA CUEVA, obra citada. El autor expresa así la justificación que propone para la actitud del legislador de 1999: “Resistencia que podría apelar en su justificación a la misma noción sustancial de Constitución que se ha consolidado en nuestra cultura jurídica. Aquella que se vincula a la separación de poderes y a la garantía de los derechos de las personas –hoy diríamos derechos fundamentales– desde la Declaración de los Derechos del Hombre y del Ciudadano de 26 de agosto de 1789. (...) no es extraño que, más allá de las convicciones que pudieran mantener sobre el significado sustantivo de la protección de datos personales, los legisladores prefirieran prescindir de toda manifestación sobre el particular para no invadir el espacio propio del constituyente ni el que corresponde al TC.”

en los que había estado desde los años ochenta del siglo XX, circunstancias que se mencionan como resumen, y es al principio de la primera década del siglo XXI cuando la importante informatización de la Administración Pública junto con el funcionamiento de las grandes corporaciones a nivel mundial (la denominada *globalización*) generaron un impresionante movimiento de datos, también a nivel de datos personales, que pusieron en riesgo los DDFF de las legislaciones europeas. Es verdad que la doctrina elaboró múltiples análisis, pero los autores no tenían tampoco la visión de futuro que después se desarrolló en la realidad. Los hechos fueron anteriores a la Ley, esta vez, como ya se ha comentado, a una velocidad de cambio social inalcanzable por los estudiosos del Derecho, tanto legisladores, como jurisprudencia o doctrina en general²⁰⁰.

La inacción en España contrasta con la actividad europea en la regulación de la protección de datos personales, se recuerda, desde el Convenio 108, la Sentencia del Tribunal Federal de Alemania de 15 de diciembre de 1983 sobre la ley del Censo, la Directiva 95/46/CE del 95 y el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, que cobra vigencia en el Tratado de Lisboa. La STC 292/2000, de 30 de diciembre se consideró por la doctrina como excepcional, pues en su contenido jurídico ni explica un derecho constitucional, ni complementa el régimen jurídico de la CE, sino que reconoce un derecho que no fue incluido en la propia Constitución. La Sentencia realizó una operación compleja e interpretativa del artículo 18.4 CE con las

²⁰⁰ MURILLO DE LA CUEVA criticó esta pasividad ante los hechos como “la escasa conciencia de la necesidad que viene a satisfacer el derecho la protección de datos y a la consistencia del derecho a la intimidad explican la fuerza con la que se razonó desde las categorías propias de éste y el poco interés habido en dictar la ley que limitase el uso de la informática prevista por aquel precepto constitucional.” El interés era tan escaso que “fue necesario esperar catorce años para que se aprobara y aún sucedió que el origen de la LORTAD no se debe a que las Cortes Generales sintieran la urgencia de cumplir un mandato del constituyente, ni a que percibieran la entidad de los riesgos que acechan a los individuos como consecuencia del uso incontrolado de información personal, sino a que era preciso dotarse de un sistema de protección de datos de carácter personal para entrar en el Acuerdo de Schengen, objetivo de política europea perseguido por España.” Murillo de la Cueva dedica un epígrafe completo de su análisis titulado “El reconocimiento del derecho fundamental visto desde 2009, diez años después de la promulgación de la LOPD.”

posibilidades que le otorgaba el Derecho Internacional y el derecho de la CEE, a través de los elementos integradores de la interpretación normativa que permite el artículo 10.2 CE, como se ha comentado, definiendo ejemplarmente un nuevo derecho para el ordenamiento español.²⁰¹

Si se hubiera extendido un análisis al futuro, visionando las posibles amenazas al derecho fundamental a la protección de datos personales, se observa que se pudieron prever con muchas coincidencias reales, las posibles soluciones a las amenazas y lesiones a DDFF constitucionalmente reconocidos. Sin esa prevención, pocas soluciones se pudieron aportar. La colisión con otros derechos fundamentales se produce en la práctica igualmente, como son la colisión con la libertad de expresión, la libertad religiosa, el derecho de acceso a los Registros y Archivos Administrativos, las pretensiones de aprovechamiento económicos de datos personales, la exigencia de la seguridad pública o privada. Ante todos estos retos y amenazas, el derecho fundamental a la

²⁰¹ Obra colectiva citada, página 90. MURILLO DE LA CUEVA se referenció a sí mismo y también a Ricard Martínez en esa página. Ambas citas también se tratan en esta tesis. MURILLO DE LA CUEVA, P., "La Constitución y el derecho a la autodeterminación informativa", *Cuadernos de Derecho Público*, nº 19-20, 2003, pág. 27-44. y MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica a la autodeterminación informativa*, Madrid, 2004. Debió de ser un reconocimiento muy importante para ambos autores que el TC utilizara sus teorías como base para su Sentencia. En su texto el autor afirmó la excepción de la doctrina del TC en la sentencia 292/2000, pues el TC: "Aquí ha reconocido un derecho que no está escrito en la Constitución mediante una operación interpretativa compleja, construyéndolo con los materiales que le ofrece el artículo 18.4 gracias a la luz que le suministran el Derecho Internacional y el ordenamiento comunitario. Con la iluminación que proyectan esos elementos integradores de la interpretación de las normas sobre derechos a los que remite el artículo 10.2 de la Constitución el Tribunal Constitucional ha podido hallar en la Constitución este nuevo derecho y presentarlo con sus rasgos principales bien definidos." Murillo de la Cueva reconoció en ese epígrafe la importancia del reconocimiento del derecho autónomo y fundamental a la protección de datos personales, con la enorme carga de consecuencias y garantías, tanto normativas como judiciales, "en el aseguramiento de un contenido esencial frente al legislador". Pero también recogió las críticas a una posible limitación de la potestad legislativa. Aunque afirma que ya en el año 2009 esas cuestiones estaban superadas en la práctica, por el Tratado de Lisboa y por el Tribunal Europeo de Derechos Humanos, el cual se manifestó de manera muy próxima al TC, en Sentencias del año 2000, 2005 y 2008, que el autor referenció. En la actualidad, no es motivo de discusión.

protección de datos es un derecho en posición preferente pues otorga un sustrato material que consiste en evitar los prejuicios que ocasionaría la lesión de DDFF a través del uso antijurídico de datos personales.²⁰²

Existen dos cuestiones respecto al objeto de la LOPD, actualmente muy presentes. Por una parte, la falta de concienciación social, tanto individual (las personas, los ciudadanos) como colectiva, de autoridades públicas, entidades sociales y empresariales, de la auténtica necesidad de protección de los datos personales. Este peligro aumenta cada día porque las amenazas de usos indebidos por terceros de datos personales junto con los avances tecnológicos para captar, transmitir en tiempo real y conservar indefinidamente informaciones, datos, incluido los de carácter personal, son difíciles de separar de cualquier evento humano. Por otra parte, la entrada en vigor de la Disposición Final Tercera de la Ley 11/2007, de 22 de junio, de Acceso de los Ciudadanos a los Servicios Públicos, el 31 de diciembre de 2009, reconoció el derecho (y prácticamente el deber) de los ciudadanos a relacionarse electrónicamente con la Administración General del Estado. El enorme caudal de información personal aumentó los riesgos, pues es más problemático cada día mantener la seguridad de los sistemas y la calidad de los datos.

Existe, además, otro reto para la seguridad de los datos: regular *internet*, como fuente de información, es casi imposible; una solución global está lejos de alcanzarse. No existen normas internacionales con un marco jurídico uniforme para la gestión de las redes de comunicación. La disparidad entre la normativa europea (Tratado de Lisboa, Directiva 95/46/CE, actual RGPD) y la regulación de EEUU en materia de protección de datos así lo manifiesta. Frente a la reglamentación europea, en EEUU se ha optado por criterios auto-reguladores y de buenas prácticas, por códigos de conducta consi-

²⁰² Véase MURILLO DE LA CUEVA, obra citada: El derecho a la protección de datos personales genera “un sustrato material: su idoneidad para satisfacer una necesidad básica en las condiciones en las que convivimos en las sociedades posindustriales tras la transformación que han introducido en ellas las tecnologías de la información y las comunicaciones (...) consistente en evitar los perjuicios que puede deparar a los afectados el uso incontrolado por terceros de la información personal que les concierne para lo que es necesario que mantengan el poder de disposición sobre ella”.

derados por la doctrina como poco rigurosos, poniendo atención en las prácticas de las grandes empresas multinacionales.²⁰³

Se menciona la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad que se celebró en Madrid en el año 2009 como antecedente de la actual realidad.²⁰⁴ RALLO LOMBARTE, como Director de la AEPD, presentó el texto de la *“Propuesta conjunta para la redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de Carácter Personal”*. Es muy curioso que el Director de la Agencia hablara de privacidad, en la presentación del texto, utilizando el neologismo transmitido por el idioma inglés, y no utilice el término derecho fundamental ya consolidado por la más alta normativa europea y, por ende, la española. Quizá tuvo como motivación llegar a una universalidad del derecho, que sin esa contribución norteamericana parece tan improbable. En la Memoria de la AEPD del año 2009²⁰⁵ se reflejó en su punto 4 este evento de la Agencia Española, con el epígrafe *“2009, Madrid, capital mundial de la privacidad. La Resolución de Madrid: un punto de encuentro para una regulación Global.”*. Un ambicioso plan, sin duda: “avanzar hacia un instrumento legal, universal y vinculante en materia de pri-

²⁰³ Se apunta la interesante demanda de Microsoft al Gobierno de los EEUU reproducida por la prensa en abril de 2016: “Microsoft demanda a Estados Unidos por las búsquedas secretas de datos de clientes La compañía ha recibido 5.624 peticiones de información en los últimos 18 meses y en casi la mitad de los casos no ha podido informar a sus clientes” Este asunto de las prácticas empresariales de grandes corporaciones a nivel internacional se apunta en otro epígrafe, bajo el ámbito de aplicación de la LOPD.

http://internacional.elpais.com/internacional/2016/04/14/actualidad/1460655633_558327.html abril 2016

²⁰⁴ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, “Estándares internacionales sobre protección de datos personales y privacidad. Resolución de Madrid.”]. http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf a 30 de agosto de 2015.

²⁰⁵ Curiosamente también con el título siguiente: “El derecho fundamental a la Protección de datos de Carácter Personal: situación actual y perspectivas de futuro”. Aquí se habla de derecho fundamental a la protección de datos y no de “protección de la privacidad”. Esta confusión de términos no es ventajosa para la aclaración de conceptos.

vacidad, que contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado y que cuente con el más amplio consenso institucional y social”²⁰⁶. Por lo demás, la Propuesta compuesta de VI partes, incluyó lo que ya recogían los textos internacionales y españoles, en cuanto a principios y derechos.

2.2. El objeto del nuevo Reglamento Europeo 2016/679 de protección de datos personales (RGPD).

El artículo 1 RGPD establece como objeto de la norma europea la protección de los derechos y libertades fundamentales de las personas físicas respecto a sus datos personales junto con la libre circulación de estos datos en la UE, en lo cual pone especial énfasis, al mencionar en su punto 3 que la libre circulación no podrá ser restringida ni prohibida en la UE por motivos relacionados con la protección de las personas físicas. Un solo marco normativo para toda la UE, que pretende estar exento de múltiples interpretaciones. No se mencionan los derechos fundamentales a la intimidad y al honor (como sí se realizó en la LOPD), con cierto carácter prevalente hasta este momento frente al resto de los derechos fundamentales, sino que se alude a los derechos y libertades fundamentales en general, expresando el reconocimiento de lo que estaba ocurriendo en la práctica, *la total vinculación de los datos personales con todos los DDFF, que se veían afectados por la desprotección del derecho a la protección de datos personales*. La UE no hizo otra cosa que hacerse cargo de sus obligaciones para generar la confianza que permitiera a la economía actual, denominada *economía digital*, desarrollarse en toda la UE. El RGPD no tiene un objeto diferente a las normas anteriores, más bien pretende que se consigan los objetivos de uniformidad en la normativa europea y de efectividad de la protección de datos personales. En este plazo que se está desarrollando actualmente, de convivencia de las dos normas (LOPD

²⁰⁶ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Memoria 2009"]. Página 37 http://www.agpd.es/portaIwebAGPD/LaAgencia/informacion_institucional/common/memorias/2009/AEPD_memoria_2009.pdf a 30 de agosto de 2015

española y RGPD europeo) se presentan serios interrogantes al respecto, que la AEPD o la Comisión Europea no han respondido aún (marzo de 2017).

3. Ámbito de aplicación.

El derecho a la protección de datos en su ámbito de aplicación ha sido, a lo largo de los años transcurridos, lo más difícilmente asumible por los responsables de tratamiento e incluso por los mismos titulares de datos. La norma española (LOPD) concebida bajo una visión territorial de las leyes, se enfrentaba en pocos años a un mundo sin fronteras territoriales físicamente definidas. Se hace necesario, en cualquier caso, citar y analizar esta regulación vigente, en convivencia actual con el nuevo RGPD. El ámbito de aplicación de la LOPD tuvo su regulación en el artículo 2 y también en los artículos destinados a la regulación de las transferencias internacionales de datos personales, artículos contenidos en el Título V de la LOPD. Se abordan estas cuestiones desde la visión de 2017, 18 años después de la promulgación de la LOPD y 10 años después de la promulgación del Reglamento, con la entrada en vigor del nuevo RGPD, el cual será de obligada aplicación en mayo de 2018.

El artículo 2.1 de la LOPD tuvo una orientación desde el derecho internacional privado. junto con el artículo 4.1 de la Directiva 95/46/CE²⁰⁷. Estableciendo una comparativa entre el texto de ambos artículos, hasta la LOPD no existía en España una norma que determinase expresamente el ámbito de aplicación de la normativa de protección de datos. El Convenio del Consejo de Europa de 1981 no lo contemplaba. Hasta 1999, para dar solución a los casos sobre protección de datos personales, se aplicaba la ley personal del titular cuyos datos eran objeto de tratamiento, la aplicación directa de la ley del foro a los tratamientos vinculados al territorio del Estado y para casos de

²⁰⁷ SANCHO VILLA, D., "Artículo 2.1 Ámbito de aplicación territorial.", *Comentario a la Ley de protección de datos de carácter personal*, Madrid, 2010, pág. 99-115. Fue premio de la AEPD por su estudio "Transferencia internacional de datos" editado en el año 2003.

responsabilidad por daños, se aplicaba la ley del lugar del hecho dañoso, aplicación que se mantiene para los casos de responsabilidad extracontractual.

3.1. La regulación establecida en la LOPD de 1999 y su Reglamento de 2007
Los casos recogidos en el artículo 2.1 se formularon en tres puntos, a), b) y c), que se tratan separadamente. Cuando el establecimiento del responsable del tratamiento se localizaba en España, las condiciones generales de aplicación del artículo 2.1.a) se podía analizar desde el punto vista territorial, subjetivo y objetivo.

3.1.1 El concepto de territorialidad.

Bajo un concepto de territorialidad, el artículo 2.1.a) LOPD determinó como regla general que es aplicable la Ley española *cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento*. La LOPD no reflejó exactamente el contenido de la Directiva 95/46/CE en su artículo 4.1.a) por cuyo texto se aplicaba la ley del Estado miembro *cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro*. Esta opción del legislador europeo matizó la estricta territorialidad del tratamiento. La posible dificultad en la interpretación conjunta de ambos textos fue la utilización de una solución para atribuir mayor peso al lugar de localización del tratamiento de los datos personales que al *lugar de establecimiento del responsable* de dicho tratamiento. La interpretación del artículo 2.1.a), sin embargo, ha sido a favor del sentido de la Directiva 95/46/CE, aplicándose en el régimen español el criterio del *establecimiento del responsable del tratamiento en España*, no solamente como lugar de tratamiento de dichos datos. Un ejemplo de informes de la AEPD viene a aclarar completamente la diferencia: la inclusión de datos de clientes españoles en una base de datos alojada en la sede central de una empresa en Francia. En este caso, la AEPD consideró que el tratamiento de los datos se somete a la ley francesa de protección de datos persona-

les²⁰⁸. El Reglamento de desarrollo de la LOPD de 2007²⁰⁹ aportó más sencillez al complejo concepto, pues el artículo 3.1.a) del Reglamento concreta el concepto de aplicación de la Ley española a todo tratamiento *efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español*. El legislador de 2007 se inclinó a favor de la Directiva 95/46/CE.

3.1.2 El concepto de aplicación subjetiva.

La aplicación de la LOPD se produjo sobre responsables de fichero o tratamiento que realizaban su actividad en España, por tanto, se articulaba la aplicación de la Ley española de protección de datos sobre el tratamiento que desarrollaba el encargado del tratamiento *al amparo de la ley del establecimiento del responsable*. Así se dedujo del texto de la Directiva 95/46/CE, en cuya exposición de motivos, Considerando 18, se formula: “resulta conveniente someter el tratamiento de datos efectuado por cualquier persona que actúe bajo la autoridad del responsable del tratamiento establecido en un Estado miembro a la aplicación de la legislación de tal Estado”. Por tanto, y continuando con el mismo ejemplo del informe jurídico mencionado, las actividades de tratamiento que se realicen en una empresa sita en España como encargada del tratamiento de un responsable francés, están sometidas a la ley francesa, para determinar las obligaciones del tratamiento de este encargado, los derechos de los afectados, y demás derechos establecidos para protegerlos.

Estas cuestiones sobre determinación de responsabilidades entre responsable de tratamiento y encargados de tratamiento fueron una constante de indeterminación. Aquí basta precisar lo que se consideraba la aplicación de la Ley española al encargado de tratamiento establecido en España de las normas de seguridad que se establecen en el Reglamento de 2007, en su capítulo VIII. El régimen imperativo de seguridad técni-

²⁰⁸ Informe jurídico 568/2008, AEPD. Ejemplo de la autora citada.

²⁰⁹ El cual es considerado por la doctrina como una pieza esencial para aclarar e interpretar la LOPD y la Directiva,

ca amplió su ámbito de aplicación al encargado del tratamiento establecido en España, en una lectura conjunta del artículo 2.1.a) y el artículo 9 LOPD, pues este último precisó que las medidas técnicas y organizativas deben ser aplicadas por el responsable y en su caso, encargado de tratamiento, por lo cual, siguiendo con el ejemplo propuesto, el encargado de tratamiento en España de un responsable de tratamiento francés deberá adoptar todas las medidas de seguridad previstas en el capítulo VIII del Reglamento de la LOPD²¹⁰.

3.1.3 El concepto de aplicación objetiva.

Bajo el concepto de aplicación objetiva, se estableció la regla general del artículo 2.1.a) LOPD, la cual determinó la aplicación de la ley española a las actividades de tratamiento del responsable en su establecimiento en España. Teniendo en cuenta el Considerando 19 de la Directiva 95/46/CE, en cuyo enunciado²¹¹ no considera relevante la forma jurídica de ese establecimiento, el Reglamento recogió ese concepto²¹², que fue práctica en España hasta la promulgación del mismo. Por tanto, lo más importante no son las posibles formas jurídicas del establecimiento o la concurrencia o no de personalidad jurídica, sino la circunstancia de la realización efectiva de operaciones de tratamiento en el mismo establecimiento del responsable del fichero. Por ejemplo, podrán ser establecimientos en el sentido del artículo 2.1.a) LOPD las sucursales, las filiales, las agencias, etc. Desde esta perspectiva objetiva, el artículo 2.1.a) LOPD se completó con el artículo 3.1 a) del Reglamento, estableciéndose la interpretación de que *lo determinante para que se aplique la ley española son las actividades*

²¹⁰ Véase SANCHO VILLA para este y otros ejemplos.

²¹¹ Considerando 19 Directiva 95/46/CE: “El establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa con personalidad jurídica, no es un factor determinante al respecto”.

²¹² El texto del artículo 3.2. del Reglamento es el siguiente: “a los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad”

*del responsable del tratamiento en un establecimiento dentro del territorio español.*²¹³

En cualquier caso, todo este asunto de aplicación de la ley se tuvo que contemplar en un entorno real y preciso para cada caso concreto, valorando las circunstancias, pues para dejar más espacio a la interpretación, el artículo 2.1.c) junto con el artículo 4.1.c) de la Directiva 95/46/CE, dejó al interprete la posibilidad de considerar que un tratamiento en España es un *medio en el foro*, al contemplarse como establecimiento del responsable en un tercer estado.

3.2. Las cuestiones que plateaba la regla general sobre el ámbito de aplicación de la LOPD.

La regla general fue que se aplicaba la ley del responsable del tratamiento de los datos, no la ley del afectado, el titular de los datos personales, lo cual generó muchas controversias en la práctica, al margen del ejercicio de los llamados derechos del titular de datos personales²¹⁴. La tecnología fue otra vez mucho más rápida que las posibilidades de regulación de sus consecuencias, por lo cual, con el avance hacia situaciones de tratamiento tan sofisticadas como los llamados sistemas *big data* (se recuerda, tratamiento de datos masivos o grandes cantidades de datos) en el llamado *clouding* o *nube* (tratamiento y almacenamiento en la nube o en servidores con acceso

²¹³ Continuando con los ejemplos ilustrativos de práctica de aplicación de estas normas, “un empresario con un establecimiento en Suecia y otro en España no podría en principio pretender la aplicación de la legislación de protección de datos sueca a los tratamientos que ha realizado en su establecimiento en España, por el hecho de disponer de un establecimiento de Suecia”. Ejemplo de la autora citada.

²¹⁴ Por lo que SANCHO VILLA considera que “la relación de tratamiento no se plantea en términos de equilibrio; mientras que el afectado es una persona física que consiente un tratamiento en el contexto del derecho privado (o asume el impuesto por la ley en el contexto del derecho público), cabe presumir que el responsable es un agente sofisticado que asocia determinados beneficios al tratamiento de datos personales de terceros, derivados de la explotación comercial de la información, de la mejora de sus sistemas de información o del suministro de bienes y servicios (o bien vincula al tratamiento determinadas finalidades públicas en el caso de responsables de derecho público)” En este momento, toda la doctrina confirma las diversas insuficiencias y controversias.

múltiple por *internet*) es una tarea casi imposible determinar cuál es el domicilio físico de un responsable o (peor) un encargado de tratamiento, pues diferentes usuarios en diferentes países pueden tratar datos personales en la *nube* desde puntos diferentes del planeta en muchos casos, en diferentes servidores, soportes a su vez de los datos personales, situados en territorios completamente distantes, tanto a nivel material de kilómetros como a nivel jurídico. La situación de asimetría y armonización de los niveles de protección, entre muchas posibilidades de localización posibles, produce que la regulación del legislador de 1999 sea en este momento cuestionada²¹⁵. Se atendió a muchas interpretaciones y a muchas preguntas de las que cabe destacar ¿Dónde quedan los derechos del afectado? ¿Cómo se ejercen sustancialmente, ya no sólo nominalmente? ¿El consentimiento otorgado debe contemplar la posibilidad de que se pierda la pista de dónde y quién realmente está almacenando información personal, con qué finalidad, y cruzando dicha información con otras bases de datos? ¿Estos datos que teóricamente son para usos estadísticos o comerciales, por ejemplo, pueden ser almacenados para otras posibles finalidades? Estas preguntas se reflejan sólo en cuanto a la vinculación entre responsables y/o encargados de tratamiento de datos²¹⁶.

²¹⁵ En el 2009 SANCHO VILLA continuaba con su análisis con las siguientes palabras: “el legislador ha optado con alcance general por la ley del establecimiento del agente que trata los datos, asociando así los derechos de protección de la persona a la ley del país donde se desarrolla la esfera de actividad del responsable. Esta construcción encuentra su fundamento en un criterio de proximidad objetiva entre el establecimiento del tratamiento y el país donde éste se produce, lo que se vincula con la lógica del mercado y se construye sobre la ley de origen (ley de establecimiento del responsable)” (...) “la ventaja para el profesional de la solución elegida es que le permite centralizar sus operaciones de tratamiento al amparo de una única ley, la del país del establecimiento donde ocurren, sin tener que atender a una pluralidad de leyes estatales en función de la residencia del afectado”.

²¹⁶ Véase TORRES, J., *Empresas en la nube*, Barcelona, 2011, pág. parte IV. Un libro fácil de entender para su momento, pero que no entra en el derecho a la protección de datos, salvo para afirmar que “es necesario también que el propio mundo tecnológico del *cloud computing* mejore mecanismos que la favorezcan, como el perfeccionamiento de políticas de encriptación o nuevas prácticas estandarizadas, garantizando altos niveles de disponibilidad, accesibilidad o escalabilidad, pero sobre todo también, integridad, confidencialidad y trazabilidad de los datos” No tan entusiasta y mucho más rigurosa, la

La regla general llevaba también a otra contemplación de la misma en la visión de la relación entre varios responsables y/o varios encargados de tratamiento. La comunicación se hace en muchas ocasiones necesaria para operaciones comerciales o para la ejecución de contratos. Según el artículo 2.1.a) LOPD, como norma general, sería aplicable de manera distributiva la ley del establecimiento de cada responsable en el contexto del Espacio Económico Europeo (en adelante, EEE) Esta misma interpretación se desprende del texto del artículo 4.1.a) de la Directiva 95/46/CE²¹⁷. Se concluyó que la ley aplicable sería la de cada uno de esos lugares a los tratamientos efectuados en ese territorio. El límite a la regla general se encontraba en las condiciones de aplicación subjetiva, cuando el tratamiento se realizaba por varios encargados del tratamiento junto con el responsable; en ese caso, no rige la norma de aplicación distributiva de la ley del establecimiento de los encargados del tratamiento, sino la ley del responsable.

El artículo 2.1.c) contemplaba el hecho de que el responsable del tratamiento se encuentre en un país fuera del EEE, por lo que el afectado no podía ejercer sus derechos en ese ámbito. El artículo era una transposición del 4.1.c) de la Directiva 95/46/CE. El texto de la ley española es el siguiente: *“Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.”* Se consideraba que la LOPD generaba una norma especial, la cual mejoró la aplicación de la ley del establecimiento del responsable (que era la regla general) en beneficio de una norma que se centra en los recursos empresariales situados en territorio español. La regla especial no regía cuando un responsable del tratamiento que utiliza medios en España tiene su establecimiento en un Estado miembro del EEE. Estos supuestos se regían por la norma general (ley del estable-

autora GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015. Con eviten acierto jurídico, presenta el fenómeno del *cloud* en relación a múltiples riesgos. Es una referencia apreciable, a la que se recurrirá en más ocasiones, por su actualidad.

²¹⁷ Como ejemplo cita SANCHO VILLA la posibilidad de que los datos sean tratados por un responsable en su establecimiento en España, en una filial de Francia y en una sucursal de Alemania.

cimiento del responsable en EEE), pues los Estados del EEE no se consideraban a estos efectos terceros estados. En estos casos presentados por el artículo 2.1.c) se aplican el artículo 5.1. (párrafo segundo) LOPD²¹⁸ y el artículo 3.c) del Reglamento²¹⁹. Ambos obligaban a tener un representante en España del responsable del tratamiento. Este mandato favorecía el ejercicio de los derechos del titular de los datos y fundamenta la competencia internacional de los Tribunales Españoles.

El artículo 2.1.b) LOPD contemplaba el supuesto de la aplicación de la ley española cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho internacional público. Es el *supuesto de Derecho internacional*. Se considera que este artículo manifestó una situación de extraterritorialidad de los ficheros o tratamientos mantenidos por una misión diplomática, bajo el principio *auctor regit actum*²²⁰. Sería el caso de los Registros civiles de misiones consulares (por ejemplo, para inscripciones matrimoniales).

Por tanto, existía un vacío normativo que no se podía dejar sin reflexión: ni el legislador europeo, ni el español tuvieron en cuenta la regulación del supuesto en el que se pudiera determinar el régimen aplicable al tratamiento de los datos de un afectado que reside en Europa realizado por un responsable en un tercer Estado que no utilizaba medios permanentes en la UE²²¹. En la Sentencia de 13 de mayo de 2014 para el asunto C-131/12 (conocido como *caso Google*) el TJUE respondió a la pregunta de la

²¹⁸ El texto del artículo 5.1. (párrafo segundo) LOPD dice: “Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.”

²¹⁹ Y el texto del artículo 3.c) del Reglamento: “Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito. En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

²²⁰ Sáncho Villa, obra citada.

²²¹ Página 114, obra citada.

AN para determinar el ámbito de aplicación material y territorial de la Directiva 95/46/CE y de la LOPD. El TJUE argumentó con el texto del Considerando 19 de la Directiva 95/46/CE, y conformó la doctrina discutida de que la empresa *Google Spain* tenía una actividad económica en España en una instalación permanente, filial de *Google Inc.*, con tratamiento de datos personales. El TJUE concluyó que *“las actividades del gestor del motor de búsqueda y a las de su establecimiento situado en el Estado miembro de que se trate están indisociablemente ligadas, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión (web de Google) sea económicamente rentable y dado que el motor es, al mismo tiempo, el medio que permite realizar las mencionadas actividades”* (Cuestiones prejudiciales nº 56). El impacto de esta Sentencia y el denominado derecho al olvido (derecho de supresión en el RGPD) se analizará en otros epígrafes. En este momento sólo se quiere plasmar la interpretación del TJUE respecto al ámbito de aplicación de la normativa sobre protección de datos. Parte de la doctrina contrastó la Sentencia *Google* con una comparativa entre la protección de datos y la protección de marcas (que había sido analizada en el asunto C:2011:474 L'Oréal S.A entre otros vs. eBay International AG, Sentencia de 12 de julio de 2011; en este caso el TJUE pretendía también una interpretación extensiva de la norma para proteger eficazmente las libertades y los DDFF²²². Otra parte de la doctrina se mostró seriamente en contra del ámbito de aplicación de la normativa sobre protección de datos a una empresa internacional como *Google*, alegando que es simplemente un motor de búsqueda de información²²³. El TJUE se centró en la actividad económica de publicidad

²²² Véase GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 163.

²²³ Véase BOIX PALOP, A., "La construcción de los límites a la libertad de expresión en las redes sociales.", *Revista de Estudios Políticos.*, nº 173, 2016, pág. 99. En esa línea, COTINO HUESO, L., "El conflicto entre las libertades de expresión e información en internet y el derecho a la protección de datos. El derecho al olvido y sus retos: "un falso derecho, a juzgar por un falso tribunal", *Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia*, Madrid, 2014. Y anteriormente en COTINO HUESO, L., *Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías.*, Valencia, 2010, pág. 386 y ss.

dirigida a los usuarios o *banners* de la empresa para considerar que su actividad se realizaba en territorio español, aunque las instalaciones técnicas y los recursos humanos no estuvieran en ese territorio o en territorio del EEE.

3.3. Ámbito de aplicación del nuevo RGPD.

El artículo 3 RGPD regula la aplicación de la norma europea al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. Esta diferencia es importante. Lo que prioriza la nueva normativa son las actividades de un establecimiento, no dónde se realice el tratamiento de los datos, que pudiera ser en otro lugar diferente, dentro o fuera de la UE. Es decir, la localización física de los equipos informáticos (generalmente grandes servidores) o de los trabajadores que realicen el tratamiento no es determinante, sólo es vinculante para la aplicación del RGPD que las actividades de un establecimiento del responsable del tratamiento o de su encargado se realicen en la UE. En el punto 2 del artículo 3 RGPD se especifica aún más el ámbito de aplicación a interesados (titulares de datos) que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

Las dos situaciones tienen una fuerte relevancia comercial y política. La gestión de *big data* (recordemos, gestión masiva de datos) se basa en técnicas de análisis y comportamientos en *internet* e influye especialmente en la gestión de venta de productos y servicios, lo cual se fomenta, como se ha comentado, desde la norma europea, que se formula desde la mayor libertad posible para el tráfico de bienes y servicios. Se deja incluso la posibilidad abierta de que no sólo se aplique el derecho fundamental a la protección de datos personales a titulares ciudadanos/residentes de la UE y a em-

presas que tenga su actividad en la UE sino también a otras, que tengan relación con la oferta de bienes o servicios y con el control del comportamiento. Por último, el artículo 3.3 RGPD abre la aplicación del derecho fundamental a la protección de datos a la situación en el que el responsable del tratamiento de datos personales no está establecido en la UE, sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

La nueva norma europea regularía dos tipos de problemáticas analizadas por la doctrina. Por una parte, que los servicios a través de internet utilizados por los ciudadanos europeos con diversas finalidades y cuyo tratamiento de datos generalmente se había sustraído a las obligaciones y garantías que la normativa de los Estados miembros ofrecía, queden garantizados por el derecho de la UE. Por otra parte, se hace especial referencia a las finalidades de tratamiento de datos para análisis masivos de conducta, pues se consideró una fuente extraordinaria de riesgos para los DDFF de los ciudadanos de la UE, en especial para los derechos a la libertad, la dignidad y la no discriminación por diversas motivaciones²²⁴. El riesgo consiste en este caso en lo que se denomina *masificación de los instrumentos jurídicos*, como enormes cantidades de leyes y de sentencias, todas normas ineficaces, al no cumplir su objetivo. Este movimiento centrífugo de la normativa sobre protección de datos personales que Europa parece ampliar constantemente a otros ámbitos del Derecho, aparece como criticable por la doctrina²²⁵.

4. La realidad sin regulación: las Transferencias Internacionales de Datos personales

²²⁴ En este sentido, las ideas de GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 234.

²²⁵ Véase la exposición crítica de BOIX PALOP, A., "De McDonald's a Google. La ley ante la tercera revolución productiva.", *Teoría y derecho: revista de pensamiento jurídico*, nº 1, 2007, pág. 124-147, pág. 129. También ÁLVAREZ RIGAUDIAS, C., "El poder del usuario digital", *Hacia un nuevo Derecho Europeo de protección de datos*, Valencia, 2015, pág. 293 y ss. La autora parecía decantarse por la flexible normativa sobre privacidad en los EEUU.

La transferencia internacional de datos desde la UE a un Estado fuera del territorio europeo necesitaba de la autorización expresa de la Autoridad Nacional encargada de la protección de datos (en nuestro caso español, AEPD), después de ser solicitado por el responsable exportador que tiene su ubicación en la UE (España, como es el caso) y además aportar suficientes garantías adecuadas. El artículo 33.1 LOPD reguló estas situaciones de manera deficiente para un desarrollo del comercio internacional a través de los sistemas informáticos y de telecomunicaciones. El llamado ámbito de aplicación no es en estos momentos un territorio, un punto geográfico, como hasta ahora la ley lo había designado. La denominada *nube*, como se ha comentado anteriormente, impide este concepto. No existe, en muchos casos, una ubicación fija. Los proveedores de servicios a través de *internet* fueron contrarios a establecerse sólo en países del EEE o en países que presentaran las mismas garantías que los del EEE. El titular tenía y tiene, aún en el presente, el problema de no poder materialmente determinar en cada momento la localización de sus datos, tanto en procesos como en almacenamientos. No sabía quién los trata, porque no tenía el *dónde*. Esto no solamente dificultaba la aplicación de la LOPD en cuanto a su ámbito legal-territorial; además, hacía prácticamente imposible las restricciones de flujos de datos transfronterizos. La pregunta fue obvia: *¿Qué Ley se aplica en la nube?*²²⁶

4.1. Las conexiones en *cloud computing* o en *nube* según la AEPD.

²²⁶ Es una de las preguntas que la prestigiosa UIT (ITU en español, en algunas publicaciones) realizó a través de la jurista internacionalmente reconocida Stephanie Liston, en ese momento consejera de Charles Russell LLP, en su Informe Anual 2013. El capítulo se titula *“La nube: Protección de Datos y Privacidad. ¿Quién es el propietario de la nube?”*. La UIT es el organismo especializado de Naciones Unidas para las Tecnologías de la Información y la Comunicación. Según su página web, elaboran técnicas que garantizan la interconexión continua de las redes y las tecnologías, además de que se esfuerzan por mejorar el acceso a las TIC (Tecnologías de la Información y la Comunicación) de las comunidades insuficientemente atendidas de todo el mundo. Esta primera página realiza una declaración más: *Por medio de nuestra labor, protegemos y apoyamos el derecho fundamental de todos a comunicar* ITU INTERNATIONAL TELECOMMUNICATION UNION (UIT EN ESPAÑOL), [itu.int"]. A 20 de agosto de 2015.

La AEPD tardó algunos años en publicar una serie de consejos o *Guía* para aclarar estas cuestiones, si bien es cierto que se trataba de unas declaraciones de meras intenciones, y no de auténticas normas efectivas. En concreto, se trató de la *Guía para clientes que contraten servicios de cloud computing* con fecha de 2013. La AEPD delimitó el concepto de *cloud computing*, los tipos, las modalidades de servicio, la portabilidad de la información, las garantías contractuales que la AEPD consideró necesarias, enunció algunos riesgos que pueden ser tenidos en cuenta, junto con algunos consejos y sugerencias. Entre los temas abordados en la *Guía del Cloud Computing*, resultaba de interés su aplicación en las AAPP. La AEPD generó una definición de lo que consideró *cloud computing*²²⁷ como una nueva forma de prestación de los servicios de tratamiento de la información, válida tanto para una empresa como para un particular y, también, para la Administración Pública. *Una solución cloud computing permite al usuario optimizar la asignación y el coste de los recursos asociados a sus necesidades de tratamiento de información. El usuario no tiene necesidad de realizar inversiones en infraestructuras, sino que utiliza la que pone a su disposición el prestador del servicio, garantizando que no se generan situaciones de falta o exceso de recursos, así como el sobrecoste asociado a dichas situaciones.* La AEPD no estaba siendo restrictiva en cuanto a la descripción de los servicios en nube. Estaba, más bien, describiendo su vertiente más práctica y motivadora para su contratación²²⁸. El

²²⁷ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Guía para clientes que contrates servicios de Cloud Computing"].

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf
a 20 de agosto de 2015.

²²⁸ La AEPD continuó describiendo: "En un entorno de *cloud computing* la gestión de la información está de forma virtual en manos del cliente que contrata los servicios de la nube, que la trata a través de Internet accediendo a soluciones de bases de datos, correo electrónico, nóminas o gestión de recursos humanos de acuerdo a sus necesidades. En función del modelo utilizado, los datos pueden no estar realmente en manos del contratista, toda vez que la propiedad, el mantenimiento y gestión del soporte físico de la información, los procesos y las comunicaciones pueden encontrarse en manos de terceros. El proveedor del servicio puede encontrarse en, prácticamente, cualquier lugar del mundo y su objeti-

denominado *cliente* por la terminología de la AEPD, que, en este caso, no hablaba de titulares de datos personales, no sabe dónde están sus datos, si es un particular. Así mismo reconocía la AEPD que si el cliente de los servicios de *cloud computing* es una empresa o profesional responsable del fichero, ese cliente puede también ignorar dónde están almacenados y disponibles por *internet* los datos que trata en la realidad y de los que es responsable, por mucho que contractualmente le confirmen que esos datos están en la UE²²⁹. Como se desprende del enunciado del presente epígrafe, no se controlan los datos materialmente pero sí se mantienen las regulaciones de una ley que no contemplaba realmente semejante supuesto en 1999. La AEPD insistía en la importancia de identificar a los proveedores de *cloud computing dentro* delEEE o en países que garanticen un nivel adecuado de protección de los datos, afirmando que se debía tener en cuenta la localización de todos los recursos pues, por la misma naturaleza del servicio de *cloud*, los datos pueden estar en cualquier momento en cualquier sitio, pero los derechos y obligaciones relativos a dichos datos han de garantizarse siempre. Para añadir más incertidumbre, la AEPD reconocía que los contratos por los que se rigen estos servicios son *de adhesión*, no permiten que el cliente tenga la capacidad para fijar las condiciones de contratación, adecuándolas a sus obligaciones respecto a la ley española. El contrato de adhesión son condiciones generales de contratación, con cláusulas contractuales cerradas, las cuales se rigen en su mayoría por normas de derechos extranjeros y con sometimiento a tribunales, en muchos casos, pintorescos. La AEPD concluyó que esta situación generaba un evidente desequilibrio, pero que eso no exime a las partes de las responsabilidades de la LOPD.

vo último será proporcionar los servicios citados optimizando sus propios recursos a través de, por ejemplo, prácticas de deslocalización, compartición de recursos y movilidad o realizando subcontrataciones adicionales.”

²²⁹ La AEPD lo confirmó: “Como consecuencia de lo anterior, el mismo contratista puede desconocer la localización precisa de sus datos y no disponer del control directo de acceso a los mismos, de su borrado y de su portabilidad, ya que la información no está físicamente en su poder, aunque, si esa información contiene datos de carácter personal, sí está bajo su responsabilidad desde el punto de vista de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)”.

4.2. Deberes del responsable de tratamiento de datos en nube.

El responsable del tratamiento debía tener en cuenta dos aspectos, según la AEPD. El primer aspecto era evaluar los tratamientos y el nivel de protección de datos. Respecto a este requisito, la AEPD mostró su conformidad con los servicios en *nube* al afirmar que *la transferencia de datos a servicios de computación no excluye en principio a ningún tipo de dato, siempre que hubiera un balance positivo entre los riesgos asumidos y las salvaguardas, en forma de medidas organizativas y técnicas, proporcionadas por el proveedor*. Se opina que la pretensión de la AEPD sería imposible en la mayoría de proveedores de servicios en nube. Conocer todos los intrincados medios técnicos del proveedor de servicios y que éste garantizara los sistemas de seguridad y de ubicación es sólo nominal, porque en la realidad sería muy difícil, salvo que se tenga una tercera entidad que controle al proveedor, lo cual, para la gran mayoría de responsables de tratamiento de datos, pequeñas y medianas empresas, podría convertirse en literalmente inalcanzable. En segundo lugar, verificar las condiciones en que se presta el servicio. Previamente a la contratación, el responsable del tratamiento verificaría este, con el fin de determinar si ofrecen un nivel adecuado de cumplimiento. La AEPD aportó ejemplos destacados, como una *lista de control* que incluía elementos relativos a la información proporcionada, ubicación del tratamiento, la existencia de sub-encargados del tratamiento, las políticas de seguridad de la empresa receptora de los datos, junto con los derechos que pudiera ejercer el usuario y obligaciones legales del prestador del servicio.

El primer punto pudiera ser posible; debe ser el responsable del tratamiento quien evalúe la información que se lleve a los servicios externos en *nube*. Este punto es el más determinante, pues la información que todos pueden saber (por ejemplo, información que debe constar en Registro Mercantil, que se considera accesible por cualquiera, es información pública) no es información que no pueda estar a la vista en cualquier ubicación. Diferente es la información íntima, o lo que la LOPD considera datos especialmente protegidos, como datos médicos, por ejemplo. En ese caso, el

control técnico de seguridad en el tratamiento de esa información se hace indispensable.

La ubicación, identidad de los usuarios que acceden a los sistemas de almacenamiento y tratamiento de datos, la seguridad aplicada, y el ejercicio de los derechos del titular de los datos deben ser aspectos totalmente verificables, tanto por el denominado *cliente* (la persona física, la empresa o entidad que contrata los servicios de *cloud*) como por el titular de los datos objeto de tratamiento. Se mantiene por esta tesis que en los casos de contratación de servicios en *cloud* sólo proveedores certificados por el Estado o la *Unión Europea* podrían ofrecer servicios en *nube* para datos especialmente protegidos. El responsable del tratamiento también debería tener la obligación de informar al titular de los datos del uso de los servicios en la *nube* en el tratamiento de sus datos, para que el titular tenga conocimiento del hecho en el momento del consentimiento y que el lugar físico donde ejercer los efectivos derechos del titular sea en su proximidad, no en otro país, sino bajo los Tribunales y Autoridad de control de protección de datos que por nacionalidad le sean pertinentes.

Otro asunto, la ubicación física del tratamiento de datos, es verificable si se conocen las técnicas de localización a través de *internet*, pero no en todos los servicios en *nube* está garantizado, al igual que no está garantizado que el proveedor no contrate con sub-encargados, las políticas de seguridad sean difusas y los derechos de usuario sean más nominales que reales porque la comunicación con el operador por *internet* sea defectuosa. Desde posibilidades de acceso a los datos que no funcionan a situaciones en las que la empresa no existe dentro del EEE, y todos sus datos son falsos. Las dificultades de verificación son más que evidentes para un particular titular de datos personales y/o para una pequeña empresa cliente de servicios gratuitos en la *nube*. En la mayoría de ocasiones, un usuario con una formación limitada a su oficio no va a poder diferenciar entre una aplicación en *nube* y una aplicación en su equipo local, no sabe realmente que trabaja con programas *online*²³⁰.

²³⁰ Un ejemplo son las asesorías o gestorías online, que ofrecerían a sus usuarios una serie de aplicaciones para que ellos mismos introduzcan los datos de sus operaciones mercantiles (clientes y proveedo-

La AEPD no sólo permitió desarrollarse a las empresas en esas situaciones, sino que las ignoraba, permaneciendo al margen. Incluso se tenía la sensación de que el legislador renunciaba a regularlas.

4.3. El movimiento internacional de Datos de Carácter Personal.

Esta cuestión se reguló en el Título V de la LOPD. Como se comentaba en la visión temporal de esta exposición, la sensibilidad hacia la protección de datos personales comenzó por el tratamiento de datos personales en las Administraciones Públicas (AAPP). En el caso de las transferencias internacionales de datos (a partir de ahora TID), fueron los países que tenían vínculos en común, comerciales, políticos o de otra índole, los que iniciaron las TID y pronto se adhirieron a esa práctica las grandes corporaciones. Fue con la llegada de *internet* y el abaratamiento de los sistemas automatizados de datos, cuando eclosionaron las transferencias continuas de datos personales a otros países. En un principio se fomentó su práctica, pues así se adquirieron

res) y los datos de sus empleados (información laboral) entre otras informaciones, las cuales, dependiendo de la actividad del cliente de la asesoría, serán de diferente nivel de seguridad. En los aludidos casos es prácticamente imposible que el usuario, sin formación informática adecuada, sepa diferenciar entre una situación u otra, entre una aplicación que está en un servidor online y una aplicación que se encuentre en un servidor local, en la oficina de su asesor de confianza. En la práctica empresarial la experiencia fue más lejos. Empresas de suministro de programas de gestión empresarial (contabilidad, Cuentas Anuales para el Registro Mercantil, nóminas, tributación, Seguridad Social, entre otras gestiones) se denominaban a sí mismas encargadas del tratamiento, cuando no deberían ser más que proveedores de software, teniendo acceso sin más a multitud de equipos repletos de datos de otros responsables de tratamiento, sin control ninguno ni responsabilidad, pero sobre todo accedían (y acceden) a los datos que estos equipos almacenan. No se diferencia entre tablas de almacenamiento de datos y programas de software. Estas empresas, proveedores de software muy extendidas, son valoradas por sus clientes, responsables del tratamiento de datos, sin que se tenga en cuenta, desde dónde accede su personal, la identificación del mismo, y, sobre todo, no se controla si esos datos son exportados a cualquier servidor, pues carecen estas PYMES de entidades verificadoras de tales actos. Un asesor sabe de contabilidad o de tributos, pero no conoce de tecnología informática.

mayores niveles de comunicación entre países y con ello se agilizaron las posibles relaciones. La regulación de la LOPD para estos aspectos fue sumamente complicada, tanto que las PYMES muchas veces preferían eludirla y no realizar TID a otros países o al menos no dando constancia de su práctica. En las grandes empresas, la realidad dista mucho de la regulación; aunque generalmente sí tenían ficheros autorizados por la AEPD para las TID. Sin embargo, no siempre los datos estaban donde se decía que estaban, o al menos, no solamente.

La AEPD definió la transferencia internacional de datos como *tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español* (art. 5.1.s) Reglamento de la LOPD)²³¹. Como la propia AEPD reflejó, esta definición se encontraba en el Reglamento y se ajustaba a la Directiva 95/46/CE. La LOPD reguló las TID en los artículos 33 y 34, sólo dos artículos, extensos, en el Título V. Se completó con el Reglamento, que dedicó un Título a la materia, el VI, con los artículos del 65 al 70, también sumamente amplios²³².

La TID es una *cesión específica* a la que la LOPD no dedicó una definición. Así se puede concluir por la definición del artículo 3.c) LOPD que tiene el siguiente texto: a) *Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*. Fue el Reglamento en su artículo 5.1.s) el texto que aportó la siguiente definición: s) *Transferencia internacional de*

²³¹ https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php a 12 de diciembre de 2015.

²³² El exportador de datos se define como “la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realiza una transferencia de datos de carácter personal a un país tercero” (art. 5.1.j) del Reglamento).

El importador de datos es la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos, en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargado del tratamiento o tercero” (art. 5.1.ñ) del Reglamento).

*datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español. Otra definición para orientar el concepto de TID se encontró en la Sentencia C-101/01 del TJCE, de 6 de noviembre de 2006, caso *Lindqvist*. La Sentencia excluyó la difusión de datos personales por *internet* en una página web del concepto de TID. Actualmente la AEPD incluyó en su web el apunte aclaratorio a este concepto, pues *hacer referencia en una página web a una persona e identificarla por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, sí constituye un tratamiento de datos de carácter personal*.²³³*

Se aplicaba la LOPD cuando el exportador de datos tuviera su domicilio en el territorio español, como se define en el artículo 5.1.j) del Reglamento. Se excluyó expresamente mencionar al responsable del fichero o tratamiento, para evitar confusiones que dieran lugar a situaciones de interpretación. Cualquier transferencia de datos personales que se realizara por una persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español a un país tercero es una TID. El exportador debía cumplir una serie de garantías antes de realizar la exportación y contar con la autorización de la AEPD. Estos dos puntos que se resumen fácilmente fueron en la práctica una gran cantidad de normas europeas que se pueden resumir en lo que la Comisión Europea, en función del artículo 26.4 de la Directiva 95/46/CE, concretó en lo que se denomina *cláusulas contractuales tipo* (a partir de ahora, CCT) que la propia Comisión aprueba en diversas Decisiones²³⁴. Se justificaba la falta de claridad en la complejidad que conlleva querer una libre circulación de personas y capitales y una seguridad de los datos personales, para su protección. Los derechos funda-

233

https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/cuestiones_notificacion_transferencia/index-ides-idphp.php

²³⁴ Se citan como ejemplos las Decisiones de la Comisión 2001/49; 2002/16; 2004/915. En ellas se autorizaron las CCT.

mentales se convirtieron en un límite para el objetivo de libre circulación económica dentro del EEE.

La AEPD no excluyó su competencia sobre este asunto y sometió la TID a la autorización previa, bajo la aclaración de que el artículo 34.k) LOPD regula una situación entre Estados y no se extiende respecto a los contratos entre las partes, cuando se refiere al *nivel adecuado de protección*²³⁵. Sin embargo, la propia AEPD aprobó el sistema de certificación denominado de *Puerto Seguro (Safe Harbor)* sobre la base del artículo 25 de la Directiva 95/46/CE en la Instrucción AEPD 1/2000, no falto de controversia en los años posteriores. Por otro lado, en las grandes corporaciones internacionales existió lo que se denominó reglas corporativas vinculantes, en inglés *binding corporate rules* (a partir de ahora, BCR)²³⁶. Tanto las CCT como las BCR tienen como

²³⁵ Esta cuestión de *nivel adecuado de protección* no puede ser imprecisa al azar, después de más de 20 años de vigencia en el caso de la Directiva. La doctrina española es y fue sumamente crítica en ese aspecto. Véase ÁLVAREZ RIGAUDIAS, CECILIA; "Las Transferencias Internacionales de datos personales y el nivel equiparable o adecuado de protección."]. <http://www.uria.com/documentos/publicaciones/1467/documento/art1.pdf?id=2064> Otra obra de la misma autora ÁLVAREZ RIGAUDIAS, CECILIA; "Comentario a los artículos 33 y 34 LOPD. Las Transferencias Internacionales de datos personales.", *Comentario a la Ley de Protección de Datos de Carácter Personal*, , 2010.

²³⁶ Véase lo que el Gobierno de EEUU incluye en su web sobre información de exportaciones y la cuestión de las TID. <http://www.export.gov/safeharbor/> The European Commission's Directive on Data Protection went into effect in October of 1998, and would prohibit the transfer of personal data to non-European Union countries that do not meet the European Union (EU) "adequacy" standard for privacy protection. While the United States and the EU share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the EU.

In order to bridge these differences in approach and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "Safe Harbor" framework and this website to provide the information an organization would need to evaluate – and then join – the U.S.-EU Safe Harbor program.

The U.S. Department of Commerce in consultation with the Federal Data Protection and Information Commissioner of Switzerland developed a separate "Safe Harbor" framework to bridge the differences between the two countries' approaches to privacy and provide a streamlined means for U.S. organiza-

objetivo algo no bien definido, las garantías adecuadas de protección de la privacidad, en inglés, *adequacy standard for privacy protection*.

4.3.1 La Sentencia de *puerto seguro* en EEUU del Tribunal de Justicia de la Unión Europea (TJUE) de 6 de octubre de 2015.

El TJUE invalidó la decisión de la Comisión del año 2000 a través de la Sentencia denominada como *Safe Harbor* o *puerto seguro*. La Sentencia del TJUE sobre el asunto C-362/14, de 6 de octubre de 2015, probablemente influida por el denominado caso *Snowden*, abrió un nuevo tiempo en la interpretación del derecho fundamental a la protección de datos personales, junto con un movimiento ciudadano más concienciado cada día sobre la incidencia que extiende el tratamiento de datos personales sobre los DDFF en general, los derechos y libertades del Título I, Capítulo II de la CE. La prensa, además, hizo una publicidad de este asunto muy impactante²³⁷. Se asumieron como ciertas algunas de las informaciones difundidas en los medios de comunicación, cuestiones que además EEUU no negó, alegando razones de seguridad nacional.

La Sentencia del TJUE²³⁸ se sintetizó en el siguiente texto²³⁹: “El Sr. Maximillian Schrems, ciudadano austriaco, era usuario de Facebook desde 2008. Como ocurre con los

tions to comply with Swiss data protection law. This website also provides the information an organization would need to evaluate – and then join – the U.S.-Swiss Safe Harbor program.

²³⁷ Tómese como ejemplo la publicación del diario Expansión de 26 de octubre de 2015, titulado “¿Y si el puerto no es tan seguro?” del que se aporta el link a título de ejemplo: <http://www.expansion.com/juridico/opinion/2015/10/26/562e855846163f52648b4604.html>

Otro ejemplo puede ser un interesante documental emitido en TVE2 en diciembre 2015 cuyo link se expone para su consideración en caso de interés. <http://www.rtve.es/alacarta/videos/documentos-tv/documentos-tv-disidentes-digitales/3407639/>

²³⁸ TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, “Sentencia 06 de octubre de 2015. Caso Puerto Seguro.”]. <http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES>

demás usuarios que residen en la UE, los datos proporcionados por el Sr. Schrems a Facebook se transfirieron total o parcialmente de la filial irlandesa de dicha red social a servidores situados en territorio de los EEUU, donde fueron objeto de tratamiento. El Sr. Schrems presentó una denuncia ante la Autoridad irlandesa de control, por considerar que, a la luz de las revelaciones realizadas en 2013 por el Sr. Edward Snowden en relación con las actividades de los servicios de información de Estados Unidos (en particular, la *National Security Agency* o NSA), la normativa y la práctica de Estados Unidos no garantizaban una protección suficiente de los datos transferidos a ese país frente a las actividades de vigilancia por las autoridades públicas. La Autoridad irlandesa desestimó esa reclamación debido a que, en su Decisión de 26 de julio de 2000 la Comisión había considerado que, en el marco del régimen denominado de *puerto seguro*, Estados Unidos garantizaba un nivel adecuado de protección de los datos personales transferidos. La *High Court de Irlanda* (Tribunal Supremo irlandés), que conoció del asunto, deseaba saber si esa decisión de la Comisión impedía a una Autoridad Nacional de control investigar una denuncia en la que se alega que un país tercero no garantiza un nivel de protección adecuado y, en su caso, suspender la transferencia de datos denunciada.

En su Sentencia, el TJUE estimó que la existencia de una Decisión de la Comisión que declara que un país tercero garantiza un nivel de protección adecuado de los datos personales transferidos no podía dejar sin efecto ni limitar las facultades de las que disponen las Autoridades nacionales de control en virtud de la Carta de los Derechos Fundamentales de la Unión Europea y de la Directiva 95/46/CE. El Tribunal de Justicia destacó en ese sentido el derecho a la protección de los datos personales garantizado por la Carta y la función que ésta atribuye a las Autoridades nacionales de control.

Desde el año 2000 estaba en vigor la Decisión de la Comisión. En ese año, no existía todavía Facebook, ni la gestión en la nube o *cloud computing*, ni las máquinas que

²³⁹ TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, "Comunicado de prensa Nº 117/15 06 de octubre de 2015 Sentencia en el asunto C-362/14"]. <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf>

hacen posible las nuevas técnicas (servidores informáticos que ahora ocupan un espacio físico cada vez más reducido y amplían sus capacidades de memoria y procesador, ya comentados). Las Autoridades nacionales de los distintos miembros de la Unión Europea habían realizado multitud de estudios y trabajos sobre el asunto. Se abogaba desde entonces por una regulación internacional sobre la TID, que pudiera otorgar la protección debida a los titulares de datos y también facilitara el flujo de datos a nivel internacional, necesario para un sistema de gestión cada vez más globalizado. Aun así, algunas voces ya se dejaban oír a nivel europeo ante el avance de los nuevos hechos²⁴⁰.

La Sentencia centró su atención en las competencias de las Autoridades de Control de los distintos Países Miembros de la Unión Europea, manifestando claramente que, *incluso ante una Decisión de la Comisión, las Autoridades nacionales de control, ante las que se haya presentado una solicitud, deben poder apreciar con toda independencia si la transferencia de los datos de una persona a un país tercero cumple las exigencias establecidas por la Directiva 95/46/CE*. El Tribunal se consideró la única Autoridad competente para declarar la invalidez de un acto de la Unión, como en el caso presente en la Sentencia, una Decisión de la Comisión.

El régimen o sistema de *puerto seguro* era un acuerdo de autorregulación, no era una ley aplicable. Las entidades -privadas- estadounidenses que lo desearan, se sumaron al acuerdo. Pero no obligó en ningún caso a las Autoridades Públicas de EEUU. Las Autoridades Públicas estadounidenses prevalecen sobre cualquier entidad privada y sus competencias están por encima del régimen de *puerto seguro*, por lo tanto, las entidades privadas de EEUU están obligadas a dejar de aplicar, sin limitación, las reglas de protección previstas por ese régimen cuando entren en conflicto con las exigencias estatales federales de seguridad nacional.

²⁴⁰ “El hecho de considerar durante 15 años a EE UU como un puerto seguro era defectuoso desde el principio y viciado en la práctica”, defendió el director de *European Digital Rights*, Joe McNamee.” Frase publicada en el diario El País a 6 de octubre de 2015.

http://internacional.elpais.com/internacional/2015/10/06/actualidad/1444157153_404914.html

El Tribunal expresó claramente lo que ya se tenía por cierto en los medios de comunicación y en los profesionales involucrados. El régimen estadounidense de *puerto seguro* posibilitaba injerencias por parte de las Autoridades públicas estadounidenses en los DDFF de las personas, y la Decisión de la Comisión no ponía de manifiesto que en EEUU existieran reglas destinadas a limitar esas posibles injerencias ni que prevaleciera una protección jurídica eficaz contra éstas. Con esa afirmación, el Tribunal reconoció que no existía una protección jurídica eficaz para los DDFF de los ciudadanos desde la perspectiva europea. Además, cabe resaltar que el Tribunal habló de DDFF en general, no lo limitó al derecho fundamental a la protección de datos personales, con la expresión indubitable *derechos fundamentales de las personas*. En su análisis, el Tribunal comprobó que a través de las TID a EEUU las Autoridades de este país accedían a los datos personales transferidos desde los Estados miembros de la Unión Europea, los trataban de manera incompatible con la normativa de la EU y *yendo más allá de lo que era estrictamente necesario y proporcionado para proteger la seguridad nacional*.

También el Tribunal señaló el hecho de que *las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitieran acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión*. Esto significó que los derechos de las personas recogidos en la LOPD y la protección a los DDFF no tenían un sistema eficaz para su ejercicio. No existía control de la información personal por el titular de los datos. Es más, la vida privada resultó seriamente lesionada por el ejercicio del poder por parte de las Autoridades Públicas de EEUU. Otro derecho también lesionado fue el de la tutela judicial efectiva, al negarse el posible ejercicio de acciones en Derecho; la negación de la tutela judicial efectiva, niega la existencia del Estado de Derecho, en palabras del Tribunal.

Una Resolución tan demoledora, debería haber terminado con una revisión urgente y total de toda la práctica y regulación de los DDFF, en especial a través de la visión actual de su ejercicio y de su protección ante su vulneración, constante, diaria e imposible de controlar, junto con una revisión de las relaciones económicas y políticas entre la UE y EEUU.

La AEPD emitió también un comunicado de prensa²⁴¹ y una declaración conjunta²⁴² en el mismo mes de octubre 2015. En esas notas de prensa se manifiesta la opinión de generar una *posición sólida, colectiva y común sobre la aplicación de la Sentencia* de todas las Autoridades de protección de datos de la Unión Europea. En ese momento, faltaba la Sentencia del Tribunal Supremo de Irlanda, el competente para realizar una valoración de los hechos denunciados por un nacional austriaco, el Sr. Schrems. El Grupo de Trabajo del Artículo 29 (GT29) ya había manifestado reiteradamente la cuestión de la vigilancia masiva e indiscriminada dentro de las prácticas de EEUU. Se añade en esta nota que se había también manifestado la problemática de que los poderes estatales accedan a información privada (*de particulares*) excediendo lo que puede ser necesario en una sociedad democrática. El texto reconocía la exigencia de amplio análisis de las leyes nacionales ante cualquier adecuación al mandato de la Sentencia. Se pretendía por el GT29 *encontrar soluciones políticas, jurídicas y técnicas que permitan transferencias de datos al territorio de EEUU respetando los derechos fundamentales* La propuesta de *soluciones deberían ir siempre acompañadas por mecanismos claros y vinculantes e incluir, al menos, obligaciones sobre la necesaria supervisión del acceso por parte de las autoridades públicas, sobre transparencia, proporcionalidad, mecanismos de reparación y derechos recogidos en la legislación de protección de datos.*

Se vuelve a resaltar que *se trataba de derechos fundamentales en general, no solamente se referían al derecho fundamental a la protección de datos personales.* La pregunta de esta tesis es si la legislación sobre protección de datos es suficiente para proteger y hacer efectivo el ejercicio de los Derechos y Libertades Fundamentales o se deben modificar y crear otros mecanismos legales más acordes con la nueva situación técnica, social y económica, que permita una conjunción de todos estos factores.

²⁴¹ Véase

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_06-ides-idphp.php

²⁴² Véase

http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_19-ides-idphp.php

Ahora mismo la regulación no sólo es ineficaz, es también obsoleta. El espacio o ámbito de aplicación está seriamente cuestionado, pues es un espacio *no físico*, es un espacio en las redes de comunicación, no tiene capacidad efectiva de control territorial. Por eso, las llamadas Autoridades de control de los países miembros tienen un escollo ya al inicio de su gestión: la idea de un ámbito de aplicación territorial (físico) frente al ámbito de aplicación imposible de territorializar (denominado virtual o *ciberespacio*, pues no hay terminología jurídica para este hecho), que es *internet* y los medios de comunicación de redes. Reconoció esta nota de prensa de la AEPD la ilegalidad de las TID a EEUU bajo la Decisión de *puerto seguro*, y por ello, se pondrían en marcha diferentes campañas informativas a todas las empresas que realicen TID. La nota de prensa terminó con un párrafo al menos calificable de pintoresco. Es el siguiente: En particular, y en el contexto de la Sentencia, *las empresas deberían reflexionar sobre los eventuales riesgos que asumen al transferir datos y considerar la oportuna puesta en práctica de todas las soluciones legales y técnicas para mitigar esos riesgos y respetar el acervo comunitario de protección de datos.*

¿Las empresas?

Es una competencia del Estado proteger a los ciudadanos de los posibles incumplimientos y violaciones de sus derechos y, además, el Estado debe garantizar el ejercicio de los derechos (su eficacia, artículo 9.2 CE). ¿Van a ser las empresas los entes en los que derive la protección de los Derechos y Libertades Fundamentales? Es más, la soberanía reside en el Pueblo (español), sólo a través de los mecanismos legales aprobados por sus representantes y a través de los Poderes del Estado se puede realizar *valoraciones*. Las Empresas son personas jurídicas, con una importancia vital en la economía y en la sociedad de los países, pero no tienen, en teoría, relevancia jurídica ni competencia como para generar decisiones sobre DDFF, *¿o sí tienen esa relevancia normativa?* Hasta ahora, las empresas han sido para el derecho fundamental a la protección de datos personales, únicamente, responsables de ficheros o tratamientos. En este punto se debe diferenciar entre grandes corporaciones y PYMES. De lógica, para las PYMES también representó la adecuación a las normas sobre protección de datos un coste muy importante. Para las grandes corporaciones no es más que un escollo,

por tanto, superable²⁴³. Pero este asunto es claramente cuestión de normativas, no de gestión empresarial²⁴⁴. Las empresas realizarán su actividad en función de la norma que se disponga por los Parlamentos, Gobiernos correspondientes y sus legislaciones. Facebook no realizó un hecho antijurídico, lo que realizó Facebook lo hizo porque se le permitía hacerlo, porque nadie lo limitó y los usuarios acceden a facilitarle todo lo que piden como empresa, con tal de seguir en la red de contactos.

Este tema se unió por simple deducción con el importantísimo Tratado de Asociación Transatlántica de Comercio e Inversión (TTIP)²⁴⁵. La protección de datos se quería

²⁴³ http://www.elconfidencial.com/tecnologia/2015-10-07/la-nueva-decision-europea-en-privacidad-afectara-a-miles-de-empresas-espanolas_1049523/ En palabras del abogado que sirve de referencia al diario El Confidencial, Samuel Parra: "Con la decisión del TJUE se crea un limbo legal en el que cualquier cliente en España de estas 'pymes' podría denunciarles por transferir sus datos a servidores en EEUU. Si la denuncia es ante la Agencia Española de Protección de Datos, las multas podrían llegar a los 600.000 euros. Para Facebook esto es calderilla, pero para una pyme, aunque la multa sea de 50.000 o 100.000 euros, es un golpe que la hunde." Como explica este experto al diario, la Sentencia no implica que Facebook o Amazon estén obligados a dejar de transferir inmediatamente datos personales a EEUU, pues serán las Agencias de cada país Miembro las encargadas de estudiar si estas transferencias son conformes a derecho o no, caso por caso. Para las grandes corporaciones supone añadir un párrafo o dos en los términos de uso o en las condiciones de contratación, que nadie va a leer, se aceptan y listo. Son las PYMES españolas que hayan contratado un alojamiento de hosting en EEUU o las que tengan comercio con empresas en ese país las que serán seriamente afectadas. Otro experto en derecho e Internet, Calos Sánchez-Almeida, en su opinión, las empresas españolas deberían consultar a la AEPD sobre la legalidad de su actividad con EEUU y esta Agencia "debería pronunciarse de oficio y no esperar a la denuncia de algún ciudadano", que es lo más conveniente y lógico.

²⁴⁴ http://www.elconfidencial.com/ultima-hora-en-vivo/2015-10-06/facebook-el-caso-schrems-tiene-que-ver-con-normativas-y-no-con-empresas_706898/

²⁴⁵ Véase la visión de la relación entre el derecho a la protección de datos en la UE y el TTIP en el estudio de DIX, A., "Datenschutz und transatlantische Freihandelszone ", *Karlsruher Dialog zum Informationsrecht / Zentrum für Angewandte Rechtswissenschaft (ZAR), Karlsruher Institut für Technologie (KIT)*, nº , 2016.

El diario El País manifestó este punto en artículos que se referencian. http://internacional.elpais.com/internacional/2015/10/06/actualidad/1444157153_404914.html
http://internacional.elpais.com/internacional/2015/10/06/actualidad/1444154032_422524.html

excluir del TTIP, al considerar la Comisión que se trataba de un derecho fundamental (por la Sentencia del TJUE, se trató de varios DDFF, en general, que de un solo derecho afectado) La transmisión de datos personales se hacía indispensable para el comercio electrónico, uno de los importantísimos temas del Tratado (reserva de un hotel, compras por *internet*, seguros de todo tipo, como de vehículos de mercancías, por ejemplo) pero la transmisión de datos de redes sociales, o lo que es más importante, el uso y tratamiento que se daban a todos esos billones de datos que se generaban al día, es lo que no estaba claro entre la Unión Europea y EEUU.

Con toda sinceridad y lógica, lo que no se puede negar es el avance de la sociedad actual en cuanto a transmisión de datos personales. Es cierto que las leyes de protección de datos pueden tener efectividad dentro de un ámbito territorial limitado, pero es imposible saber realmente dónde se almacenan esos datos una vez que están en algún servidor del mundo virtual de la comunicación y quién los trata. El titular no puede conocer estos aspectos. Su actuación se limita a reaccionar ante manifestaciones del tratamiento hacia el exterior de los sistemas informáticos, como puede ser un correo electrónico que no le es conocido, un envío de mercancía que no había solicitado, una información de publicidad de una empresa con la que nunca ha tratado. Al igual que los *banners* de publicidad de Facebook, miles de tratamientos se llevan a cabo en las redes de *internet*, en servidores desconocidos, para ofrecer productos y servicios a los usuarios, consumidores y titulares de datos personales, sin su conocimiento y, por tanto, sin su consentimiento explícito para esos tratamientos específicos. La cuestión, además, ya es un hecho generalizado, no se puede controlar. ¿Cómo se podría negar en este momento el uso de las redes sociales y del comercio electrónico, que, por ejemplo, China o Corea del Norte, intentaron limitar? ¿Puede alguien tan siquiera imaginar el impacto que tendría en la sociedad actual una prohibición de uso y acceso a la *nube* o a redes como *Instagram*, la profesional red *Linkedin*, o los comentarios de libre expresión en *Twitter*? La revolución se produciría de inmediato en las calles. ¿Qué pueden hacer los Gobiernos de la Unión y las Autoridades de Control? ¿No permitir el acceso a *internet*, por ejemplo? Lo de menor calificación sería de conducta autoritaria. Sin embargo, estamos ante una situación antijurídica material, que

afecta a los Derechos y Libertades Fundamentales. ¿Son obsoletos estos derechos y libertades fundamentales? ¿Declina o renuncia sus derechos el titular de los datos personales por el uso de la economía y sociedad global? ¿Deben las empresas, en especial, las PYMES, resultar exentas de cualquier responsabilidad en cuanto a reclamaciones de titulares de datos personales, cuando ese mismo titular exhibe su conducta en *internet*, y otorga sus datos más valiosos sin ningún límite? ¿Deben incluso ser liberadas las empresas de mantener la rigurosa seguridad de datos personales que obliga la LOPD bajo la perspectiva de que los propios titulares de datos no atienden a su protección según la propia ley y normativa Europea?

4.3.2 La desprotección jurídica del ciudadano ante las TID

No son necesarias muchas habilidades técnicas para un tratamiento ilícito de datos personales fuera del ámbito de aplicación de la LOPD. Sin el consentimiento del afectado, simplemente, ya se viola su derecho fundamental a la protección de datos personales y, por ende, se violan otros derechos constitucionalmente protegidos²⁴⁶. El mundo estaría dividido en tres sectores reguladores de la protección de datos perso-

²⁴⁶ ORTEGA GIMÉNEZ, A., *La (des) protección del titular del derecho a la protección de datos derivada de una transferencia ilícita.*, Madrid, 2014. En una edición más reciente, pero con una temática similar, ORTEGA GIMÉNEZ, A., *Transferencias internacionales de Datos de Carácter personal Ilícitas*, Pamplona, 2016. El autor presenta en la primera obra mencionada una tesis doctoral, cuyo objeto de estudio es el hecho de la transferencia internacional de datos personales. Es editada por la propia AEPD y tiene un prólogo de su Director en ese momento, D. José Luis Rodríguez Álvarez. En esa obra el autor pretende demostrar, que el titular de datos personales se encuentra en una situación de (completa, se añade) desprotección jurídica ante una transferencia internacional de datos ilícita. Tomando como punto de referencia la existente doctrina sobre este asunto, asume el autor ese estudio desde la perspectiva del derecho internacional privado. Aun formando parte de una disciplina de derecho privado, el autor se inicia expresando que “sin demasiadas dificultades técnicas, la información puede ser objeto de un tratamiento ilícito; esto es, de una transferencia internacional de datos personales sin consentimiento del interesado, concluyendo en una violación de sus derechos fundamentales (perspectiva de esta tesis que se presenta), constitucionalmente protegidos”

nales. Un primer grupo lo conformarían los Estados donde existe legislación en materia de protección de datos, del que España y la UE forman parte, junto con otros países en mayor o menor concordancia. El segundo grupo lo conforman los Estados en los que se está trabajando a favor de una legislación en materia de protección de datos. Y en un tercer grupo se encuentran los Estados donde la legislación en materia de protección de datos personales no existe. La ausencia de protección determinaría lo que se denominan *paraísos de datos*, esto es, Estados donde pueden tratarse todo tipo de datos de carácter personal, sin ningún tipo de restricciones legales. Los datos, una vez tratados, se pueden transferir a otros países, con un nivel de protección adecuado y legalmente eludir, de esta forma, la aplicación de la legislación de protección de datos del país de origen de los titulares (*fraude de ley*), dificultando o imposibilitando que el titular del derecho a la protección de datos de carácter personal obtenga tutela judicial, en el caso de un litigio internacional por el tratamiento de sus datos de carácter personal²⁴⁷.

Por esas razones, toda la regulación existente en esta materia está disponible para su revisión. La totalidad de la normativa caería ante la realidad que vence a las Autoridades y Gobiernos respecto a la protección del titular del derecho fundamental a la protección de datos, y con ello a todos los derechos y libertades fundamentales en su ejercicio dentro de la sociedad actual. Sin datos personales, parece ser que no se tiene presencia en el mundo del siglo XXI, al igual que en el siglo XIX comenzaron los diferentes Registros de datos (Registro Civil; Registro de la Propiedad; Registro Mercantil) que tanto aportaron a la seguridad jurídica y en la que se basaron el reconocimiento de diversos derechos, desde la propiedad privada a los derechos del ciudadano, pero también jugaron un papel importantísimo en las aberraciones políticas del siglo XX. Estos cambios mal previstos, mal analizados y sin mucha motivación para su regulación adecuada parecen haber vencido a los juristas y expertos, generando no ya una normativa defectuosa, como bien reconoce la Sentencia del TSJE (caso de *puerto seguro*), sino un vacío total en la realidad, anterior a esa Sentencia y al nuevo RGPD, pues la norma carecía de eficacia y efectividad, por tanto, era sólo nominal, ante el

²⁴⁷ Pág. 14, obra citada.

mercado mundial y la sociedad global que actúan sin fronteras físicas territoriales. Las ventajas se han dejado sentir en las transacciones económicas y en las relaciones sociales, eso es indiscutible, pero los inconvenientes se traducen en una complejidad de intereses difíciles de conciliar, como son el legítimo interés a la protección de la intimidad personal, las aspiraciones comerciales de las empresas multinacionales en el tratamiento internacional de datos y la libertad de información y comunicación como DDFF, entre otros que abarcan diferentes ramas del Derecho, prácticamente a todo el sistema jurídico, en especial, al más puro derecho constitucional con su aliada permanente, la teoría-filosofía jurídica ²⁴⁸. Lo que no se atrevieron a mostrar los Gobiernos de la Unión Europea se ha dado en la realidad al verse claramente la situación (des)-regulada de todo un espectro de derechos y libertades fundamentales a través de la protección (o situación de des-protección) del derecho fundamental a la protección de datos personales²⁴⁹. Se abriría toda la cuestión a otra pregunta: ¿es el Estado del nacional dañado por una falta de regulación en este tema responsable de la situación? De facto, se ha hecho imposible la articulación de sus derechos en el mundo vir-

²⁴⁸ Obra citada, pág. 15. Las ramas del derecho que el autor consideró involucradas son el Derecho Internacional Público, por la celebración de acuerdos entre Autoridades de control; El Derecho internacional Privado, por las situaciones privadas derivadas del incumplimiento de un contrato internacional de tratamiento de datos personales o la violación de derechos del titular, que pueden requerir indemnización, asunto que como se ha visto, es meramente disciplina de Derecho Civil; y el Derecho Público Administrativo por la naturaleza de las sanciones al responsable del fichero o tratamiento.

²⁴⁹ Como el autor de esta obra citada expresó, se ve claramente que la Directiva del 95 “beneficia a las empresas que se encargan del tratamiento y/o transferencia de datos de carácter personal en detrimento de las personas físicas titulares de los datos (..) objeto de tratamiento y/o transferencia”, y apunta a tres razones que se han analizado en el artículo correspondiente al ámbito de aplicación de la LOPD: a) no se aplica la ley del país donde se produce el tratamiento ilícito de los datos personales del afecto (*lex loci delicti commissi*) sino la ley del país del establecimiento del responsable del tratamiento de datos; b) se apuesta por la ley conocida por las empresas que se encargan del tratamiento y/o transferencia de datos personales; c) se evita a las empresas que se encargan del tratamiento y/o transferencia de datos una multiplicidad de leyes, queda sometida a un solo derecho nacional. Obra cita, págs.95-96.

tual y global. ¿Quién debe proteger los DDFF de un ciudadano en esta situación actual?

El Reglamento del Parlamento Europeo y del Consejo de 11 de junio de 2007, relativo a la ley aplicable a las obligaciones extracontractuales, denominado “*Roma II*”, que comenzó su aplicación el 11 de enero de 2009²⁵⁰, excluyó el tratamiento ilícito de datos personales de su aplicación. Sólo se pudo regular esta materia hasta ahora a través del Código Civil español, artículo 10.9, que toma como referencia el *locus delicti*, o ley aplicable del lugar donde hubiera ocurrido el hecho del que se deriven los daños. Pero esa norma pudiera no tener incidencia en la realidad del ejercicio de los DDFF que ordenan toda la UE y el Derecho Español, fue una cuestión que la Sentencia del TJUE de 2015 dejó atrás. Se recuerda que el titular no conocía con certeza dónde están sus datos personales y quién los trata. Es imposible de saber dentro del entramado de cesiones (lícitas y/o ilícitas), almacenamientos, aportaciones (voluntarias, involuntarias, conscientes, necesarias o simplemente producto del ocio), y funcionamiento de la sociedad mercantil (ejemplo ya citados de tratamiento de datos personales para gestión y compras de bienes y servicios por empresas que operan, cada vez más, por *internet*: bancos, hoteles, viajes, productos de consumo, formación y educación, videojuegos, relaciones humanas, entre otros ejemplos de conductas)

Como ya se apuntó, la solución no pasaría por una restricción de las conductas ampliamente extendidas. No sería posible imaginar una actividad diaria sin comunicación y, por tanto, sin transmisión de datos personales. Qué ocurre entonces en EEUU, por-

²⁵⁰ Artículo 1.2.g del Reglamento del Parlamento Europeo y del Consejo de 11 de junio de 2007: *Se excluirán del ámbito de aplicación del presente Reglamento: (...) g) las obligaciones extracontractuales que se deriven de la violación de la intimidad o de los derechos relacionados con la personalidad; en particular, la difamación.* La norma quiere tener carácter universal dentro de la UE, su justificación se encuentra en la voluntad de garantía de funcionamiento del mercado interior y en las relaciones de los Estados Miembros con otros operadores internacionales, facilitando las tareas de los jueces nacionales ofreciéndoles una solución única para la determinación de la ley aplicable a las obligaciones extracontractuales, indiferentemente del Tribunal nacional ante el que se presente el litigio. Se refuerza la seguridad jurídica, principio del derecho europeo, al conocer la norma aplicable a una relación, junto con la libertad y la justicia. Obra citada, pág. 102-103.

que en ese país no se restringe el uso de datos personales salvo en un grupo de supuestos relevantes a nivel federal, sin perjuicio de que los diferentes Estados tengan alguna regulación adicional, fruto más de su actividad judicial que de normas legislativas. Las normas federales son la denominada por su acrónimo HIPAA (*Health Insurance Portability and Accountability Act* o Ley de transferibilidad y Responsabilidad del Seguro sanitario) del año 1996, por la que se reguló quién y cómo se puede tener acceso a la información de los seguros médicos, exclusivamente disponible para profesionales de la medicina y con la finalidad de coordinar la atención médica²⁵¹; la denominada también por su acrónimo FACTA (*Fair and Accurate Credit Transactions Act* o Ley Federal de Transacciones Crediticias Justas y Exactas) del 2003. Regula las posibles incidencias de seguridad de información en el crédito a los consumidores que puedan ser víctimas de un robo de datos²⁵²; y mencionar también la normativa denominada por su acrónimo COPPA (*Children's Online Privacy Protection Act* o Ley de protección de la privacidad de menores de los Estados Unidos) de 1998. Esta ley federal protege a los menores de 13 años de sitios web malintencionados o dañinos para y con los menores de edad.²⁵³ Es de resaltar la denominada *Privacy Act* o Ley de Privacidad de 1974, evolución jurídica de la *Freedom of information Act* FOIA o ley de libertad de información de 1966, que tiene muchos puntos en común con el derecho europeo a la protección de datos personales, aunque no sea configurado como norma constitucional tal y como se conoce en la UE²⁵⁴.

Las diferencias entre EEUU y la UE se reduce en una comparativa a los siguientes supuestos:

Europa	EEUU
Se confía en el Estado.	Se confía en el individuo.

²⁵¹ <http://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html>

²⁵² <https://www.privacyrights.org/facts-facta-fair-and-accurate-credit-transactions-act#1>

²⁵³ <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>

²⁵⁴ <https://foia.state.gov/Learn/PrivacyAct.aspx>

Normativas generales de Protección de datos	Sólo normativas sectoriales.
Agencias o Autoridades de Control	No existe Autoridad alguna de control.
Conflictos y casos tipificados en Ley.	Resolución de casos en Tribunales.
Norma preventiva.	Compensación de daños a través de Tribunales.
Protección a todo residente en la UE.	Se protege sólo a ciudadanos de EEUU
Se recaban datos imprescindibles y pertinentes.	Se recaban todo tipo de datos que el titular quiera aportar para la empresa o negocio con el que se relaciona.
Los ciudadanos piden protección a su Estado.	Los ciudadanos confían en su mercado con un enfoque liberal, el mercado, piensan, se auto-regula.
Sanciones por infracciones y penas por delito tipificado.	No existe ninguna referencia tasada. Se estudia en los Tribunales caso por caso.

En el sistema jurídico norteamericano, la definición de la privacidad o *privacy* se configuró con el paso del tiempo, delimitándose los intereses constitucionales que lo integran como ámbitos de la esfera privada que preservan la soledad requerida por el ciudadano, el secreto, la individualidad, la intimidad, la libertad de elección en asuntos personales, el control de la información propia, el desarrollo de la personalidad, así como del sustrato esencial de la inviolable dignidad humana, aspectos que se consideran por su sistema jurídico como inherentes a su condición de ser humano, ya no sólo con su ciudadanía democrática, donde el derecho a la privacidad es un elemento jurídico esencial denominado en su sistema *concepto de libertad de la Decimocuarta Enmienda*²⁵⁵. Resalta que en el siglo XXI los EEUU parecen proteger el derecho a la privacidad con normativas similares a las europeas en el contenido material. El bien jurídico protegido por el derecho a la privacidad es la información personal (*informational privacy*), afirmándose por la normativa federal que el principal atributo en el

²⁵⁵ Véase el análisis de SALDAÑA, N., "El Derecho a la Privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego.", *Teoría y realidad Constitucional*, nº 28, 2011. Los asuntos de los Tribunales norteamericanos analizados por la autora son de relevancia, aun no siendo la temática de esta exposición.

derecho a la privacidad es *la capacidad de la persona para controlar el flujo de información que le concierne, decidiendo cuándo, cómo y en qué forma es tratada la información personal*. Una definición muy similar a que se otorgó al concepto de derecho de autodeterminación informativa o derecho a la protección de datos personales en Europa²⁵⁶.

EEUU es un Estado que mantiene un elevado nivel de afinidad con Europa y con el que une historia e intereses tanto empresariales como humanos. Imaginemos qué puede unir a la UE con cualquier país del África subsahariana, Asia Central, alguna República de la Unión de Repúblicas Rusas o países donde los Derechos y Libertades Fundamentales ni existen ni se han nombrado jamás. Allí, en algún servidor con acceso remoto desde cualquier punto del planeta, podrían estar almacenados y tratados billones de datos personales de nacionales de la UE. Y no se puede ni acceder, ni rectificar, ni cancelar, ni oponerse a su tratamiento, tampoco se podría reclamar indemnización alguna ni existe tan siquiera la posibilidad, porque el tratamiento en esas condiciones es desconocido para el propio titular y si lo conociera, el ejercicio sería un imposible o al menos improbableísimo. Se diría, viendo un escenario de comparativas, que los ciudadanos de la UE queremos una regulación a la europea, pero actuamos y vivimos nuestras conductas a la americana, pues los hechos no se corresponden con las palabras en la prensa y en la política. Singular, sin lugar a dudas²⁵⁷. A los ciudadanos nadie los puede apartar de los usos extendidos en la red. No ya sólo *Facebook*, otro ejemplo

²⁵⁶ SALDAÑA, obra citada, p. 302.

²⁵⁷ Como se puede apreciar en la web del Parlamento Europeo con titulares como los siguientes: “El PE (Parlamento Europeo) moderniza las normas para salvaguardar la privacidad del ciudadano”; “Moraes defiende que se equilibre la protección de la privacidad y la necesidad de vigilar”; “Albecht indica que con la reforma de la protección de datos los europeos “estarán mejor informados”, “EEUU debe poner fin al espionaje masivo o afrontar las consecuencias, advierte el PE”; entre otros que se pueden visualizar y leer (de interés) Encomiable labor la de los eurodiputados. Pero la realidad, se repite de nuevo, es otra bien distinta. Véase en este sentido la clarificadora apreciación de GARRIGA DOMÍNGUEZ, A., “La protección de los datos personales en internet: problemas actuales”, *Derechos Humanos y protección de datos personales*, , 2013, pág. 31-48.

<http://www.europarl.europa.eu/news/es/top-stories/20130901TST18405/Protecci%C3%B3n-de-datos>

puede ser *Amazon*, el gigante de la distribución o el grupo español *INDITEX*, con ventas de productos a todo el mundo por *internet*. El hecho se aparta de tal manera de la norma, que, aunque el Estado pusiera todas sus capacidades legales en la protección de datos personales según el sistema actual, el titular no tendría en cuenta esa normativa, las conductas se llevarían a término al uso americano²⁵⁸. Entonces surgiría la siguiente pregunta: ¿Están ejerciendo éstos ciudadanos sus derechos y libertades fundamentales al desarrollar la conducta que desean? Obviamente la respuesta debe ser sí. Todo ejercicio de derechos y libertades entraña un riesgo que está más en el sistema que ejerce el poder que en el ejercicio efectivo del derecho y libertad del individuo. La conducta rige el derecho, no al contrario. La conducta de estos ciudadanos es lícita, está realizada desde su libertad y aceptación, no es dañosa, pues si bien es cierto que los datos pueden ser tratados sin conocimiento de su titular sin saber dónde, también es cierto que es muy difícil que trascienda al ciudadano común; incluso para casos de búsqueda de sujetos antijurídicos, como realiza la NSA norteamericana, no se centran en personas anónimas, de conductas habitualmente lícitas, sino en datos que pueden llamar la atención de sofisticados sistemas informáticos que se activan al recibir un dato que tienen programado como de posible interés. Después y al final, un ser humano debe escuchar y/o leer o ver toda esa información y concluir si es una conducta que pueda justificar el enorme gasto que supone la activación de los sistemas efectivos de seguridad nacional, es decir, identificar y analizar a la persona o personas en cuestión, pero en la vida real, ya no sólo en la virtual, pues la denominada *realidad virtual* no es constitutiva de conducta antijurídica, lo es solamente las consecuencias de esa conducta en la vida real²⁵⁹.

En cuanto a la situación de las empresas, dejando a un lado a las grandes corporaciones, las PYMES sufren la protección de datos personales como una posible amenaza a

²⁵⁸ Se tienen dudas de que los usuarios de videojuegos en red pudieran mantener la protección de datos personales ante la emoción de su delirante videojuego. Qué ocurriría con los usuarios de películas en *Netflix*, sin su película diaria. Cómo se compraría lo último en tecnología sin *Amazon*, sin *Dell* o sin *Apple*

²⁵⁹ Con cierto humor jurídico, debe ser un trabajo muy poco creativo y deseable. Se recuerda a título de comentario personal la excelente película "*La Vida de los Otros*".

sus pequeñas organizaciones y economías; se puede observar que la distorsionada realidad y la normativa inaplicable europea genera más problemas que beneficios bajo su perspectiva.

Además, desde el asunto *Snowden* de revelaciones de espionaje, el *puerto seguro* y el acuerdo que lo avala se cuestionaban, cuando la UE y EEUU se encontraban en negociaciones completamente secretas para un acuerdo de libre comercio entre estas zonas económicas, calculado en más de 2.000 millones de euros diarios, un tercio del flujo comercial mundial, cifra que se vería aumentada con la aprobación del Tratado. No llevar a término el TTIP extendía los perjuicios para ambas partes a ambos lados del Atlántico, ya no sólo para las empresas norteamericanas, cuya asociación de empresas de tecnología e innovación, la ITIF, estimaba en 2014 las pérdidas posibles entre 22.000 y 35.000 millones de dólares, al defender la NSA sus actividades de vigilancia electrónica y por tanto su influencia en el servicio de *cloud* o almacenamiento en nube, sector sumamente estratégico para muchas de las compañías norteamericanas, y también para la economía europea, que tendría un incremento superior a 68.000 millones de Euros anuales si el TTIP se realizaba. A eso se añadían las acusaciones entre compañías de EEUU de estar al servicio del gobierno chino, por ejemplo²⁶⁰. EEUU deseaba y defendía una red *internet* libre y abierta, pero no parece que estos conceptos signifiquen lo mismo para EEUU que para la UE. La cesión de datos al Gobierno no es una opción para las empresas norteamericanas, mientras para la UE, la cesión de datos a los Gobiernos se haría bajo, al menos en teoría, férreas garantías y sólo

²⁶⁰ PÉREZ MARTÍNEZ, J., "El derecho a la privacidad. Debate a ambos lados del Atlántico.", *Telos. Cuadernos de comunicación e innovación.*, nº , 2014, pág. 44-47. En un estudio de la Fundación Telefónica, se analizó con brevedad el escenario en el tema del derecho fundamental a la protección de datos y sus consecuencias en 2014 sobre las relaciones comerciales y económicas. En otra posición mucho más crítica LÓPEZ AGUILAR, J., "Data protection package y parlamento europeo", *Hacia un nuevo derecho europeo de protección de datos*, Valencia, 2015, pág. 45 y ss. En la página 73, el autor califica la situación de vigilancia o espionaje por parte de los EEUU como escandalosa, porque "ningún superpoder tecnológico autoriza o legitima la demolición de las garantías de nuestra libertad que están todavía hoy consignadas en la letra inviolable de nuestras Constituciones escritas (Artículo 18 CE y 8 de CDFUE)"

para su tratamiento autorizado por ley. Las empresas norteamericanas, buscando puntos de negociación factibles, remitieron una carta al Presidente Obama para que esta obligación de cesión de datos no fuera tan amplia, limitando los aspectos que pudieran contravenir las relaciones con otros países, pensando, lógicamente, en la EU.

La diferente percepción del derecho fundamental a la protección de datos por EEUU y la UE se debe a que, para los EEUU se está tratando de *privacy*, concepto que se aplica solamente a voluntad del individuo, mientras que la UE defiende un derecho fundamental constitucional, minuciosamente regulado, con rango de derecho público-constitucional y administrativo, que implica serias consecuencias en otros derechos fundamentales. Además de esta diferente percepción, *el debate de fondo no es sobre derechos, sino sobre intereses económicos*. Con estos antecedentes, la STJUE de *puerto seguro* sólo plasmó las diferentes interpretaciones de la realidad y de la norma. EEUU y la UE estarían abocados a entenderse, si no quieren que la UE se rompa en varios sistemas más o menos afines²⁶¹.

Otro texto muy interesante puede ser la Resolución de la AEPD con fecha de 9 mayo de 2014, por la que la Agencia resuelve la petición de *Microsoft Corporation*. La citada empresa solicitó autorización para la transferencia internacional de datos a EEUU,

²⁶¹ COMISIÓN EUROPEA, UNIÓN EUROPEA; "La Unión Europea y los Estados Unidos. Socios Mundiales con responsabilidades mundiales."]. Se nombra a la protección de la información y de los datos personales en la página 15 del texto, bajo el epígrafe "Unidos por los valores" - "Democracia y Derechos Humanos". De hecho, existía ya cooperación en el intercambio de datos personales entre organismos policiales de Europol y EEUU; también el intercambio de datos de viajeros, que desde hace muchos años se lleva a la práctica si se quiere viajar a EEUU. Se puede añadir en este punto las diferencias que ocupan al Reino Unido y a la UE, puesto que el Reino Unido ha realizado un referéndum cuyo resultado fue la aprobación por el pueblo británico de la salida de su país de la UE, y negocia en este momento una nueva situación. Quizá todo ello estuviera también ligado al desarrollo de la aprobación del Tratado de libre comercio, pues Reino Unido no iba a formar parte de un bloque que estuviera fuera de los intereses de sus empresas, íntimamente relacionadas con EEUU. La UE tendría mucho interés en el Tratado (que es una iniciativa de la administración del Presidente Obama), como puede apreciarse en la documentación de la Comisión que se referencia, pero no está claro en este momento cuál será la respuesta de la UE.

tal y como lo exige el artículo 33 LOPD y 70.2 del Reglamento, con la aprobación del Director de la AEPD, con la declaración de que *las garantías establecidas en la documentación que presenta son adecuadas para realizar TID a los EEUU y que los clientes que contraten los servicios MOS (Microsoft Online Services, de almacenamiento de datos en clouding) y suscriban los contratos aportados queden autorizados a realizarlas siempre y cuando las notifiquen previamente al Registro General de protección de Datos (RGPD)*. En este asunto la AEPD dio por aceptables las garantías que el Grupo Microsoft ofreció²⁶². Sobre el asunto cabe preguntarse, ¿se encuentra esta Resolución aún vigente después de la STJUE? A tenor de lo expuesto, la respuesta debe ser negativa. Pero en la realidad todo el sistema informático europeo, dependiente de la empresa Microsoft en un alto porcentaje de casos, siguió funcionando meses después de la Sentencia, sin interrupción. La AEPD se limitó a enviar una nota de comunicación²⁶³ a los responsables de ficheros o tratamientos inscritos en el RGPD de la AEPD cuyas TID a EEUU se encontraban bajo la regulación de *puerto seguro* por la que *a la mayor brevedad y en todo caso antes del 29 de enero de 2016, informe al RGPD sobre la continuidad de las transferencias y, en su caso, sobre su adecuación a la normativa de protección de datos*” la AEPD, si no recibía contestación o modificación de las TDI, *procedería a iniciar el procedimiento para suspenderlas temporalmente*²⁶⁴.

²⁶² <<https://news.microsoft.com/es-es/2014/06/06/aepd-servicios-cloud-microsoft/> La empresa publicó esta información en su web bajo el titular “La Agencia de Protección de Datos (AEPD) confirma las garantías de los servicios corporativos de Microsoft en la Nube para la exportación de datos”

²⁶³

https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/Comunicacion_responsables_-_Puerto_Seguro.pdf

²⁶⁴

http://www.elconfidencial.com/tecnologia/2015-12-08/ultimatum-de-la-aepd-a-empresas-espanolas-prohibido-usar-dropbox-o-google-apps_1116043/ Citando al abogado Pablo Fernández Bruguero: “si una empresa española usa, por ejemplo, un widget de Twitter en su página web o ha subido a su perfil fotografías en las que aparezcan personas identificables, podrá solicitar la autorización del Director de la Agencia Española de Protección de Datos. Para ello tendrá que presentar antes del 29 de enero un escrito de solicitud, el contrato empresa-Twitter firmado por ambas partes y una traducción jurada al español, y poderes suficientes de los firmantes, además de la correspondiente traducción jurada al español”.

La AEPD aplicó la Sentencia del TJUE anulando el intercambio de datos personales entre EEUU y Europa, con incidencias en los usuarios de las plataformas *Dropbox*, *Google Drive* o *Mailchimp*, *Facebook*, *Instagram* o *Twitter*²⁶⁵. Poco tiempo después, Europa y EEUU llegaron a un acuerdo político sobre las TID con un nuevo marco de protección denominado *Privacy Shield* (Escudo de privacidad) La comisaria europea de justicia, Vera Jourova, presentó en el verano de 2016 lo que denominó *garantías frente a las intervenciones de los servicios secretos de EEUU en los datos de ciudadanos europeos*. Las intervenciones de las autoridades de Seguridad norteamericanas se suponen limitadas y no generalizadas, para un restablecimiento serio de las relaciones entre ambos ámbitos políticos y geográficos. Sería la Comisión Europea el organismo que verificará estas condiciones cada año. También se presentó por parte de la Comisaria de Justicia varios cambios a tener en cuenta, como son la posibilidad de los ciudadanos para demandar a las empresas a través de un mecanismo contencioso específico, de forma gratuita y con plazo límite para la solución de las quejas en materia de protección de datos personales. En el mismo sentido, las peticiones en relación a los servicios de inteligencia o seguridad nacional serán examinadas por un defensor de los derechos de los afectados, que se crearía *ex professo* para esta cuestión, independiente de los gobiernos implicados. El Departamento estadounidense de comercio supervisará las normas de contratación y de tratamiento de datos personales. Por el momento, no se han adaptado las normas que hagan efectivo el citado avance político y, en consecuencia, los datos personales de los europeos se siguen almacenando en servidores extranjeros, sometidos a sus leyes territoriales o a ninguna ley.²⁶⁶

²⁶⁵ El diario El Confidencial con fecha 10 de diciembre de 2015 confirma la generalizada opinión. http://www.elconfidencial.com/tecnologia/2015-12-10/que-pueden-hacer-las-empresas-para-cumplir-las-exigencias-de-la-aepd_1117426/>

²⁶⁶ En este momento, el llamado Grupo de Trabajo del artículo 29 (GT29) ha presentado sus conclusiones frente al nuevo *Privacy Shield*. Las noticias sobre las actividades de este grupo se pueden encontrar en su página web http://ec.europa.eu/justice/data-protection/article-29/index_en.htm // http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm.

No se han determinado todavía en qué consistirá la nueva regulación. El GT29 parece ser que solicitó a la Comisión mayores garantías de las previstas. Otro asunto a tratar como reacción a estas cuestiones

Se puede diferenciar que, por una parte, está la norma y los DDF de los ciudadanos, ante el uso del Gobierno de EEUU de tratamiento de datos personales sin límites (*masiva e indiscriminadamente*), bajo el argumento de la seguridad nacional, lo cual se considera en Europa una lesión al derecho fundamental de protección de datos y otros derechos fundamentales. Por otra parte, las actividades extendidas mundialmente de pequeñas y medianas empresas europeas -entre las que se incluyen las españolas- que se puede ver en mayor o menor grado afectadas por esta colisión de normas, por ejemplo, existen empresas en España que venden servicios de almacenamiento de datos en servidores o en empresas de EEUU. Estas debieron ser las más afectadas, pues, en teoría, deberían interrumpir su actividad. En otro grado se encuentran las empresas que utilizan servicios de almacenamiento de servidores, que pueden contratar a otra empresa, sita en suelo de la UE, que confirme las garantías para las TID, más bien, que no realice TID. Todo ello implicaría una serie de trámites ante la AEPD y cambios técnicos en sus sistemas. Los costes serían inapreciables. Las grandes compañías norteamericanas están colaborando con las empresas españolas para firmar contratos en los que se comprometen a tratar los datos conforme a la normativa europea y dentro del EEE. Una solución técnica que están estudiando las empresas de mayor calado es la generación de almacenamiento de datos en *nubes isla*, almacenamiento en nube, pero por países o por áreas legales, para que la correspondiente legislación se adapte a ellas. Puede ser que todos estos cambios impliquen movimientos en las empresas, pero para los usuarios todo siguiera igual, puesto que las Condiciones

es la demanda de *Microsoft* contra el Gobierno de EEUU ante un tribunal federal sobre protección de datos personales, por las búsquedas secretas de sus clientes, que se apunta como un comentario. La compañía recibió unas 5.624 peticiones de información y en la mitad de los casos no pudo informarlos. El Gobierno de EEUU solicita informaciones de usuarios y las empresas norteamericanas tienen el deber de aportarlos. La empresa solicitaba unos límites razonables al Departamento de Justicia sobre este asunto, que, según *Microsoft*, viola la Quinta enmienda, la cual garantiza el derecho de la empresa privada a informar a sus clientes en caso de que las actividades del Gobierno afecten a sus datos personales. Aunque sería necesario el apoyo de muchas más empresas y ciudadanos para que esta acción prospere.

http://internacional.elpais.com/internacional/2016/04/14/actualidad/1460655633_558327.html

Generales de Contratación (que se consideran en su mayoría contratos de adhesión) para particulares siguen solicitando el consentimiento a los usuarios particulares para la transferencia de datos a cualquier servidor o país. Con lo cual, los datos realmente se siguen tratando en algún lugar del mundo, sin conocimiento del lugar físico por parte de su titular. Y todos los movimientos que se generan actualmente tienen como base las redes sociales más conocidas (y ya mencionadas), sin que ninguno de estos nuevos líderes se alce en contra de ellas, muy al contrario, las utilizan con frecuencia y facilidad²⁶⁷. En estas redes sociales, cuya TID es evidente, entre otras cosas, porque lo que desea el usuario es esa transcendencia abierta, mundial, de todo lo que expone, realmente existen varios tipos de usuario, pues no es lo mismo ser una personalidad conocida que ser un simple individuo, sin relevancia pública. La personalidad pública, quien es famoso por alguna razón (política, religiosa, prensa sensacionalista, *prensa rosa*, espectáculo) tiene cuentas especiales en las redes sociales donde su personalidad se identifica, tiene una personalidad confirmada de autenticidad, donde controla los tratamientos y contenidos que se exponen con su nombre e imagen; este tipo de cuentas en redes sociales no son gratuitas. El ciudadano sin relevancia pública no tiene esa ventaja frente al uso, tratamiento y destino de sus datos personales. Por otra parte, la doctrina entiende que la eficacia en la normativa depende altamente de la participación de los sectores afectados por las normas. Las TDI no son una excepción, por su conexión con el sistema de almacenamiento y tratamiento de datos en la nube (cloud), con el tratamiento de grandes cantidades de datos (big data) y con todos los fenómenos de comunicaciones en red que han propiciado una nueva dimensión de lo social hacia un concepto mundial. Esta realidad conduce a plantearse en el ámbito jurídico la eficacia de una co-regulación o autorregulación para el sistema jurídico de protección de datos personales (lo cual se tratará ampliamente en otros epígrafes) donde la legitimación perdida del sistema actual sea sustituida por la

²⁶⁷ Es conocida la afición del presidente Obama a las redes sociales, al igual que otros líderes mundiales, en una especie de directa comunicación con otros inexistente.

legitimación de la heterorregulación de los diversos sectores por parte de los diferentes Estados en sus sistemas jurídicos²⁶⁸.

4.4. Las normas europeas que establece el nuevo RGPD para las TID.

El RGPD dedica el capítulo V a las transferencias de datos personales a terceros países u organizaciones internacionales. El principio general para las TID se plasma en el artículo 44 RGPD, por el que sólo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del RGPD, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en esa norma, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización in-

²⁶⁸ Véase COTINO HUESO, L., "Algunas cuestiones clave de protección de datos en la nube. Hacia una "regulación nebulosa"", *Revista catalana de dret públic.*, nº 51, 2015, pág. 86-103, pág. 93. El autor se refirió explícitamente a los sistemas de *cloud*, pero se aportan sus ideas en este punto como clarificadoras en línea de una posible solución de ámbito mundial. En palabras del autor "Se afirma así que la regulación no debe venir únicamente de normas institucionales de poderes públicos, sino de la mano de un *regulador nebuloso (cloud-regulator)*. Esta regulación nebulosa resulta de la que genera las normas con la participación de la comunidad afectada (instituciones, individuos y las entidades empresariales implicadas), y tal regulación tiene necesariamente que ser aceptada y hacerse propia por los Estados e instituciones, que tienen que hacer valer tales normas. Esta regulación nebulosa de la nube, como infra se concreta, parece que va tomando cuerpo en razón de la acción no normativa de autoridades de protección de datos, al mismo tiempo que la consolidación de regulación técnica de origen privado por parte del sector. Y sobre esta base ya preexistente van a aprobarse normas propiamente dichas por la Unión Europea, sus instituciones y los Estados. Estas normas contendrán disposiciones básicas más generales que, a su vez, reenviarán al desarrollo de futuras normativas técnicas. Y esta normativa más concreta que en su día se apruebe por instituciones europeas o por Estados, sin duda, tendrá bien en cuenta la normativa técnica privada preexistente."

ternacional²⁶⁹. La Comisión decidirá qué países u organizaciones internacionales tiene el mismo nivel de garantía y de protección de datos que la UE. En esos casos, como actualmente, no es necesaria autorización específica, pues se basan en una decisión de la Comisión sobre su adecuación (artículo 45.1 RGPD). Para evaluar el nivel adecuado de protección, la Comisión debe tener en cuenta el Estado de Derecho, el respeto de los Derechos Humanos y las libertades fundamentales, además de la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos junto con la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes

²⁶⁹ Como establece el Considerando 101 RGPD, “Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales.”

de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros a través de compromisos internacionales vinculantes en relación con la protección de datos personales (artículo 45.2.a), b) y c) RGPD)²⁷⁰. Las autorizaciones de la Comisión serán revisadas al menos cada cuatro años, valorando los cambios y las condiciones políticas y sociales del tercer país u organización internacional, modificando, derogando o suspendiendo las TDI que fueron autorizadas (artículo 45.3, 4 y 5 RGPD)²⁷¹. Algo más novedoso es el artículo 46 RGPD, que regula lo que denomina *transferencias mediante garantías adecuadas*. No parece que se necesite una decisión de la Comisión ni una autorización de las autoridades de control para TID a países u organizaciones internacionales que hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas y que, además, cuenten con un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; o cuenten con normas corporativas vinculantes de conformidad con el artículo 47; o también con cláusulas tipo de protección de datos adoptadas por la Comisión en una decisión de conformidad, ya comentada; también se mencionan las cláusulas tipo de protección de datos adoptadas por

²⁷⁰ Considerando 102 RGPD: “El presente Reglamento se entiende sin perjuicio de los acuerdos internacionales celebrados entre la Unión y terceros países que regulan la transferencia de datos personales, incluidas las oportunas garantías para los interesados. Los Estados miembros pueden celebrar acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales siempre que dichos acuerdos no afecten al presente Reglamento ni a ninguna otra disposición del Derecho de la Unión e incluyan un nivel adecuado de protección de los derechos fundamentales de los interesados.”

²⁷¹ El Considerando 103 RGPD aporta que “La Comisión puede decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece un nivel de protección de datos adecuado, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas en lo que se refiere al tercer país u organización internacional que se considera ofrece tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin que se requiera obtener otro tipo de autorización. La Comisión también puede decidir revocar esa decisión, previo aviso y completa declaración motivada al tercer país u organización internacional.”

una autoridad de control y aprobadas por la Comisión; se menciona también el denominado código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o un mecanismo de certificación aprobado con arreglo al artículo 42, además de compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados (artículo 46.1 y 2 RGPD). Todo ello parece que se permite determinar por el responsable o el encargado del tratamiento de los datos, sin que sea necesario realizar ningún procedimiento ni petición ante las Autoridades de control, respetando y evaluando las garantías adecuadas, que pueden consistir en normas corporativas vinculantes o cláusulas tipo/cláusulas contractuales adoptadas por la Comisión o por alguna de las autoridades de control ²⁷². La nueva norma europea desea la implicación de los responsables y encargados del tratamiento para ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas tipo de protección de datos. En estos artículos y en el considerando 110 se promueve que los grupos empresariales o uniones de empresas que tengan una actividad económica conjunta puedan invocar normas corporativas vinculantes autorizadas para sus TID de la Unión a organizaciones dentro del mismo grupo empresarial o unión de empresa. Esas normas corporativas incorporarían todos los principios esenciales y derechos apli-

²⁷² Considerando 108 RGPD: “En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto.”

cables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal.

Se requiere la autorización de la Autoridad de control competente para TID que se basen en cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados (artículo 46.3).

Las TID no autorizadas serán las exigidas por un órgano jurisdiccional o autoridad administrativa de un tercer país a un responsable o encargado de tratamiento de datos personales que no se base en un acuerdo internacional. Se admiten las TDI que se basen en un acuerdo internacional vigente entre el tercer país y la EU o alguno de sus Estados miembros (artículo 48 RGPD)

La evidente ampliación del ámbito de aplicación no permitirá alegar en la práctica de las empresas internacionales que no les serían aplicables las normas europeas, con la intención de mejorar la situación jurídica y las garantías de los ciudadanos europeos, que antes de esta normativa debían desistir de su derecho a la protección de datos o solicitar la tutela de los mismos ante Tribunales de justicia internacionales o de otros sistemas jurídicos, como el de EEUU. También se aclara en el RGPD la posición de algunas plataformas de teóricos servicios gratuitos de intercambios, pero que en la realidad servían a otros fines, como pudiera ser el comercial por una red social de clientes o el político-social con evidente sentido de prospección de opiniones para agencias o empresas de estadística social.

4.4.1 Las excepciones a la norma general de las TID.

El RGPD establece la posibilidad de realizar TID para determinadas circunstancias reforzadas, como son cuando existe el consentimiento explícito del interesado, el cual debe ser informado exhaustivamente de los riesgos o cuando la transferencia es pun-

tual y necesaria en relación con un contrato o una reclamación. La excepción de interés público establecida por el Derecho de la Unión o de los Estados miembros es lógica dentro de la UE, o para consulta de un registro público establecido por ley o por personas que tengan un interés legítimo, a petición de las mismas, teniendo en cuenta los DDFF de los titulares e informando a la autoridad de control (artículo 49 RGPD)²⁷³. El responsable o el encargado del tratamiento deben garantizar a los interesados derechos exigibles y efectivos con respecto al tratamiento de sus datos en la Unión, una vez transferidos estos, de forma que sigan beneficiándose de sus DDFF y las garantías de los mismos (considerando 114).

4.4.2 La cooperación internacional en el ámbito del derecho a la protección de datos personales.

El RGPD se decanta, como se expone, por una implicación directa de las empresas con actividad internacional, entre otras organizaciones, en la protección de los DDFF a través del derecho a la protección de datos personales. Dentro de la UE se piensa por amplia doctrina que las normas están definidas y los derechos protegidos por las facultades que se otorgan al titular de los datos, el cual puede solicitar la protección de los Tribunales. Fuera del territorio de la UE, se puede poner en mayor riesgo o hacer inviable a los titulares de datos personales el ejercicio de los derechos de protección de datos (el *haz de facultades* que estableció el TC en el año 2000) o acudir a las Autoridades de control de los Estados miembros, ya que estas no podrán (ni pueden en la actualidad) tramitar reclamaciones ante terceros países, ni tan siquiera podrán investigar fuera de las fronteras de la UE. Aunque sea más efectiva la implicación empresarial, la UE también quiere desarrollar mecanismos de cooperación internacional para facilitar y proporcionar asistencia internacional mutua entre países, en la ejecución de legislación en materia de protección de datos personales. La Comisión y las Autoridades de control intercambiarían información y cooperación en actividades re-

²⁷³ Considerandos 111 y 112.

lativas al ejercicio de sus competencias con las autoridades competentes de terceros países, como ya se está realizando entre España, Portugal y los países de habla hispano-portuguesa en América, generando una interesante doctrina y nuevos derechos dentro de los países que se van interesando por la protección de datos personales, debido muy probablemente a la intensidad de intercambios económicos y culturales que unen a los países mencionados. Más difícil sería la situación en África y en Asia, donde, salvo Japón y Corea del Sur, la colaboración internacional en la protección de datos se encuentra con barreras difíciles de romper, pues, recordemos, China, aunque firmó en 1998 el Pacto Internacional de derechos civiles y políticos, va incorporando muy lentamente esos principios a su Constitución y a sus leyes. El RGPD establece en el artículo 50 (Cooperación internacional en el ámbito de la protección de datos personales) que la Comisión y las autoridades de control, en cuanto a relaciones con terceros países y organizaciones internacionales, se encargarán de tomar medidas para crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales, se prestarán, también mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales; fomentarán que las partes interesadas en la materia participen en los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales y promoverán el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países. Es sumamente evidente que el carácter global de las actividades y las interrelaciones de empresas y países generan una falta grave de efectividad a las regulaciones nacionales, las cuales no pueden resolver territorialmente los problemas que se plantean por las nuevas tecnologías, en un mundo global. Por tanto, si el mundo es global, las soluciones también deberán serlo. El Derecho Internacional se encuentra ante un reto que no puede eludir. Al igual que defi-

nió en su momento las relaciones entre los Estados sobre materias de Derechos Humanos y Derechos Fundamentales, deberá definir la regulación de unas situaciones sin fronteras, extraterritoriales, sin definición de ubicuidad, para los Derechos en general, Civil, Penal, o Mercantil junto con el derecho fundamental a la protección de datos personales²⁷⁴.

4.4.3 Las normas corporativas vinculantes

El nuevo RGPD define en su artículo 4. 20) las normas corporativas vinculantes como las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta. Todo grupo empresarial o

²⁷⁴ PÉREZ MARTÍNEZ, J., *Las reglas del juego en el ecosistema digital. Level Playing Field*, Madrid, 2016, pág. 124 y ss. Los autores utilizan una interesante terminológica que sólo se apunta como posibilidad de base a futuras definiciones: *ecosistema digital global*. Utilizan también expresiones en inglés como *Lever playing field*, que abarcan significados generales en cuestiones de mercados y competencia entre empresas, con la intención de generar reglas uniformes para todos los que intervienen en un escenario tecnológico global. Véase también las ideas al respecto de DOMÍNGUEZ MEJÍAS, I., "Hacia la memoria selectiva en Internet. Honor, intimidad y propia imagen en la era digital a partir de la jurisprudencia española.", *Revista Iberoamericana de Ciencia, Tecnología y Sociedad - CTS*, nº 11, 2016. También el análisis formulado por ORTEGA GIMÉNEZ, A., *Transferencias internacionales de Datos de Carácter personal Ilícitas*, Pamplona, 2016, pág. 75 y ss.. El autor argumenta que "Si conseguimos aproximar el marco jurídico de la UE a la nueva realidad social y tecnológica que vivimos hoy día habremos logrado no sólo garantizar el funcionamiento del (comillas del autor) "mercado interior de datos de carácter personal" sino también favorecer las relaciones comerciales entre la UE y terceros estados. Y la hoja de ruta de la UE la conocemos. Los objetivos están marcados: reforzar los derechos de las personas de modo que la recogida y el tratamiento de sus datos de carácter personal quede instrumentalizado, buscar la reducción de los trámites burocráticos para las empresas y garantizar niveles elevados de protección para los datos enviados fuera de la UE mediante la mejora y simplificación de los procedimientos de transferencia internacional de datos."

unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de la UE a organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal²⁷⁵. La norma europea se remite sin lugar a dudas a lo que la LOPD denominó Códigos tipo, regulados en los artículos 32 y ss. y el Reglamento les dedica el Título VII, artículos 71 y ss. Los Códigos tipo son normas deontológicas de buena práctica profesional, que debían ser depositados en la AEPD y contar con la aprobación de su Director, el cual podía realizar correcciones a los Códigos propuestos por los solicitantes de inscripción. El Reglamento establece que serían vinculantes para quienes se adhieran voluntariamente a los mismos.

El nuevo RGPD dedica el artículo 47 a las normas corporativas vinculantes en íntima unión con los artículos 63 y ss., dedicados al denominado mecanismo de coherencia, una norma por la cual las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, para contribuir a la aplicación coherente del RGPD en toda la UE. Será la Autoridad de control competente quien aprobará las normas corporativas vinculantes. No es una regulación global y mundialmente aplicable, pero el ámbito de aplicación se amplía considerablemente. Las normas corporativas deben ser jurídicamente vinculantes y se aplicarán y serán cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados. Los titulares de datos personales (que en el RGPD son denominados como interesados) tendrán derechos exigibles ante el ordenamiento jurídico competente.

Las normas corporativas vinculantes deberán especificar, como mínimo, la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros. De producirse una

²⁷⁵ Considerando 110 RGPD.

TID, se deberán incluir en las normas corporativas vinculantes, informando de las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión; también informarán de los DDFF y principios generales en materia de protección de datos personales, con especial incidencia en la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes. Los derechos de los titulares de datos en relación con el tratamiento y los medios técnicos empleados, el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22 RGPD, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79 RGPD, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes. Este asunto se presenta como muy interesante, porque hasta el momento las indemnizaciones por daños en materia de protección de datos con la regulación de la LOPD no eran ni frecuentes, ni cuantiosas, ni tan siquiera en ocasiones ejercitables, como se analiza en el epígrafe correspondiente, con lo cual se abren nuevas posibilidades para los titulares de datos, no tanto para que se reclamen cantidades, como para que el derecho a la protección de datos sea respetado por todos los que intervienen en el tratamiento, por el efecto persuasivo de las posibles indemnizaciones por daños ejercitables conforme a unas normas corporativas vinculantes. Otras cuestiones que se deben regular en estas normas son las relativas al responsable o encargo del tratamiento de datos, su responsabilidad y las consecuencias en casos de violaciones normativas, también la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, las funciones del delegado de protección de datos (artículo 37 RGPD), los procedimientos de reclamación, los mecanismos establecidos

dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes, los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la Autoridad de control, el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y por último, los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes y la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

La nueva regulación europea puede interpretarse desde el punto de vista de que se dirige hacia un nuevo modelo de protección de datos, a favor de las normas autorreguladas y vinculantes generadas por los responsables de tratamiento de datos personales, en especial, las empresas. La autorregulación empresarial bajo una Autoridad de control sería una solución factible, analizada ampliamente en un epígrafe de esta exposición.

4.4.4 Las Autoridades de control independientes.

El artículo 51 RGPD expone que cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes a las que denomina Autoridad de control, las cuales tienen como labor encomendada supervisar la aplicación del RGPD, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión. Las autoridades de control se someten a aplicar coherentemente el RGPD en toda la UE, cooperando entre ellas y junto con la Comisión.

Todo ello se regula en el capítulo VII del RGPD. En cada Estado miembro pueden existir más de una Autoridad de control, pero sólo una de ellas representará al Estado ante el Comité y todas ellas están sujetas al mecanismo de coherencia del artículo 63 RGPD. Los Estados miembro tienen de plazo hasta el 25 de mayo de 2018 para notificar a la Comisión las normativas que se desarrollen en materia de Autoridades de control de protección de datos según el RGPD. Se quiere interpretar que nuestro Estado español tendrá todas las normas dispuestas para esa fecha.

5. Las múltiples excepciones a la aplicación de la Ley de Protección de datos personales.

5.1. La denominada excepción doméstica de tratamiento de datos personales.

El artículo 2.2 LOPD reguló las excepciones a la aplicación de la ley en tres supuestos. El primero de ellos es el punto a) En él, se establece que la Ley de protección de datos no será de aplicación “A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.”

El legislador trasladó a este artículo de la LOPD casi literalmente la traducción del artículo 3.2. de la Directiva 95/46/CE²⁷⁶. Este mismo concepto se contempló en el Considerando 12 de la Directiva 95/46/CE. El Reglamento del 2007 precisó en algo el texto de la Ley española²⁷⁷. Como se puede observar, la LOPD matizó y concretó lo

²⁷⁶ “Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales (...) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas”

²⁷⁷ Artículo 4.a) del Reglamento: “El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos: (...) a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de las particulares”

que la LORDAT dejó sin precisión. Los datos de carácter personal en la Ley del 92 que fueran mantenidos por personas físicas *con fines exclusivamente personales* quedaban fuera del ámbito de aplicación de la Ley. La LOPD reduce este ámbito de aplicación, pues no contempla únicamente el fin personal de la información, sino también la actividad que se realice con ella. La actividad condiciona la exclusión. Un grupo de datos, que es lo que se denominó fichero en la LOPD, como puede ser una agenda personal, con nombre, dirección y teléfono de las personas con las que nos relacionamos con fines privados, personales, domésticos, dentro de una esfera no comercial, deja de estar excluida del ámbito de aplicación de la LOPD cuando se utiliza con fines comerciales o profesionales²⁷⁸. En ese momento, quedaría bajo las exigencias de la LOPD. Esta diferencia es muy trascendente en la práctica, pues diferenciar cuándo un profesional utiliza –o no utiliza– sus contactos personales para fines profesionales es, en muchas ocasiones, difícil por no decir imposible²⁷⁹. También se incluyen en la LOPD ficheros mixtos, los que se utilizan para fines privados como profesionales o comerciales²⁸⁰. Sin embargo, la excepción tiene su sentido más común en la exclusión del ámbito de aplicación de la LOPD a una actividad exclusivamente privada o familiar²⁸¹.

²⁷⁸ MEGÍAS QUIRÓS, JOSÉ JUSTO; , "Comentario al artículo 2.2.a) LOPD. ", *Comentario a la Ley Orgánica de Protección de datos de carácter personal.*, Madrid, 2009-2010, pág. 115-133. El autor es profesor de Filosofía del Derecho en la Universidad de Cádiz.

²⁷⁹ Obra cita, página 117. Cita el autor el caso de un médico, que tiene una agenda con datos de amigos, de la que algunos son pacientes. Esta agenda, se considera un fichero y además estaría sometida a la LOPD. No sería así en la anterior LORDAT.

²⁸⁰ Destaca el autor la redacción del Reglamento, al incluir todos los supuestos posibles en cuanto a la acción que es objeto de la excepción: La LORDAT reglaba la exclusión de “mantener ficheros”, mientras que la LOPD utilizaba la expresión “efectuar tratamiento de datos personales”. El Reglamento resuelve esta discusión redactado así: “ficheros y tratamientos realizados o mantenidos”.

²⁸¹ Como ejemplo, la organización de una boda. Sería absurdo, en palabras del autor mencionado, “obligar a las personas que programan su boda o cualquier celebración familiar a cumplir los requisitos exigidos para el tratamiento de datos con la lista de invitados en las que aparecen los nombres de éstos, número de hijos, dirección a la que se debe enviar la invitación teléfono, alojamiento programado, etc.” Es un absurdo en 2009. En el año 2015, se puede cuestionar esa afirmación, veremos cómo y en qué sentido.

¿Qué quiso decir el legislador cuando habla de *actividad exclusivamente personal o doméstica*? Esta afirmación resulta matizada por la AEPD y por los Tribunales: la Sentencia del TJCE (Tribunal de Justicia de las Comunidades Europeas) de 2003 en el llamado caso *Lindqvist*²⁸², La SAN 3077/2006, de 15 de junio de 2006, o caso *Academia Militar de Zaragoza*²⁸³ y resoluciones de la AEPD que no siempre han sido estimadas por los Tribunales.

El TJCE en el caso *Lindqvist* no apreció la excepción doméstica de tratamiento de datos pues decidió 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/CE²⁸⁴.

²⁸² Sentencia de TJCE, de curia.europa.eu, el 6 de noviembre de 2003, extraído de TRIBUNAL DE JUSTICIA DE LAS COMUNIDADES EUROPEAS, con núm. C-101/01:B Lindqvist.

<http://curia.europa.eu/juris/showPdf.jsf?jsessionid=9ea7d0f130d58d2074b464664bebb043eb21ab7521c8.e34KaxiLc3eQc40LaxqMbN4ObNmPe0?text=&docid=48382&pageIndex=0&d>

clang=es&mode=lst&dir=&occ=first&part=1&cid=365906, a 20 de septiembre de 2015.

²⁸³ Sentencia de , de aepd.es, el 15 de junio de 2006, extraído de AUDIENCIA NACIONAL, con núm. Sentencia 15 de junio de 2006, Sala de lo Contencioso-Administrativo. http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/audiencia_nacional/common/pdfs/sentencia_AN_15062006.pdf

²⁸⁴ Punto 1 y 2 de las Declaraciones del TJCE que matiza con anterioridad a la Declaración en el párrafo numerado como 47. “Un tratamiento de datos personales de esta naturaleza no está comprendido en ninguna de las excepciones que figuran en el artículo 3, apartado 2 de la Directiva 95/46/CE.” (...) “Este tipo de tratamiento no puede ser incluido en la excepción de actividades exclusivamente personales o domésticas, a diferencia de la llevanza de un repertorio de direcciones o de la correspondencia (ejemplos propuestos en el considerando 12 de la Directiva 95/46/CE) pues 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 éste el caso en un tratamiento de datos personales consistente en la difusión de dichos datos por internet de modo que resulten accesibles a un grupo indeterminado de personas

En la segunda Sentencia que se aporta en este análisis, se estableció un criterio diferente. Fue el acto de celebración con motivo de las Bodas de Plata de una promoción de la Academia militar de Zaragoza en el año 2001-2002. La Comisión de celebración de este evento (*“Comisión para las bodas de plata de la XXXV promoción de la Academia Militar de Zaragoza”*) entregó una lista elaborada con las diferentes agendas particulares de todos los promocionados asistentes. Este listado, con nombre, dirección, Cuerpo al que pertenecían, etc., se entregó a una agencia de viajes con la única finalidad de contactar con ellos, informar sobre el acto y organizar así la celebración. La agencia se comprometió a destruir ese listado o a devolverlo una vez que el evento fuera realizado, y con ello, finalizado su trabajo. Las alegaciones de los miembros de la Comisión se centraron, según la Resolución de la AEPD, en que “Teniendo en cuenta la finalidad lúdica para la que se realizó el listado y que se trataba de una recopilación de datos entre los mismos compañeros de una promoción, consideraban que se trataba de un tratamiento de los previstos en el artículo 2.2.a) de la LOPD y, por tanto, fuera de su ámbito de aplicación.” La AEPD, sin embargo, consideró que habían sido vulnerados los derechos del demandante, y afirmó en su Resolución que: “Si bien el origen de datos eran agendas personales, no es menos cierto que una vez que dicha información sale de la esfera personal y forma parte de un conjunto de datos recogidos para la promoción de un evento, nos encontramos ante un tratamiento de datos sujeto al ámbito de aplicación de la LOPD”²⁸⁵

La Sala de lo Contencioso-Administrativo de la Audiencia Nacional anuló la sanción (cuantificada en algo más de 6.000 €) Y lo hizo con las alegaciones que se citan, en el FJ 3 de la SAN 3077/2006, de 15 de junio de 2006: *“Lo relevante para la sujeción al régimen de protección de datos no será por tanto que haya existido tratamiento, sino si dicho tratamiento se ha desarrollado en un ámbito o finalidad que no sea exclusivamente personal o doméstico”*. El propio Tribunal de la AN añade en el punto si-

²⁸⁵ Resolución que fue, como vemos, recurrida: R/00260/2004 http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2004/common/pdfs/PS-00116-2003_Resolucion-de-fecha-28-04-2004_Art-ii-culo-6.1-LOPD_Recurrida.pdf a 20 de septiembre de 2015. Página 6 del pdf.

guiente: *“qué se ha de entender por personal o doméstico no es tarea fácil”*. La Sala de la AN pone el ejemplo de la lista de bodas: *“Tampoco hay que entender que el tratamiento se desarrolla en un ámbito exclusivamente personal cuando es realizado por un único individuo.”* (...) *“No deja de ser personal aquella actividad de tratamiento de datos que, aun siendo desarrollada por varias personas físicas, su finalidad no trasciende de su esfera más íntima o familiar, como la elaboración de un fichero por varios miembros de una familia a los efectos de poder cursar invitaciones de boda. Y un tratamiento de datos personales realizado por un solo individuo con finalidad profesional, mercantil o industrial estará claramente incluido en el ámbito de aplicación de la ley 15/1999”*. Según la Audiencia Nacional el ámbito: *“Será personal cuando los datos tratamos afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos”*. La Sala entendió que el caso objeto de recurso se encontraba en esta definición, y por ello, consideró que no estaba dentro del ámbito de protección de datos personales²⁸⁶.

Se puede marcar la confusión en los textos jurídicos (jurisprudencia, doctrina, incluso en algún texto legal) entre vida privada (o su traducción del inglés: privacidad) e intimidad. Muchas veces se utilizan como sinónimos, cuando realmente no lo son. El ámbito de la intimidad se reduce al interior de cada persona; la esfera privada se desarrolla en un ámbito más amplio, familiares, amigos, compañeros de trabajo, de estudios, etc. Sería necesario que en los textos legales y en la jurisprudencia se gene-

²⁸⁶ La Sala considera en este punto que: *“La pretensión de que tales actividades, en cuanto al tratamiento de datos, debieran quedar sujetas a los principio de protección contemplados en la ley 15/1999 con fundamento en una concepción maximalista del principio del consentimiento, como parece expresar la Agencia de Protección de Datos, conllevaría una desnaturalización de las relaciones sociales, sometiéndolas a unos rigores formales en cuanto al manejo de datos personales totalmente ajenos al sentir social y en modo alguno exigidas por el derecho fundamental a la autodeterminación informativa, derecho que no es absoluto y que debe ser interpretado en cuanto a sus manifestaciones y exigencias partiendo de su contraposición con otros derechos y valores constitucionales, como el libre desarrollo de la personalidad, y de la realidad social a la que está dirigido.”*

rase una misma terminología²⁸⁷. Se puede añadir lo que en 1991 escribieron dos notables periodistas sobre esta diferencia²⁸⁸: *la vida privada puede ser objeto de información cuando se convierte en pública, la vida íntima es un núcleo totalmente reservado, no puede, ni debe, ser objeto de información.*

Se considera la decisión de la AN como acertada, porque los hechos estaban dentro de esa privacidad o ámbito personal. Se puede añadir un importante comentario: La consideración de actividad privada hubiera sido distinta si el listado hubiera sido dado a conocer fuera de ese círculo de personas. Así mismo se considera que otras Resoluciones de la AEPD no fueron acertadas, pues las basó en esta Sentencia de la AN, cuando los hechos eran distintos. Los datos se recopilan para fines teóricamente privados, pero si se otorga accesibilidad a un número indeterminado de personas, de todo el mundo, a través del sistema de comunicación *internet* o cualquier otro, se produce una desprotección de los mismos y, por tanto, de los titulares de dichos datos. Es el tratamiento y acceso a los datos lo que marca la seguridad y la protección de la información personal, no tanto cómo fue recopilada. Se puede recopilar datos de carácter personal y no hacer nada con ellos, simplemente almacenarlos. No tiene finalidad, no tiene sentido. Nadie accede. La problemática para los titulares de esos datos personales y, por tanto, su desprotección, se produce cuando comienzan a utilizarse, a tratarse, para lo que siempre se necesita una *finalidad legítima*. El acceso a los datos por los usuarios que van a tratarlos será el punto que más seguridad aporte a la protección efectiva, y al derecho fundamental a la protección de datos personales, derecho que va unido en la actualidad a la eficacia y efectividad de múltiples derechos. En el caso de la catequista sueca, sin ánimo ninguno de vulneración de derechos, la demandada se vio inmersa en un asunto muy desagradable para todos los implicados, por la inocencia de pensar en lo positivo de la cuestión (información de todos disponi-

²⁸⁷ Notas y referencias sobre la autora Helena BEJAR, entre otros.

²⁸⁸ DESANTES, J.M. y SORIA, C. “Los límites de la información” Asociación de la Prensa de Madrid, cita del autor. Véase página 126, obra citada: “una conversación entre dos personas sobre el tiempo, puede pertenecer a la privacidad o vida privada de esas personas, pero no a la intimidad; la consideración sería muy distinta si estuvieran hablando sobre la enfermedad de uno de los interlocutores”.

ble para todos) y no en la exposición indeseada de los titulares de datos personales. No había ninguna malicia, al igual que no puede existir intenciones discutibles en los que desean realizar un evento familiar y de amigos, como una boda. El problema surge cuando el acceso a todas esas informaciones se realiza vía *internet* sin permisos ni control de acceso ninguno, con tratamiento (copia, transmisión, modificación) también, generalizado. En ese caso, desde luego que la vulneración del control de datos por sus titulares es evidente (la foto de cuando se tenían 3 años y que la abuela guardó con cariño, pero que en *internet* se convierte en el objeto de burla de compañeros de trabajo que ni tan siquiera conocemos; la historia de nuestra mejor amiga sobre el primer novio; la fiesta de fin de año que se debe olvidar, como ejemplos) Sin las comunicaciones actuales, la falta de control estaba limitada a la prensa, en caso de que el titular se convirtiera en *famoso* y de algunos conocidos que escondían como diamantes esos documentos para no se sabe bien qué finalidades, pero no pasaba de ahí. En la actualidad, se cuestiona si realmente esta exclusión de aplicación de la LOPD para eventos llamados familiares o privados realmente lo son, debido a las telecomunicaciones y los formatos en red que promueven los intercambios de información²⁸⁹.

En una versión diferente de los hechos, cualquier empresa o institución (desde la comunidad de vecinos hasta la asociación de deportes, pasando por multitud de posibles personalidades profesionales y/o jurídicas), se ve obligada en cumplimiento de la LOPD a realizar cuantiosas gestiones derivando recursos económicos para garantizar el derecho a la protección de datos de todas sus relaciones, desde el trabajador por cuenta ajena en un taller, a la cliente de la empresa de muebles; todos, grandes, medianas y pequeñas empresas, autónomos, profesionales de cualquier sector, están condicionados por ese cumplimiento²⁹⁰. Mientras tanto, los titulares de datos se con-

²⁸⁹ Con cierto humor, pero sin eliminar su trascendencia existirá una prima que odia a alguien y que coloque en su perfil de red social de forma instantánea esa foto indexada con nombre y apellido que nunca se quiso hacer pública por su titular, con acceso ilimitado por parte de cualquier persona con un ordenador, y que, por tanto, ve ese *headhunter* que selecciona personal para la empresa en la que se ha entregado el curriculum. Por supuesto que se tienen muchas posibilidades de que el seleccionador no tenga la mejor versión del candidato/a y deseche el CV en una destructora.

²⁹⁰ Cumplimiento efectivo a través de las medidas de seguridad.

vierten en voluntarios proveedores de los mismos en webs de apps gratuitas, redes sociales (Facebook, Twiter, por ejemplo), redes de comunicaciones (hasta hace poco, WhatsApp, por ejemplo) sin leerse tan siquiera las condiciones del servicio, ya no la política de privacidad, muchas veces inexistente. Se consideraría por una parte de la doctrina, que la exposición pública por el titular de los datos de material privado y no digamos íntimo, rompe con el derecho a la protección de datos y a la obligación de protección de los mismos, que recae sobre empresas, profesionales y operadores sociales legítimos. Si una persona es capaz de exponer con voluntariedad y alegría toda su vida en *internet* (no sólo nombre y apellidos) no puede pretender que una empresa se vea involucrada en su falta de seguridad para sus propios datos y derechos, que es lo que ocurre en este momento. El ámbito de aplicación de la LOPD no debería incluir estas situaciones, no por ser pintorescas, menos frecuentes. Otros autores no coinciden con esta idea. Consideran que el usuario de los servicios en *internet* tiene una posición efectiva de debilidad frente a las empresas que ofrecen los servicios, los cuales son opacos y muy difíciles de controlar. En ese contexto, el usuario y titular de datos personales se encuentra en una situación que se ha equiparado como semejante a la de los trabajadores frente a la empresa, por lo que se debería tener una posición de salvaguarda de los derechos fundamentales del titular/usuario, parte más débil en esa relación con los proveedores y operadores de sistemas en red. Es muy posible que el Estado deba actuar en cuanto a los casos de protección de datos, incluso frente al propio titular que los expone, vulnerando sus derechos y los de otros, calificando determinadas conductas como vulneradoras de derechos fundamentales y actuando de oficio incluso invalidando la voluntad del propio titular e imponiendo a las empresas los límites a los que el titular renuncia²⁹¹. La pregunta de fondo es ¿son renunciabiles los DDFF en estos casos? ¿se puede aplicar la misma doctrina que se aplica al derecho

²⁹¹ Véase a este respecto el análisis de VILLAVERDE MENÉNDEZ, I., "La intimidad, ese "terrible derecho" en la era de la confusa publicidad virtual", *Espaço Jurídico*, nº 3, 2013, pág. 57-72. "La tesis sería: puesto que el derecho a la intimidad está ligado a la dignidad de la persona, al Estado le compete el deber positivo (artículo 9.1 CE) de adoptar medidas y arbitrar mecanismos que garanticen en la red el pleno disfrute de los derechos fundamentales de los usuarios, incluso en el caso de que éstos renuncien a su ejercicio o consientan su lesión por terceros" página 68.

fundamental a la intimidad? Según VILLAVERDE MENÉNCEZ el Estado tiene el deber de proteger y preservar la intimidad de los ciudadanos frente a las agresiones que pudieran sufrir a través de las redes en *internet* (mediante ley orgánica, pues se trata del desarrollo de derechos fundamentales). La protección del derecho a la intimidad conllevaría sin duda el riesgo de limitar los derechos a la libre información y expresión en algunos casos, que podría ser objeto de lo que se denomina en la terminología legal anglosajona *prior restraints* o censura previa, posible sólo en algunos casos en los países democráticos con libertades de expresión e información constitucionales, como puede ser la protección de los menores ante ciertos contenidos o la calificación de películas, videojuegos u otras actividades. Las empresas proveedoras de servicios de comunicación (*YouTube, Facebook, Instagram o Twiter*, por ejemplo) ya contemplan restricciones en los contenidos y en los accesos, evitando muchas situaciones ilícitas, en especial para salvaguardar la intimidad de terceros y para ejercer un control sobre los contenidos que los ciudadanos pretenden publicar. Aparte de esta actuación empresarial, quizá sería prudente no dejar sin regular determinados aspectos sobre el uso de las diferentes formas de comunicación, como puede ser el acceso de menores de edad, la comprobación de la personalidad, la seguridad en la exposición de datos personales de otros, etc.

Como otros ejemplos de excepciones domésticas, la AEPD dictó dos importantes Resoluciones sobre la exclusión de la LOPD a los datos que formen parte del ámbito privado o íntimo. La primera es la Resolución E/04001/2011²⁹². Este asunto trató de un acoso a un niño por parte de otros escolares a través de una red social. En estos casos se cuestiona la denominada *excepción doméstica* pues hay supuestos en que se están revelando datos personales a la red o a un entorno no privado, como pueden ser la utilización de la red social como una asociación o como una parte de una empresa,

²⁹² AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Resolución E 04001/2011"]. http://www.agpd.es/portalwebAGPD/resoluciones/recursos_reposicion/rr_sobre_archivo_de_actuaciones/common/pdfs/REPOSICION-E-04001-2011_Resolucion-de-fecha-13-08-2012_Art-ii-culo-6-LOPD.pdf a 28 de septiembre de 2015.

con finalidades comerciales, políticas o benéficas, por ejemplo; en estos casos el usuario tiene todas las obligaciones de un responsable de datos que está revelando datos personales a terceros. Otro caso es la inclusión de datos en redes sociales abiertas. En este asunto la exención doméstica sólo se aplica si la red social garantiza la privacidad, con acceso restringido a los contactos seleccionados, en los que no puede haber, a su vez, réplicas o copias de esa información. Cuando el acceso a la información es abierto a cualquier usuario, se facilita el perfil de usuario a toda la red social o son datos de los denominados *indexables* por los motores de búsqueda por *internet*, el usuario asume todas las obligaciones de cualquier responsable de ficheros, y si realiza estas acciones se considera que está revelando datos personales protegidos por la LOPD a otros. Cuando el usuario configura el acceso a su perfil social para todos los usuarios de la misma tampoco se considera que sea de aplicación la exención doméstica. Y el otro supuesto es cuando se publican en una red social o cualquier otro medio de acceso a información a través de *internet* datos sensibles como son los de origen étnico, creencias religiosas, ideas políticas o filosóficas, datos de salud, vida sexual, violencia, y cualquier dato denominado sensible o íntimo. En este caso tampoco se aplica la excepción doméstica, por el carácter de los datos publicados, especialmente protegidos²⁹³.

El segundo texto es el informe 615/2008²⁹⁴, que analiza la pregunta de unos particulares sobre si pueden compartir datos de sus hijos (incluyendo imágenes) realizando

²⁹³ Se comenta la iniciativa de 2017 sobre el control de datos de violencia (terrorismo, abusos, agresiones) a través de imágenes que la empresa Microsoft hizo pública. Se trata de un programa (software) capaz de identificar el contenido de las imágenes personales y no permitir su divulgación, denominado *PhotoDNA*, el cual permite identificar a quien las divulga. <http://www.elindependiente.com/economia/2016/12/07/facebook-abusos-internet/> Facebook ha emitido un comunicado en el que informa de su aplicación <http://newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/>. Otras empresas también comunicaron su adhesión al proyecto.

²⁹⁴ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Informe sobre implicación de la LOPD a la actividad de particulares que comparten fotos de sus hijos por Internet."]. http://www.agpd.es/portaIwebAGPD/canaIdocumentacion/informes_juridicos/ambito_aplicacion/com

actividades extraescolares. En el informe de la Agencia se concluye que: *“Para que nos hallemos ante la exclusión prevista en el artículo 2 LOPD, lo relevante es que se trate de una actividad propia de una relación personal o familiar, equiparable a la que podría realizarse sin la utilización de internet, por lo que no lo serán aquellos supuestos en que la publicación se efectúe en una página de libre acceso para cualquier persona o cuando el alto número de personas invitadas a contactar con dicha página resulte indicativo de que dicha actividad se extiende más allá de lo que es propio de dicho ámbito”*²⁹⁵.

El RGPD sigue manteniendo la excepción doméstica en el artículo 2. c), Ámbito de aplicación material, excluyendo la aplicación de la normativa a los tratamientos de datos personales efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. No ha precisado en exceso, dejando de nuevo sin definir qué se puede considerar tratamiento doméstico de datos personales en la actual civilización de las redes sociales y los mensajes.

mon/pdfs/2008-0615_Inaplicaci-oo-n-LOPD-a-actividad-de-particulares-que-comparten-fotos-de-sus-hijos-a-trav-ee-s-de-Internet.pdf a 28 de septiembre de 2015.

²⁹⁵ Véase la página 4 del Informe citado. Existe actualmente una fuerte controversia en cuanto a las fotos que se comparten por Internet de los hijos de padres separados o divorciados, que no se ponen de acuerdo en cuanto a la publicación de la imagen del menor. Son muchos casos que acaban ante el juez, pues los progenitores que comparten la patria potestad discrepan en este asunto y deben ser los Tribunales quienes decidan. Las Sentencias no son unánimes en su criterio. Se dictan Sentencias por los Juzgados de Familia que permiten la publicación de imágenes del menor siempre que el otro progenitor no se oponga expresamente. En otras, se solicita el consentimiento expreso del otro progenitor. Además, se añade que algunos jueces entran a considerar el uso razonable y adecuado de la imagen del menor, para que no atente a su honor e intimidad en el futuro, incluso al margen del consentimiento de los progenitores (artículo 2 LO 1/1996, de protección del menor). La LOPD establece que los menores de 14 años deben contar con el consentimiento de ambos progenitores para publicar datos personales ellos mismos, pero en el caso de progenitores que publican datos, la controversia está abierta a determinar todavía si los datos de menores de edad pueden publicarse por un tercero (progenitor u otro familiar, amigo o persona relacionada con el menor)

5.2. Las excepciones sobre materias clasificadas.

El artículo 2.2.b) excluyó del ámbito de aplicación de la LOPD a los ficheros sometidos a la normativa sobre protección de materias clasificadas. El Reglamento del 2007 tuvo prácticamente la misma redacción. Se trata de una cuestión sumamente controvertida, como consecuencia de las implicaciones sobre los DDFF en la ciudadanía²⁹⁶. Según una parte de la doctrina, los ciudadanos tendrían un evidente y necesario *derecho a conocer* basado en el artículo 20 CE, derecho a recibir información veraz, vinculado con el artículo 53.1 y 2.; además todos estos aspectos se manifiestan en el apartado 2 del artículo 1 CE. El artículo 105 b) CE recoge con rango constitucional una norma que

²⁹⁶ Véase DEL CASTILLO VÁZQUEZ, ISABEL CECILIA; , "Artículo 2.2.b) Ficheros sometidos a la normativa sobre protección de materias clasificadas. ", *Comentario a la ley de protección de datos de carácter personal.*, Madrid, 2009. La autora comienza su análisis con una frase que operaba en la legislación del Régimen preconstitucional: "Nada nuevo se descubre cuando afirmamos que el verdadero control a la actividad política es posible gracias a la transmisión de la información que obra en los poderes públicos y el consiguiente conocimiento de las cosas públicas, "Porque las cosas públicas que a todos interesan pueden y deben ser conocidas por todos". Según las notas de la autora, lo extrae de la ley 9/1968 de 5 de abril, de Secretos Oficiales, modificada por la Ley 48/1978 de 7 de octubre. También su tesis doctoral DEL CASTILLO VÁZQUEZ, I., *Protección de datos: Cuestiones constitucionales y administrativas: el derecho a saber y la obligación de callar*, Madrid, 2007. Y el artículo DEL CASTILLO VÁZQUEZ, I., "Transparencia, acceso a la documentación Administrativa y protección de datos de carácter personal.", *Revista Foro Nueva Época*. Servicio de publicaciones de la Universidad Complutense de Madrid, 2007, pág. 231-254. De otros autores, hacia una visión desde el Derecho Penal, que no se analiza en este trabajo, PEDRAZ PENALVA, E., *Protección de datos y proceso penal*, Madrid, 2010. Resaltan en esta obra colectiva los textos de ÁLVAREZ GARCÍA, F., "El acceso por parte de las Fuerzas y Cuerpos de Seguridad del Estado a ficheros de datos personales", *Protección de datos y proceso penal*, Madrid, 2010, pág. 53-88. El autor afirma que "resulta evidente que seguridad, protección de datos y transparencia han de encontrar la forma de convivir". Citando a PIÑAR MAÑAS, el autor añade que "no existe en absoluto una contradicción entre tales derechos o situaciones de libertad (libertad de expresión, transparencia, seguridad...) y la protección de datos. Más bien al contrario: sólo respetando el derecho fundamental de todos a la protección de datos personales se conseguirá un marco adecuado de respeto a la libertad de expresión y al derecho de acceso a la información; un correcto desarrollo del mercado y una eficaz lucha contra el terrorismo". Cita de pág. 57.

muchos juristas consideran muy apropiada, aunque otros piensan que es una norma administrativa a la que la CE le otorgó ese rango. Por el artículo 105 b) CE *la ley regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad nacional y defensa del Estado, la averiguación de delitos y la intimidad de las personas*. Con el derecho de acceso a la documentación que las AAPP gestionan, se ha creado una Administración democrática donde la participación ciudadana y la transparencia obran como principios, y hacen posible el derecho a la información y la libertad de expresión²⁹⁷.

El problema es saber qué entiende el legislador por seguridad nacional, defensa del Estado, averiguación de delitos e intimidad de las personas. El ATS 821/2006, de 26 de septiembre estableció que *“sería preciso admitir que el sacrificio de algunos derechos o de aspectos parciales de los mismos, es necesario en ocasiones para garantizar la propia supervivencia del sistema democrático e incluso para asegurar a los ciudadanos la misma existencia y eficacia de aquellos derechos individuales”*²⁹⁸. Y añadió una definición a este límite, *“la existencia de un derecho a la libre información que lleva aparejado el derecho a investigar y a recabar el conocimiento de los datos, no conlleva la necesaria obligación, en todos los casos, de suministrar información por cualquier persona y en cualquier circunstancia, lo que, por otra parte, tendrá un distinto alcance según se trate de particulares o de AAPP”*²⁹⁹. Aunque existiera un derecho fundamental reconocido, no significa que se aplique sin control, por la simple petición, sino que debe ser reconocido como tal. La realización del derecho de acceso dependerá del caso, estará a juicio de la situación por parte de quién gobierne las AAPP y, en última instancia, serán los Tribunales quienes lo reconocieran. Se diferencian dos ámbitos de exclusión por la norma constitucional: por una parte, la exclusión de acceso a información íntima, que puede ampliarse a la privada, compuesta por

²⁹⁷ Véase MAGDALENO ALEGRÍA, A., *Los límites de las libertades de expresión e información en el Estado Social y democrático de Derecho*, Madrid, 2006.

²⁹⁸ Del CASTILLO VÁZQUEZ lo referencia en la página 135. Auto del Tribunal Supremo, Sala de lo Penal, Sección 1ª, 821/2006, de 26 de septiembre (RJ 2006, 6440)

²⁹⁹ En la Teoría general de los DDFF, el derecho de acceso a la información tiene como límite la seguridad nacional.

facetas del individuo y su personalidad, donde el derecho a la protección de datos de carácter personal es totalmente relevante y por otra, la exclusión de acceso a la información pública que afecte a la seguridad nacional, la defensa del Estado y la averiguación de delitos.

5.2.1 Las materias clasificadas.

Las leyes de protección de datos y las leyes que bloquean el acceso a los datos que se consideran materias clasificadas son totalmente divergentes y dan prioridad al bloqueo de acceso en cuestiones de seguridad nacional y afines, las llamadas materias clasificadas. Este hecho se puede considerar un límite al derecho fundamental a la protección de datos y a otros DDFF. Todos los derechos reconocidos a un titular de datos personales por la LOPD quedan sin efecto, no necesitándose el consentimiento del afectado para la inclusión de sus datos en ficheros, ni tan siquiera es necesaria la creación de un fichero, el titular no tiene porqué conocer la inclusión de sus datos en sistemas de almacenamiento, ni que están siendo tratados, ni por quién, ni si son cedidos a terceros. El titular de los datos no puede ejercer de ningún modo su derecho de acceso, rectificación, cancelación u oposición. El escenario se convierte rápidamente en un pensamiento que va en contra de los derechos constitucionalmente reconocidos. Esta posibilidad es real y ha sido practicada en la historia del siglo XX³⁰⁰.

³⁰⁰ Véase DEL CASTILLO VÁZQUEZ, obra citada, página 140, nota 18. El régimen nazi disponía de bases de datos que funcionaban con tarjetas perforadas y que hicieron posible la efectiva persecución de elementos considerados por ese Estado como eliminables: judíos, gitanos, discapacitados, opositores, clérigos, homosexuales, etc. Bastaba la simple presunción, para que se encontraran ante la vulneración de sus derechos. En la actualidad, “los órganos automatizados del Estado podrían tener una imagen casi perfecta de cada uno de nosotros, de cómo vivimos, e incluso de lo que pensamos, si acaso consideran que es conveniente conocer esos datos para la seguridad y defensa del Estado. Técnicamente, una posibilidad así deja a los ciudadanos en el desamparo de una sociedad tecnológica avanzada, en donde el posible conocimiento de su esfera personal por parte de los órganos automatizados del Estado podría llegar a alterar gravemente el libre desarrollo de la personalidad del individuo, por cuanto pudiera verse bajo la mirada atenta de un tercero que ejerce su poder desde la información de los más mínimos e insignificantes detalles de su vida. Máxime cuando el legislador pudiera caer en la tentación

Actualmente, se debe tener por cierto que en muchos lugares de nuestro planeta ese tipo de estado existe realmente, no ha pasado en otras épocas. Es más, muchos estados denominados democráticos ejercen control sobre las informaciones y datos de sus ciudadanos y sobre extranjeros bajo el paraguas ambiguo de la seguridad nacional, almacenando todo tipo de información, con relevancia o sin ella, íntimos o no. Se recuerda los últimos escándalos del llamado espionaje a través de las redes sociales y las comunicaciones³⁰¹; como más relevante se encuentra el caso *Snowden*³⁰². Al margen de la consideración y valoración de los hechos que el Sr. Snowden llevó a cabo, existe realmente la presente situación. ¿Existe una vulneración de derechos funda-

de proteger su actividad a la hora de fijar las materias que deban ser sustraídas del conocimiento general.”

³⁰¹ Algunas notas de prensa: “EEUU espía a través de los servidores de *Apple*, *Google* o *Facebook*” http://www.elmundo.es/america/2013/06/07/estados_unidos/1370577062.html; “Los espías alemanes quieren controlar las redes sociales como sus colegas de la NSA” <http://www.elmundo.es/tecnologia/2014/05/31/5389856822601dcb668b456b.html>; “El rechazo del Senado aboca el espionaje de la NSA a un limbo legal” http://internacional.elpais.com/internacional/2015/05/22/actualidad/1432311804_288862.html; a 25 de septiembre de 2015.

³⁰² Edward Joseph Snowden era un empleado de la CIA y de la NSA de EEUU. Como formación era consultor tecnológico. Se podría afirmar que saltó a la fama mundial porque en junio de 2013 hizo públicos en los periódicos *The Guardian* y *The Washington Post* documentos clasificados como secretos y la existencia de programas de inteligencia y vigilancia masiva, por ejemplo, los llamados PRISM y XKeyscore. PRISM supuestamente puede recopilar datos de carácter personal como mails, videos, chats, voz, fotos, direcciones IP, transferencia de archivos, perfiles en redes sociales, y “cruzarlos”. Este término se emplea en informática para denominar los datos coincidentes y no coincidentes entre bases de datos. XKeyscore supuestamente intercepta mails y recopila datos como IP, teléfonos, nombres y palabras “clave” o “llave” que permiten al sistema identificar personas a través de datos. Son los llamados sistemas de “metadatos”: datos que describen otros datos y permiten su orden e indexación. Estos datos, de forma aislada no son relevantes, pero unidos generan una información de un valor importantísimo a varios niveles, no sólo para el Estado y la seguridad nacional.

mentales por los Estados? Como el Sr. Snowden manifiesta en junio de 2015 se puede pensar que *un derecho no vale por lo que esconde, sino por lo que protege*³⁰³.

La STS 921/2006, de 26 de septiembre, se prestaría para argumentar y referenciar la cuestión sobre los límites que se deben observar por parte del legislador y del gobierno a la excepción de control constitucional para los datos de carácter personal que se encuentren en los llamados asuntos de Estado o de material clasificado. El texto de la Sentencia es el siguiente: *“La existencia de una finalidad legítima, cuya satisfacción a todos beneficia, incluido el propio sistema democrático, no puede suponer la creación de espacios de impunidad para quienes contribuyen a alcanzarla, cuando en la utilización de esos medios o con abuso de los mismos, rebasen las fronteras de lo constitucionalmente admisible adentrándose en actuaciones de carácter delictivo. Tal situación de impunidad supondría en realidad la negación misma de todo aquello que justifica en un Estado democrático la existencia y actividad de esos servicios esenciales. El necesario equilibrio no puede alcanzarse negando un control real y eficaz de esa actividad, ni tampoco suprimiendo la exigencia de responsabilidades originadas por la eventual vulneración de los derechos más elementales del ciudadano”*.

La restricción de los DDFF no puede afectar a su contenido esencial. La defensa nacional no puede desarrollarse mediante la violación de los DDFF. Vulnerando los DDFF se quebraría el Estado de Derecho³⁰⁴. Esta excepción de la LOPD sobre materias clasificadas no puede suponer un espacio de impunidad para el almacenamiento indiscriminado de datos personales. Pero, ¿Lo es? ¿Tenemos conocimiento de la existencia de esas bases de datos? Lógicamente que si es secreto y roza la ilicitud ningún gobierno

³⁰³ SNOWDEN, EDWARD;., "La sociedad abierta avanza"]. http://elpais.com/elpais/2015/06/04/opinion/1433436340_438817.html a 25 de septiembre de 2015.

³⁰⁴ Véase a este respecto una obra muy clarificadora respecto a los límites de los DDFF y su contenido esencial ABA CATOIRA, A., *La limitación de los Derechos en la Jurisprudencia del Tribunal Constitucional español*, Valencia, 1999, pág. 193 y ss. Se citan la STC 159/1986, de 12 de diciembre, FJ 6; STC 254/1988, de 21 de diciembre, FJ 3; Véase también un pequeño trabajo sobre esta temática de MORENO MUÑOZ, M., "La tensión entre privacidad y seguridad en el desarrollo de internet", *Dilemata*, nº 15, 2014, pág. 181-193.

lo va a admitir, pues la ciudadanía tiene en los últimos años una acentuada conciencia sobre estos asuntos. Esa misma ciudadanía, que, en muchos casos, alimenta cada minuto las redes sociales con infinidad de datos personales. ¿Puede ser que el individuo pondere más la comunicación (diversión, relevancia social, egolatría, conductas de moda) que la privacidad o la intimidad? En caso afirmativo, ¿Tiene ese ciudadano derecho a la protección de datos que él mismo no ejerce? ¿Es intromisión o espionaje –y por tanto conducta delictiva– almacenar datos que los ciudadanos han aportado libremente a *internet*? ¿Y cuando los datos no son aportados a las bases de datos *ocultas* por el titular sino por otros, bien entidades públicas, bien empresas, bien otros ciudadanos, se está ante la violación de su derecho a la protección de datos si se incorporan a sistemas de almacenamiento en instituciones de seguridad nacional sin su conocimiento?

Las AAPP poseen todos nuestros datos personales relevantes, como se ha comentado en este texto: el Censo de Población, la Seguridad Social, las Administraciones de Hacienda, los Registros Civiles, los Registros de la Propiedad, el Ministerio del Interior con datos de Documento Nacional de Identidad y Permiso de Conducción, como ejemplos más relevantes. En todos ellos hay datos personales e íntimos. El Estado no necesita de otros datos, los tiene todos; sin ellos, no podría ejercerse la función del Estado Social, Democrático y de Derecho. ¿Qué existe entonces en las redes sociales que llama tanto la atención de las autoridades públicas? Un *seguimiento de conducta social*, puede ser la respuesta.

En España, el Centro Nacional de Inteligencia (CNI) publicó en su web un pequeño resumen de lo que se considera *Protección de la información clasificada*³⁰⁵, a través de la Oficina Nacional de Seguridad (ONS) En el citado resumen, redactado con simplicidad, se puede leer lo que para este organismo gubernamental significa información clasificada: *es cualquier información o material que requiere protección contra su divulgación no autorizada y a la que se ha asignado, con las formalidades y requisitos*

305 CNI CENTRO NACIONAL DE INTELIGENCIA; [“Protección de la información clasificada”]. [cni.es http://www.cni.es/comun/recursos/descargas/Proteccion_de_la_Informacion_Clasificada.pdf](http://www.cni.es/comun/recursos/descargas/Proteccion_de_la_Informacion_Clasificada.pdf) a 27 de septiembre de 2015.

previstos en la legislación, una clasificación de seguridad. Las materias clasificadas se rigen por la ley 9/68, de 5 de abril (preconstitucional) que fue modificada por la ley 48/78 de 7 de octubre, de Secretos Oficiales (LSO). Una materia clasificada es aquella *cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado y que se califican en las categorías de secreto y reservado, en atención al grado de protección que requieren.* El mismo CNI publica en su web también el documento denominado “*Normas de la Autoridad Nacional para la protección de la información clasificada*”³⁰⁶. La voluntad de nuestro sistema de control gubernamental parece querer informar con claridad y transparencia sobre estos procedimientos, que por su naturaleza deben ser muy confidenciales, si está en juego la seguridad de los ciudadanos.³⁰⁷

La LSO disponía que *la declaración de materias clasificadas no afectará al Congreso de los Diputados ni al Senado, que tendrán siempre acceso a cuanta información reclamen, en la forma que determinan los respectivos Reglamentos y, en su caso, en sesiones secretas.* La Resolución de la Presidencia del congreso de los Diputados de 11 de mayo de 2004, sobre secretos oficiales estableció un límite más, sólo las Comisiones o Grupos que comprendan, al menos, la cuarta parte de los miembros del Congreso, recabarán información sobre materias clasificadas como secretas o reservadas. Si la información es secreta, sólo se proporcionará a un solo diputado de cada grupo parlamentario, designado por el pleno de la Cámara con una mayoría de tres quintos³⁰⁸.

306 CNI CENTRO NACIONAL DE INTELIGENCIA, “Normas para la protección de Información clasificada”]. https://www.cni.es/comun/recursos/descargas/Normas_de_la_Autoridad_Nacional_para_la_Proteccion_de_la_Informacion_Clasificada.pdf a 27 de septiembre de 2015.

Es muy clara la información que se aporta en la página del CNI. En el punto referente a controles, expone su sometimiento al control Político, al control parlamentario, al control judicial a través del CGPJ y al control económico.

³⁰⁷ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, “Memoria 2014”]. http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/Memoria_AEPD_2014.pdf

³⁰⁸ SANTAOLALLA LÓPEZ, F., *Derecho Parlamentario Español*, Madrid, 1990.

La AEPD, reaccionando a las noticias aparecidas en los últimos años en prensa, recogió en su Memoria 2014 una serie de actuaciones respecto a la actividad de los servicios de inteligencia de EEUU y de Europa (caso *Snowden*, comentado)³⁰⁹. Desde el año 2013, todas estas noticias suponían un asunto especial para la AEPD, que no terminó de resolver sobre la cuestión, pues se habló de un ámbito de aplicación excluido de la LOPD, como se está analizando. El grupo de trabajo europeo en materia de protección de datos personales (GT29) analizó la situación de *los programas de vigilancia secreta, masiva e indiscriminada* y concluye que *son incompatibles con nuestras leyes fundamentales y no pueden ser justificadas por razones de lucha contra el terrorismo o contra otras importantes amenazas a la seguridad nacional. Las restricciones a los derechos fundamentales sólo son aceptables si son estrictamente necesarias y proporcionadas en una sociedad democrática*³¹⁰. El GT29 recomendó a los gobiernos una mayor transparencia sobre cómo operan estos programas y sobre lo que las autoridades encargadas de su supervisión hacen y deciden; también más transparencia por parte de los responsables a los que se dirigen las peticiones de acceso; el reconocimiento de producir una necesidad de mayor sensibilización de los ciudadanos; el establecimiento de un sistema legal coherente para los servicios de inteligencia, que incluya disposiciones sobre protección de datos, asegurando una supervisión eficaz de la actividad de los servicios de inteligencia y generando mayores controles para garantizar que los responsables sujetos al derecho de protección de datos europeo cumplen con sus obligaciones.

Es una tarea difícil compatibilizar la tradicional forma de gobierno con los nuevos sistemas de información y la protección de los datos personales. Como se ha visto, los primeros que alimentan las redes sociales y todo tipo de actividades en *internet* son los propios usuarios. Se podría presuponer que, si el titular de los datos publica libre-

³⁰⁹ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Memoria 2014"]. http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/Memoria_AEPD_2014.pdf a 27 de septiembre de 2015. La Agencia no hace más que recoger la Teoría General de los DDFF más aceptada, con una posición muy poco definida.

³¹⁰ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Memoria 2014"]. Página 82-83.

mente información, esta pudiera ser tratada y almacenada indiscriminadamente por cualquiera, no sólo por los Servicios de Seguridad del Estado. Veremos que también las empresas almacenan todo tipo de información con la finalidad que siempre han tenido: la actividad empresarial y mercantil, lo que en otros estudios se denomina marketing. Por otro lado, a pesar de comprometerse los derechos fundamentales, el objetivo de esos sistemas de inteligencia es prevenir situaciones de peligro para los ciudadanos, y parece ser que no encontraron mejor forma, o más fácil. Lo tuvieron fácil, pues los usuarios no inocentes y con intenciones no legales se dedican a utilizar *internet* como si fuera algo anónimo y secreto, pero nada más lejos de la realidad. Que esas redes de delincuencia (no sólo terroristas o grupos opositores, también delincuencia común) se comuniquen por mails abiertas y gratuitas (Google, Yahoo, por ejemplo) y redes sociales tipo *Facebook*, hace cuestionarse su nivel intelectual. El ciudadano que está dentro del Estado Democrático y de Derecho, que trabaja cada día con sus intereses legítimos no ofrece una conducta a los Servicios de Seguridad del Estado que sea atractiva o que llame su atención, con sus mails profesionales o personales de un contenido realmente irrelevante para estos Servicios, con sus comentarios en *Facebook* o *Twitter*, con sus fotos de vacaciones o de fin de semana en fiestas o en viajes, con datos que además, como se ha reseñado, están ampliamente completados en las bases de datos Gubernamentales (familia, relaciones sindicales o políticas, situación laboral, salud) Eso no exime de que sea cierto lo que la AEPD y el GT29 reseñan: *no puede permitirse la vigilancia secreta, masiva e indiscriminada pero no de los datos personales, que los tienen, sino de la conducta, que es sumamente valiosa.*

El nuevo RGPD es una herramienta más hacia la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas. El titular debe tener el control de sus datos personales. Para cumplir con este objetivo, se quiere reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas. El RGPD nace con la vocación de unificar el nivel de protección en todos los Estados miembros, evitando diferencias que puedan dificultar la libre circulación de datos

personales dentro del espacio de la UE. El RGPD pretende proporcionar la suficiente seguridad jurídica y la misma transparencia a todos los operadores económicos, incluso para las PYMES, al igual que un mismo nivel de derechos y obligaciones exigibles, con la cooperación de las Autoridades de control de los países miembros. La mayor exclusión a la aplicación del RGPD se encuentra en las cuestiones relativas a la protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con actividades excluidas del ámbito de del Derecho de la Unión, entre las que destacan las actividades relativas a la Seguridad Nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión. Estas exclusiones suponen un reconocimiento de la Soberanía Nacional de los Estados miembros de la UE, un límite a la aplicación del derecho a la protección de datos. Sin embargo, existe una referencia del RGPD a la Directiva UE 2016/680 del Parlamento Europeo y del Consejo. En estos casos, los Estados miembros pueden encomendar a las autoridades competentes, como se define en la Directiva 2016/680, funciones que *no se lleven a cabo* necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de tal forma que el tratamiento de datos personales para estos otros fines, en la medida en que esté incluido en el ámbito del Derecho de la Unión, entra en el ámbito de aplicación del RGPD³¹¹.

5.2.2 El terrorismo y la delincuencia organizada.

El punto c) del artículo 2.2 LOPD estableció la exclusión del ámbito de aplicación de la LOPD a *los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en esos supuestos el responsable del*

³¹¹ Considerandos 2, 7, 13, 16 y 19 RGPD.

*fichero comunicará previamente la existencia del mismo, sus características y su finalidad a la Agencia de Protección de Datos*³¹².

El legislador marcó la diferencia entre el punto b) y el punto c) del artículo 2.2. LOPD. entre la información concerniente a Seguridad Nacional y la que se refiere a actividades terroristas y de crimen organizado. Mientras los que conciernen a Seguridad Nacional estaban excluidos del ámbito de aplicación de la LOPD, los ficheros que contuvieran datos relativos a investigaciones de terrorismo o crimen organizado, con otras formas graves de delincuencia, no lo estaban³¹³. Los segundos, como se puede leer en el texto legal, debían cumplir con las formalidades establecidas en la LOPD, y la AEPD debía ser informada de la existencia del fichero, su finalidad y sus características generales. Los ficheros que contengan información policial general referente a investigación de la delincuencia y la prevención de la seguridad ciudadana se encuentran dentro del ámbito de aplicación de la LOPD y se regulan en los artículos 22 y siguientes. con un régimen general especial.

La norma no definió qué se entiende por formas graves de delincuencia organizada. Si se acude al Derecho Internacional, el artículo 2 de la Convención de las Naciones Uni-

³¹² El Reglamento tiene idéntico texto en su artículo 4 c). La Directiva 95/46/CE del 95 realizó la misma exclusión.

³¹³ ZAMORA JIMÉNEZ, ÁNGEL JOSÉ; "Comentario al artículo 2.2 c) Ficheros establecidos para la investigación del terrorismo y formas graves de delincuencia organizada.", *Comentario a la Ley Orgánica de Protección de Datos de carácter personal*., Madrid, 2010, pág. 150-155. En esta línea de conexión entre el derecho fundamental a la protección de datos personales y el Derecho Penal se encuentran también los textos de ALEGRE ÁVILA, J., "Interceptación de comunicaciones electrónicas y rango normativo", *Protección de datos y proceso penal*, Madrid, 2011. En este texto el autor analizó la STS 52/2008, de 5 de febrero que resolvió un recurso interpuesto por la Asociación de Internautas contra el Real Decreto 424/2005, de 15 de abril, el cual desarrollaba el artículo 33 de la Ley 32/2003, de 3 de noviembre, General de Comunicaciones. Otro objetivo de la regulación en el Real Decreto era el establecimiento de los requisitos técnicos y operacionales para que los mandamientos o autorizaciones judiciales que se efectuaran según el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, junto con el control judicial previo del Centro Nacional de Inteligencia y en otras normas con rango también de Ley Orgánica, fueran atendidos adecuadamente por los operadores (léase empresas) de comunicaciones. El recurso fue desestimado.

das contra la Delincuencia Organizada Transnacional, de 15 de noviembre del 2000, establecieron que un grupo delictivo organizado era *un grupo estructurado de tres o más personas que existía durante cierto tiempo y que actuaba concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados conforme a la Convención con miras a obtener beneficio de orden material*. Así mismo, el Convenio citado definió como delito grave *la conducta que constituyese un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave y como grupo estructurado consideró que sería un grupo no formado fortuitamente para la comisión inmediata de un delito y en el que no necesariamente se hubiese asignado a sus miembros funciones formalmente definidas ni hubiese continuidad en la condición de miembro o existiese una estructura desarrollada*.

Estos fenómenos delictivos organizados no estuvieron delimitados de ningún modo, y mantienen a las Fuerzas de Seguridad del Estado en constante estado de alerta. Los grupos delictivos no se encuentran limitados territorialmente, forman redes, tienen componentes legales e ilegales, en forma de empresas o profesionales que les favorecen en sus formas delictivas. Se valen de la libre circulación de personas y capitales dentro del EEE para sus fines. Les favorecen las diferentes legislaciones en los Estados miembros y las lagunas legales. Un ejemplo es lo que se ha denominado *ciberdelincuencia* que amenaza los derechos de las personas en lo que se conoce como *sociedad de la información*.

Ante el escenario delictivo, existe en la UE el *principio de disponibilidad de información*, por el cual se ejercería un intercambio transfronterizo de datos policiales entre los Estados miembros, para la prevención y lucha contra el terrorismo. Este acceso a la información puede llegar a ser directo, de una base de datos de un Estado miembro a otro (en línea). El *Convenio de Prüm*, de 27 de mayo 2005, de cooperación transfronteriza, en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal fue uno de esos instrumentos comunitarios³¹⁴. Este tipo de inter-

³¹⁴ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. , "Tratado de Prüm"]. https://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/Tratado-de-Prum.pdf a 27 de septiembre de 2015. Véase también COMISIÓN EUROPEA, ., "Comunicación de la

cambios pondría en peligro evidente la protección de datos de carácter personal. La ponderación como principio debe poner límites y garantías para que los Estados cumplan los principios de la protección de datos frente a las amenazas delictivas. En este momento, la sociedad europea ha pactado el intercambio de bases de datos personales para luchar contra el terrorismo, que en el año 2016 se manifestó con dureza en el continente, con varios atentados muy mediatizados. España sufrió durante años el acoso del terrorismo de ETA, pero no fue internacionalizado como sí lo está siendo el terrorismo de carácter *islamista*. Los ministros del Interior acordaron con fecha 22 de abril de 2016 la creación de una base de datos conectada con toda la información sobre vuelos, documentos de identidad robados, demandantes de asilo, visados de diverso carácter, entre otros. El dilema que enfrentó a los europeos era una disyuntiva entre seguridad y libertad. Los gobiernos que vivieron momentos de terror y muerte de nacionales reaccionaron con limitaciones de la libertad individual, pero después, los Tribunales o los Parlamentos de los Estados miembros de la UE restringieron o anularon esas medidas limitativas, que no tuvieron en cuenta, entre otros derechos, el derecho a la protección de datos.³¹⁵ Los Estados deberían ser conscientes de que vul-

Comisión al Consejo y al Parlamento Europeo. Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia.", *Comunicados y estudios de la UE.*, nº COM(2010)385, 2010.

³¹⁵ La anulación de la Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas por la Sentencia del TJUE C-293/12, de 8 de abril de 2014, es un ejemplo del proceder a favor de las libertades por parte de los Tribunales Europeos. El fundamento de la nulidad fueron los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea: "Toda persona tiene derecho al respeto a su vida privada y familiar, de su domicilio y de sus comunicaciones" (Artículo 7) y "Toda persona tiene el derecho a la protección de datos personales que le conciernan". Véase también VILASAU SOLANA, M., "La Directiva 2006/24/CE sobre conservación de datos del Tráfico en las comunicaciones electrónicas: seguridad vs. privacidad", *IDP Revista de Internet, Derecho y Política*, nº 3, 2006. Para las empresas de telecomunicaciones supuso inversiones muy importantes en equipamiento para poder almacenar datos y cumplir con la Directiva mencionada. El Director de la AEPD en ese momento, D. José Luis Rodríguez Álvarez, había advertido que las Autoridades Nacionales de Protección de datos no estaban totalmente de acuerdo con la norma. Perder los derechos fundamentales no facilita la previsión de crímenes, solamente resultan dañados los valores que se quieren defender. La tensión entre una visión y otra de la realidad jurídica permanece en este momento. Recientemente, el TC de Alemania ha considerado que la norma de vigilancia a sospechosos de terrorismo en el dormitorio

neran este derecho fundamental creando gigantescas bases de datos personales con accesos por cualquier otro gobierno que no es el de los nacionales titulares de los datos que se aportaran a la base de datos europea. Este cambio del ámbito de aplicación de la protección de datos, hace que la actual normativa tenga, si cabe, aún más problemas de aplicación y de eficacia. El RGPD exime también estas actividades de su regulación, como se ha mencionado. Cabe preguntarse por la compatibilidad de las medidas con los DDFF y su proporcionalidad en los medios empleados.

5.2.3 La Directiva 2016/680, relativa a la protección de las personas físicas en relación al tratamiento de datos personales para prevención de infracciones penales.

En la misma fecha de publicación del nuevo RGPD, se publicó también la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluso para la protección y la prevención de amenazas contra la seguridad pública, e igualmente regulando la libre circulación de dichos datos³¹⁶. La aludida Directiva regula la protección de las personas físicas respecto al tratamiento de datos personales por las autoridades competentes de los Estados miembros de la UE. Se consideran autoridades públicas los órganos judiciales, la policía y los cuerpos y fuerzas de seguridad de cada Estado Miembro y otros organismos o entidades que el Derecho de cada Estado miembros considere con competencias públicas en estas materias mencionadas. También resultan afectados los datos personales compartidos con *Interpol* (organismo internacional que recibe, almacena y distribuye datos personales para prevenir

o en el baño de su casa viola los derechos a la privacidad. Francia no ha podido aprobar una ley para retirar la nacionalidad a los terroristas con doble pasaporte, la Asamblea Nacional no lo ha permitido.

³¹⁶ Por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

y combatir la delincuencia internacional) reforzando el intercambio de datos personales sin mermar la garantía de respeto a los derechos y libertades fundamentales en referencia al tratamiento de los mismos. El tratamiento de datos debe ser lícito, es decir, necesario para desempeñar una función de interés público desarrollada por una autoridad competente según el Derecho de los Estados miembros y con los fines ya mencionados en este punto. Se establece una categoría de datos especialmente protegidos, como son los datos relativos a la raza, ideología, religión, creencias, afiliación sindical, datos de salud, datos de tendencia o vida sexual, junto con los muy especiales datos genéticos y biométricos que permiten la plena identificación de una persona física. La Directiva 2016/680 tiene como finalidad prioritaria la garantía a la adecuada protección de los datos de los investigados, las víctimas y los testigos por la presunta comisión de delitos, además de coordinar la cooperación entre Estados Miembros y la Interpol con la policía y los fiscales para realizar una labor eficaz contra el crimen y el terrorismo en toda Europa junto con países afines, como pueden ser EEUU³¹⁷. El 6 de mayo de 2018 debe aplicarse su normativa en los Estados miembros, por lo que estos deberán antes de esa fecha tener adoptadas y publicadas las disposiciones legales, reglamentarias y administrativas que consideren adecuadas para dar cumplimiento a lo establecido en la Directiva. La Directiva resultará de aplicación directa después de dicho plazo. Por una parte, esta nueva Directiva se puede considerar como un avance en la integración de los Estados miembros dentro de la UE. Por otro, al querer armonizar los diferentes enfoques nacionales dependientes de las Autoridades competentes en materia de seguridad nacional, el resultado es incierto. Será todo un reto armonizar los diferentes sistemas de seguridad, para lo que legisladores y gobiernos deberán estar a la altura, con la normativa adecuada. Es, en cualquier caso, preferible, la creación de una regulación para las actividades policiales que son, en su mayoría, invasivas de la intimidad de las personas, que mantener un

³¹⁷ la Directiva se estructura en 65 artículos y 10 capítulos en los que se regulan las obligaciones de los responsables y encargados del tratamiento de los datos, los derechos de los interesados, las medidas de seguridad en el tratamiento o la creación, por parte de cada Estado Miembro, de una Autoridad Independiente de Control junto con los derechos de los titulares de datos personales.

espacio desregularizado, en el que podría alegarse constantemente el interés y la seguridad nacional para sostener acciones vulneradoras de los DDFF.

5.3. Otras exclusiones.

El artículo 3.2 LOPD fue una norma denominada *supletoria* de las regulaciones específicas en los supuestos señalados, que se enumeran pero no se entra en su análisis detallado, como son los ficheros regulados por la legislación de régimen electoral; los ficheros que sirvan a fines exclusivamente estadísticos y están amparados por la legislación estatal o autonómica sobre la función estadística pública; los ficheros que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas; los ficheros que derivan del Registro Civil y del Registro Central de penados y rebeldes y los importantísimos ficheros procedentes de imágenes y sonidos obtenidos mediante la utilización de video cámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia. Todos estos contenidos tienen un fuerte componente de competencias del Estado y de la Administración Pública, por ello tienen una legislación específica. En cualquier caso, la AEPD conoció en muchos asuntos sobre las situaciones específicas excluidas. especialmente en cuanto a videograbaciones, debido a su amplia extensión en estos últimos años. Se realizará un análisis pormenorizado sobre la videovigilancia privada en un epígrafe específico.

6. Las Definiciones y conceptos aclaratorios en la LOPD y en el RGPD. Controversia entre teoría y práctica.

Uno de los puntos deficitarios de la normativa sobre protección de datos personales es el carácter ambiguo de las definiciones en los conceptos y en los denominados principios que la Directiva 95/46/CE y la LOPD mantuvieron. Tanto el concepto de *estable-*

cimiento, como se analizó anteriormente, como otros relevantes, por ejemplo, la definición de *dato personal*, adolecen de unanimidad doctrinal y jurisprudencial. Si se mantiene la actual definición de dato personal centrada en la indentificabilidad del titular, se considerará dato personal todo tipo de información referente a la persona, pues con los avances de la técnica y de las comunicaciones los perfiles de las personas se podrían identificar en la red sin mayores esfuerzos. El Tratado de Lisboa consideró el derecho a la protección de datos personales como derecho fundamental para toda la UE, pero no existía hasta el nuevo RGPD una norma unificadora de las definiciones para dotar al sistema europeo de la necesaria coherencia. Las empresas se enfrentaron a una serie de cargas burocráticas multiplicadas por tantos Estados miembros como formaban la UE, unido a una inflexibilidad normativa derivada del carácter administrativo que en España tuvo la norma, que imposibilitaban la creación de nuevos conceptos necesarios para regular la realidad en los nuevos procesos de tratamiento de datos (ya mencionados, *cloud*, *big data*, *internet de las cosas*). No existió una fuerza innovadora para acceder a la autorregulación, no se implementó la seguridad desde el diseño y la transparencia no se manifestó en las relaciones entre ciudadanos y empresas, aunque estas medidas hubieran supuesto una importante disminución de los tiempos y costes en la gestión empresarial. Tampoco las AAPP potenciaron ninguna de estas nuevas ideas que en otros países sí se desarrollaron. En especial se mostró muy débil la iniciativa y capacidad de las Autoridades de control de los diferentes Estados miembros de la UE. Aún con estas premisas, se procede a analizar las (hasta ahora vigentes) definiciones y conceptos de la LOPD³¹⁸.

6.1. Definición de dato personal.

³¹⁸ ARENAS RAMIRO, M., "Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades", *Hacia un nuevo derecho europeo de protección de datos*, Valencia, 2015, pág. 316-312. En una línea más crítica véase LÓPEZ AGUILAR, J., "Data protection package y parlamento europeo", *Hacia un nuevo derecho europeo de protección de datos*, Valencia, 2015, pág. 67-71.

La definición del artículo 3 a) de lo que la LOPD consideró dato personal es sumamente importante. No sólo para saber qué es para la ley dato personal, sino también en cuanto al ámbito de aplicación. Se toma como referencia el Informe 4/2007, *Sobre el concepto de dato personal del Grupo Europeo de Autoridades de Protección de datos*, (se recuerda, GT29) que consideró *alcanzar una definición común del concepto de datos personales sería equivalente a definir lo que entraría o quedaría fuera del ámbito de aplicación de las normas de protección de datos*³¹⁹. Por ello se planteó como objetivo *alcanzar un acuerdo sobre el concepto de datos personales, los casos en que debe aplicarse la legislación nacional sobre protección de datos y la manera en que está debe aplicarse*. El Informe 2007 tomó la definición de la Directiva 95/46/CE, en su artículo 2.1, por la cual *dato personal fue considerada toda información sobre una persona física identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*.

La LOPD definió en el artículo 3 a) dato personal como *cualquier información concierne a personas físicas identificadas o identificables*. El Reglamento del 2007, artículo 5.1 o), amplió la definición y consideró *identificable* a toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

El GT29 analizó punto por punto este concepto y, además, aportó ejemplos de sus exposiciones, dedicando especial atención a la definición de lo que se consideró más relevante. Para el GT29 la expresión *toda Información* de una persona física significó incluir en el concepto de dato personal tanto la información objetiva como la subjeti-

³¹⁹ COMISIÓN EUROPEA, "Informe de Grupo de Trabajo WP29 4/2007 sobre el concepto de datos personales.[". De 20 de junio de 2007. Página 3 del texto. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf a 29 de septiembre de 2015.

va sobre una persona, cualquiera que sea su amplitud, y con independencia del soporte técnico que la contenga³²⁰. Añadir la preposición *sobre* fue para el GT29 crucial para determinar el alcance sustantivo del concepto de dato personal, en relación con objetos y tecnologías. Un dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esta información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa, afirmó el GT29 en sus conclusiones³²¹. El concepto de *persona física* tendría un significado de *ser humano vivo*, aunque el Dictamen se ocupó también de los datos de personas fallecidas, el *nasciturus* y las personas jurídicas. Como contenido de la expresión *Identificada o identificable* consideró el GT29 el tratamiento de datos personales que determinen a un titular entre otros y los medios que se pueden utilizar para su identificación. Por ello se puso especial interés en los medios de anonimización y de cifrado de datos personales³²². Para establecer más aclaraciones a los conceptos tratados se definió como *persona identificada* a un ciudadano del que se conoce un grupo o conjunto de rasgos diferenciales (datos personales) de los demás ciudadanos, que le hacen único, por lo que se le puede identificar, individualizar. En primer lugar, dato personal es el nombre y apariencia física, junto con otro conjunto de datos más o menos amplio, físicos y no físicos, como son su psicología, su cultura, su situación social o económica, su trabajo. La definición de *persona identificable* significa que se trata de una persona que no se conoce pero que se puede individualizar de otros, puede ser identificado si se realizan suficientes actividades, no desproporcionadas, para su identificación. En ese caso, los datos personales no están vinculados de forma directa y clara,

³²⁰ Informe citado, pág. 28, donde se resumen todos estos puntos de análisis.

³²¹ Informe citado, pág. 10-11.

³²² ROMEO CASABONA, C., "Persona identificada o identificable, el afectado o interesado y el procedimiento de disociación en la protección de datos de carácter personal. Comentario al artículo 3.", *Comentario a la Ley de Protección de Datos de Carácter Personal.*, Madrid, 2010, pág. 226-256. Se recuerdan también las ideas previas mencionadas sobre las técnicas de tratamiento masivo de datos o *big data*. La AEPD utilizó estas consideraciones en diversas Resoluciones, siendo reciente la R/02189/2015, por esta razón se analizan, pues la práctica de la AEPD se remitía al Dictamen del GT29 mencionado, al argumentar qué se entiende por persona identificada o identificable.

pero la identificación sería posible al aplicar procedimientos de diversa índole, que suelen ser de carácter técnico-informático en caso de datos con soporte automatizado, como son las bases de datos; estos procedimientos deben ser sencillos en su aplicación para proceder a la identificación. Con los medios actuales, se puede llegar a la identificación de un ciudadano por elementos contextuales o circunstanciales, por medio de los procedimientos de asociación de datos o *cruce de datos* en el lenguaje tecnológico, a través del análisis masivo de datos (*big data*). Puede incluso, que la persona decidiera disociar sus datos personales para no ser identificada, pero que, a través de estos procedimientos de asociación mencionados, se llegue a la identificación³²³ El RGPD define en el artículo 4 el concepto de dato personal como *toda información sobre una persona física identificada o identificable* (el RGPD utiliza el término interesado); se considerará *persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.*

Se van a realizar algunas menciones en este punto, sin perjuicio de su matización dentro del análisis de este estudio. Para comenzar, se consideró por la AEPD como dato personal *el número de teléfono de personas físicas* cuando resulte adscrito al concreto titular del mismo o se asocie a datos identificativos adicionales como pueden ser la dirección y ésta se almacene con el número llamante³²⁴. La AEPD citó en el

³²³ Existen supuestos de informaciones que no se precisan por el GT29 (el cual incluye en su Informe 2007 muchos de lo más pintoresco) pero que pueden haber dado lugar a otros resultados jurídicos, como Resoluciones e informes de la AEPD o Sentencias de los Tribunales. Como referencia sobre la posibilidad técnica fundada de reidentificación GIL GONZÁLEZ, E., *Big Data, privacidad y protección de datos.*, Madrid, 2016, pág. 83 y ss. .

³²⁴ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Informe 285/2006 sobre número de teléfono y concepto de dato personal. "]. Página 1 del texto. http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2006-0285_N-uu-mero-de-tel-ee-fono-y-concepto-de-dato-personal.pdf a 29 de septiembre de 2015. Se apunta que la AEPD, en muchos de sus informes jurídicos no plasma el número de la sentencia a la

informe mencionado la SAN 1485/2002, de 8 de marzo, por la que se estableció que *para que exista dato de carácter personal es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados* (FJ 5). En otro informe de la AEPD sobre el número de teléfono, esta vez, número de teléfono móvil, se matizó que era necesario un grupo de datos personales para que la identificación a través de un número de teléfono sea posible³²⁵. En este caso la AEPD señaló que el número de teléfono móvil por sí mismo, sin el concurso de otros datos que contribuyan a identificar a su propietario, no tenía el carácter de dato personal; en consecuencia, la aplicación de las prescripciones contenidas en la LOPD vendría determinada por la asociación de dicho número con otros datos que permitan establecer la identidad de su titular³²⁶. La AEPD mencionó como referencia de su informe la SAN 3250/2008, de 17 de septiembre, por la cual la AN afirmó que *resulta necesario que los datos personales permitan la identificación de la persona física, no puede ser un dato personal el número aislado, sin otros datos de identificación*³²⁷. Otro dato considerado personal es el número

que se refiere. Se debe investigar en las diferentes Jurisprudencias de los Tribunales (TC, TS o AN) a cuál sentencia se refieren sus textos.

³²⁵ AEPD Informe 0575/2008
https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0575_Fichero-con-n-uu-meros-de-tel-ee-fono-m-oo-vil.pdf

³²⁶ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Informe Jurídico 0575/2008 Fichero con números de teléfono móvil."].
https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0575_Fichero-con-n-uu-meros-de-tel-ee-fono-m-oo-vil.pdf a 21 de septiembre de 2016

³²⁷ SAN 3250/2008, de 17 de septiembre de 2008, FJ 4 "el primer problema que se suscita en el presente caso es si el número de teléfono móvil puede incluirse en el concepto de *datos personales* que recoge el artículo 3.a) de la LOPD que identifica como tales "cualquier información concerniente a personas físicas identificadas o identificables". Es claro que un número telefónico asociado a un nombre y apellidos es un dato de carácter personal pues nos proporciona información sobre una persona identificada. Es más, el propio número de teléfono, sin aparecer directamente asociado a una persona, puede tener la consideración de dato personal si a través de él se puede identificar a su titular. En el presente caso la Agencia Española de Protección de Datos no ha razonado, y menos ha acreditado, que a través del número de teléfono móvil se haya identificado al titular del mismo o que a partir del citado número

del DNI. El dato del Número Nacional de Identidad, el cual no existe en todos los países y en algunos está prohibido por la propia Constitución, es un dato polémico, pues no existe uniformidad en los pronunciamientos de la AEPD. La Resolución E/00561/2004³²⁸ alegó que el criterio de la AEPD hasta ese momento no consideró dato personal al DNI por sí sólo, pero sí lo sería en cuanto resulte adscrito al concreto titular del mismo (página 3 del texto). Era un caso de denuncia a la AEPD de listados de la UNED en los que figuraban los DNI de los alumnos. La AEPD procedió a archivar la denuncia, pues consideró que en ese caso no se podía identificar a los alumnos que constan en los listados por su DNI, pero invitó a la UNED para que notificase a los interesados de otra manera más privada y confidencial, evitando listados. En otra dirección doctrinal, el informe 0334/2008 califica de dato personal al número del DNI para su tratamiento en una base de datos en la que sólo se incluya el DNI³²⁹. Alegando lo contenido en otras leyes, como el Real Decreto que regula la expedición del DNI, la AEPD concluyó que tales documentos tienen como finalidad la identificación de las personas y, por tanto, se somete su tratamiento a las normas de protección de datos. Este mismo concepto lo utilizó en diversas Resoluciones³³⁰. Actualmente mediante los sistemas de *big data* o procesamiento masivo de datos, el número de DNI permite una

fuese posible tal identificación, de forma que el citado número de teléfono ayuno de otras circunstancias que identifiquen o pudiesen permitir identificar al titular del mismo impide que pueda encajarse en la definición legal de dato de carácter personal.”

³²⁸ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Resolución E/00561/2004 DNI como dato personal"].

http://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2005/common/pdfs/E-00561-2004_Resolucion-de-fecha-20-04-2005_Art-ii-culo-11-LOPD.pdf a 29 de septiembre de 2015.

³²⁹ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Informe sobre DNI como dato personal 0334/2008"].

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2008-0334_La-creaci-oo-n-de-una-base-de-datos-en-la-que-s-oo-lo-aparezca-el-DNI-o-el-NIF-queda-sometida-a-toda-la-normativa-de-Protecci-oo-n-de-Datos.pdf a 29 de septiembre de 2015.

³³⁰ Otras resoluciones de la AEPD con referencia al Informe E/00561/2004: <http://www.agpd.es/portalwebAGPD/resultados-ides-idphp.php> a 29 de septiembre de 2015.

identificación muy acertada de los titulares de datos, además de conseguir, a través de sólo ese número, muchos otros datos relacionados con los ciudadanos. Es por esta razón, que el RGPD dedica una especial atención a los números de identificación personales, como el caso del DNI español. El RGPD considera que un número de identificación es un dato personal, sin matizaciones, en su artículo 4.1. Matiza aún más asignando una mayor importancia a este dato personal en el texto del artículo 87 RGPD, por el cual los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general y se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo a las normas de tratamiento que determina el RGPD.

Otros datos considerados de carácter personal son *las imágenes obtenidas por recursos tecnológicos para diversas finalidades*. La importancia del uso de la videovigilancia provocó que la AEPD dictará la Instrucción 1/2006 de 08 de noviembre de la AEPD. Esta Instrucción, en su Exposición de Motivos, estableció que las imágenes obtenidas por videovigilancia son un dato de carácter personal. La *Guía para la videovigilancia* publicada por AEPD consideró que su uso es *particularmente invasivo*, no sólo por las cámaras de videovigilancia, también por otros sistemas como videocámaras en general (todo teléfono móvil tiene, en este momento, un dispositivo que graba imágenes) o *webcam*³³¹.

En cuanto a *la dirección IP*, tanto los Tribunales como la AEPD consideraron la dirección IP como dato personal cuando permite la identificación de una persona. Técnicamente existe una diferencia entre las llamadas IP fijas o estáticas y las IP dinámicas. Casi todos los usuarios de *internet* tienen una IP dinámica, pues las IP llamadas estáticas tienen un coste aplicado por el proveedor de servicios de telecomunicaciones, no son para todos los usuarios. Una IP es un número de protocolo de identifica-

³³¹ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Guía para la videovigilancia"]. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf a 29 de septiembre de 2015. La problemática sobre grabación de imágenes y su incidencia en los DDFF se analizará en otro epígrafe, por su importancia

ción en *internet*, en castellano. Se le conoce por sus siglas en inglés: *Internal Protocol*. Se emplea para el envío y recepción de información mediante una red de comunicaciones. Una IP dinámica cambia constantemente al momento de cada conexión, por lo cual, localizar un dato de carácter personal con esa IP es muy difícil. Sólo los equipos técnicos encargados de la Seguridad Nacional o de similares características podrían seguir una IP dinámica. La IP fija o estática sí es identificable si se asocia a una persona, pero no es habitual que una persona física tenga este tipo de IP. Sólo se da en casos de empresas con determinada envergadura económica y de comunicaciones, no suele emplearse para particulares. Sobre la IP como dato personal, existen múltiples dictámenes e informes de la AEPD, el más conocido es el Informe 327/2003³³². Recientemente la STS 3896/2014, de 3 de octubre, reconoció que la IP es un dato personal en combinación con otros datos, tanto técnicos como de referencia a una persona física, por lo cual sería posible su identificación³³³. La doctrina anterior

³³² AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "IP como Dato Personal. Informe 327/2003"]. https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf

³³³ La página del CGPJ resume esta Sentencia del TS manifestando que: "El Tribunal Supremo ha rechazado la pretensión de la asociación Productores de Música de España (Promusicae) de recopilar sin consentimiento de los afectados los datos de los usuarios de redes P2P (peer to peer) -mediante las cuales se comparten archivos musicales- con el fin de ejercer la defensa de los derechos de propiedad intelectual de los productores y editores de fonogramas y videos musicales. El Alto Tribunal, que confirma la sentencia dictada en el caso por la Audiencia Nacional en septiembre de 2011, establece que Promusicae no está eximida del deber de informar a los usuarios de redes P2P sobre el tratamiento de sus datos que establece la Ley Orgánica de Protección de Datos." La asociación de productores reclamaba, entre otros datos, poder tratar las direcciones IP (Internal Protocols) sin informar a los afectados, al considerar que con ese dato era incapaz de llegar a conocer la identidad del usuario. El Supremo, en una sentencia de la que ha sido ponente el magistrado José María del Riego, señala que "las direcciones IP son datos personales", ya que contienen información concerniente a personas físicas "identificadas o identificables". Para rechazar otro de los argumentos de Promusicae, el TS destaca que "no puede equipararse el conocimiento por el titular de que su dirección IP es visible en las redes P2P, con su consentimiento para su tratamiento automatizado junto con otros datos de su tráfico". La Sentencia no comparte tampoco la alegación de los productores de que para poder concretar las conductas ilícitas de los usuarios de redes P2P no tenían más remedio que tratar las direcciones IP. El Supremo

no estuvo en esta línea reciente, pues la pregunta es obvia: ¿Cómo puede saber con certeza el responsable de un fichero de datos personales que la IP registrada es la de un terminado titular, usuario de servicios en internet?³³⁴

6.2. Definición de Fichero.

El punto b) del artículo 3 de la LOPD definió qué es un *fichero* para la ley española³³⁵. Fichero, término utilizado por nuestra lengua para determinar otros objetos, tiene un significado en protección de datos que difiere de la definición del Diccionario de la RAE y de otras definiciones técnicas tanto de telecomunicaciones como de informática. La mayoría de usuarios no sabe diferenciar qué entiende la LOPD por *fi-*

indica que el recurrente no ha justificado de forma suficiente esa necesidad por inexistencia de medidas protectoras alternativas en el ordenamiento jurídico, bien en el orden civil, en particular en la Ley de Propiedad Intelectual, bien en el orden penal, que fuesen más respetuosas con el derecho a la protección de los datos personales. La sentencia estima que, en este caso, por sus características de extensión y falta de acreditación de su estricta necesidad para la finalidad legítima perseguida, no está justificado limitar el contenido esencial del derecho fundamental a la protección de datos de un número desconocido de personas.”

³³⁴ GUERRERO PICÓ, M., *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Navarra, 2006, pág. 423. La autora añade que no es siempre forzoso que abonado y usuario sean la misma persona, tanto para equipos privados o familiares como de empresas o profesionales, equipos de espacios públicos, como centros sociales, bibliotecas, universidades o asociaciones.

³³⁵ DAVARA RODRÍGUEZ, M., "El concepto de fichero en la normativa sobre protección de datos. Comentario al artículo 3", *Comentario a la Ley de Protección de Datos de Carácter Personal*, Madrid, 2010, pág. 213-226. El profesor DAVARA tiene multitud de publicaciones sobre protección de datos y el llamado derecho Informático o de las Tecnologías de la Información. Como un comentario anecdótico, se añade que hubo momentos de actividad profesional en que los usuarios de datos personales, los responsables y trabajadores de las empresas clientes, no *acertaban* al intentar entender eso de *fichero*, que para unos era el *archivador* de papeles, para otros era el *archivo* informático, para otros era un mueble para guardar cosas, entre otros posibles ejemplos de la experiencia en la realidad. Forma parte de nuestra experiencia recordar que un cliente (pequeña asesoría de empresa) había dado de alta en la AEPD cerca de 30 ficheros, es decir, todos sus programas informáticos de gestión, porque fue eso lo que entendía por fichero. Otro caso curioso fue una empresa que pensaba que un fichero era toda su actividad de hostelería y que sería *seguida* por el Gobierno de la Nación en su gestión.

chero. Se distingue entre tres tipos de definiciones a la voz fichero: fichero lógico, fichero físico y fichero jurídico.

El fichero lógico es el producto de una organización interna del sistema de información correspondiente. Es el fichero informático incluido en un programa de software al que se accede en un equipo informático y en el que se pueden tratar los datos de carácter personal o datos de otro tipo. Este tipo de fichero no es el definido en la LOPD.

El fichero físico se considera el lugar material donde se encuentra la información, por tanto, un fichero automatizado estará ubicado en un sistema informático, y éste puede ser desde un ordenador personal, hasta diversos servidores. Si se trata de un fichero no automatizado, en papel, como libros, legajos, archivadores, serán estos el soporte físico del fichero. En este caso, pueden contener datos personales y también todo tipo de datos.

El fichero jurídico es un grupo de datos personales determinado para una finalidad específica. Puede segregarse del sistema principal y/o puede encontrarse en diferentes localizaciones automatizadas (informáticas) o no automatizadas, incluso, en diferentes ubicaciones físicas. Lo definitorio es que se tengan perfectamente localizados los datos personales, se tenga conocimiento y localización del tratamiento al que son sometidos para la finalidad del fichero o tratamiento. Se debe garantizar el cumplimiento de todos los principios de protección de datos y se debe permitir el ejercicio de todos los derechos al titular de los datos personales, cumpliendo la normativa sobre protección de datos³³⁶.

La AEPD en su Informe Jurídico 0279/2009 realizó una definición de fichero³³⁷ tanto en lo que la AEPD denomina soporte papel como (en soporte) automatizado, aplicable

³³⁶ DAVARA reconoce en sus conclusiones la dificultad de comprensión del concepto de fichero, es más, la enorme dificultad para determinar su organización. Es una enorme *capacidad interpretativa* e incluso *creatividad interpretativa*, en palabras del autor.

³³⁷ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. , "Concepto de Fichero. Informe Jurídico 0279/2009"].

http://www.agpd.es/portaIwebAGPD/canaIdocumentacion/informes_juridicos/naturaleza_pub_pri_fic

a toda su actividad. El informe comienza con el texto y definiciones legales. El artículo 3 b) define como fichero *todo conjunto organizado de datos de carácter personal, cualquier que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*. El artículo 5.1.k) y n) del Reglamento define fichero para los aspectos de la ley como *todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados cualquier que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso*; el apartado n) tiene el siguiente texto para definir los *ficheros no automatizados*: *todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativo a las personas físicas, que permita acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica*.

La AEPD se explicó con un ejemplo la consulta jurídica realizada. En primer lugar, los ficheros no automatizados, en soporte de papel, con la ordenación de los documentos por fecha en una carpeta, no constituye un fichero, al no estar éste estructurado conforme a criterios relativos a las personas físicas, y siempre que acceder a los datos personales incorporados en los documentos exija esfuerzos desproporcionados. Si, por el contrario, existía una correlación entre las fechas de los documentos y los sujetos a quienes se envían los mismos, lo que implica acceder sin esfuerzos desproporcionados a los datos personales, la carpeta constituía un fichero no automatizado de datos de carácter personal. En cuanto a los ficheros automatizados, la AEPD se remitió a la segunda pregunta de la consulta, sobre si los documentos incorporados a un soporte electrónico, sin ningún orden lógico, constituye un fichero según la LOPD. La AEPD destacó que *el archivo de documentos en un sistema informático lleva implícita una organización*, así, todo sistema informático permite hacer búsquedas de documentos, lo que en definitiva convierte a la carpeta (se supone que electrónica, de un PC o sistema informatizado) en la que se incorporen los documentos como fichero, dado que se cumple con los criterios de la definición, se permite el acceso a los documentos

[heros/common/pdfs/2009-0279_Constituci-oo-n-y-creaci-oo-n-de-ficheros-en-soporte-papel-y-automatizados.pdf](https://heros.common/pdfs/2009-0279_Constituci-oo-n-y-creaci-oo-n-de-ficheros-en-soporte-papel-y-automatizados.pdf)

con independencia de la forma o modalidad de su creación, organización, almacenamiento y acceso.

De estas dos respuestas se podría concluir que, si los datos personales están en un soporte no automatizado, de papel, pero su modo de organización no responde a estos datos personales sino a otro concepto, como puede ser la fecha de factura, por ejemplo, podría no ser un fichero según la LOPD y, por tanto, no era necesario inscribirlo como tal ante el Registro de ficheros que la AEPD tenía a disposición de los ciudadanos. En caso contrario, si los datos sin criterio de organización en datos personales se encuentran en soporte automatizado, en un sistema informático, aunque no esté organizada en función de datos personales, será un fichero, según la LOPD, porque puede buscarse la información personal de forma automática.

El RGPD establece la definición de fichero en el artículo 4.6 considerado así *todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica*.

En la práctica de inscripción de ficheros se incluían en prácticamente todos los casos el tratamiento automatizado y no automatizado de los datos contenidos en cualquier forma organizada de gestión de datos, siguiendo como criterio los grupos de datos y su finalidad diferente. Por ejemplo, en una empresa se generan grupos de datos similares en su tipología de clientes y proveedores, datos que son necesarios para gestionar la actividad comercial como finalidad. El fichero *clientes y proveedores* tiene como tipos de datos nombre, apellidos, DNI o CIF, dirección y número de teléfono. Junto con estos datos, se necesitaba para la actividad de la empresa el número de cuenta corriente de los clientes. Para otras empresas puede ser imprescindible el rostro o la huella dactilar de los clientes y proveedores, por diferentes razones, por ejemplo, seguridad. Además, se necesita para cumplir con las obligaciones frente a las AAPP información económica en cuanto a retenciones fiscales, por ejemplo. El fichero *clientes y proveedores* tenía un nivel de seguridad según los datos que gestione, pero era un fichero con independencia de su soporte, automatizado o no. Los grupos de datos y su finalidad era lo que determinaba su inscripción con un nivel u otro. La

AEPD dejó completamente claro que el tratamiento de datos de forma automatizada generaba la obligación de inscripción. No existe esa claridad normativa frente a los datos no automatizados, si bien se consideraba que también se debían inscribir siempre, sobre todo porque un dato automatizado se transforma con facilidad en no automatizado cuando se imprime un documento en papel, por ejemplo, y ocurriría a la inversa, un documento en papel o en otro soporte se transforma en dato automatizado a través de un escáner (digitalización) y almacenado en un sistema informático. Sólo hay que ver las mesas de trabajo de las empresas (no se habla de AAPP) para comprobarlo. Muchas veces el soporte de datos en papel es mucho más peligroso para la protección de datos personales que el sistema automatizado o *internet*, se olvida que un papel también *vuela*, se puede leer, fotografiar, fotocopiar, enviar y es medio de comunicación tan eficaz como otros.

6.3. Definición de fuente accesible al público.

En el punto j) del artículo 3 LOPD la ley definió como fuentes accesibles al público los tipos de listados o bases de datos denominados ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tenían consideración de fuentes de acceso público de forma exclusiva el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y Boletines Oficiales y los medios de comunicación. La anterior LORDAT no definió qué se consideraba por la Ley *fuentes de datos personales accesibles al público*. No generó un concepto de lista cerrada, sino una enumeración con carácter indicativo, más abierta a la interpretación y al uso de listados considerados públicos para fines mercantiles o intencionados. Es más, permitía el uso de estos datos sin consenti-

miento ni conocimiento por parte del titular. La LOPD también adoleció de buena sistemática, al encontrarse en una contradicción³³⁸. En un principio, consideró ficheros accesibles al público los que podían ser consultados por cualquier persona, que no estuvieran limitados por una norma y los que no tuvieran exigencias de ningún tipo, salvo, si procedía, el pago de una cuantía o contraprestación. A continuación, la norma realizó un listado cerrado, exclusivo y exhaustivo de lo que se considera fuentes de acceso público que lista en el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo, junto con los diarios oficiales, boletines oficiales y los medios de comunicación, lo cual podría interpretarse como una contradicción, que se aclaró por el Reglamento de 2007, cuando en el artículo 7 cambió el orden de exposición, invirtiendo la sistemática del artículo 3 j) LOPD con la lista taxativa de fuentes accesibles al público y concretó qué requisitos debían cumplir. Se redactó en un artículo lo que se entendería como fuente accesible al público, como son el censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre; las *Guías* de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica; las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional; los diarios y boletines oficiales y los medios de comunicación social. Las diferencias entre los datos personales públicos y los datos obtenidos de fuentes accesibles al público se pueden concretar a continuación en los siguientes epígrafes.

³³⁸ DE LA SERNA BILBAO, M., "Fuentes Accesibles al público. Comentario al artículo 3. ", *Comentario a la Ley de Protección de Datos de Carácter personal*, Madrid, 2010, pág. 256-295.

6.3.1 Los datos personales accesibles al público no por ello están exentos de protección.

En la STC 292/2000, de 30 de noviembre, el TC manifestó que el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. *Por consiguiente, también alcanza a aquellos datos personales públicos, que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos.* También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo. (FJ 6). Constituye esta doctrina la base de múltiples argumentaciones posteriores respecto a la accesibilidad de terceros en la normativa sobre datos personales. Es un marco referente para la actuación de las empresas y ciudadanos. Se convirtió en el punto de apoyo para los ciudadanos que desearan ejercer sus derechos de acceso, rectificación, oposición y cancelación. Se podría considerar un principio fundamental sobre el que se sustentan otros derechos fundamentales, en el que la mayoría de la doctrina jurídica se referencia. Sólo las fuentes accesibles al público enunciadas en el artículo 3 LOPD se pue-

den tratar como tal. Otras informaciones, como son una red social o una página web gratuitas, no constituirían fuentes accesibles al público³³⁹.

6.3.2 La accesibilidad general no es sinónimo de fuente accesible al público.

Las fuentes accesibles al público son las que la LOPD y su Reglamento reconocen. Las fuentes de datos accesibles al público en general, como pueden ser los Registros de la Propiedad y los Registros Mercantiles, tienen como función publicitar datos que son importantes para gestionar la vida jurídico-civil-mercantil. No necesitan el consentimiento del titular de los datos personales para acceder a ellos y a su información, pero sí es necesario un *interés legítimo y directo* que se debe acreditar y ser utilizados para la finalidad acreditada, no para otra. Se cita el Informe 184/06 de la AEPD, como ejemplo por el que se consideró que el uso de la información de un registro de vehículos por una persona anónima que los facilitó a otros no es un tratamiento de datos personales legítimo. También puede ser un ejemplo el uso de información sobre hipotecas inscritas en el Registro de la Propiedad para generar información personal de sus titulares. Estos usos vulneran la LOPD, por lo que serían objeto de sanción. Lógicamente, sería difícil establecer quién fue la persona (con acceso a los sistemas de tratamiento) que filtró y utilizó datos personales para fines de publicación de los mismos o para un tratamiento no legítimo; se considera que la protección en estos

³³⁹ Es la posición que se mantiene por GARRIGA DOMÍNGUEZ en sus obras. Sí podrían ser fuentes accesibles al público los periódicos en su edición digital, grupos de discusión, comunidades abiertas a los usuarios sin restricción. En este caso, según GUERRERO PICÓ sí se puede hablar de fuentes accesibles al público, no siendo el mismo caso la recopilación de datos personales destinados a una finalidad distinta de la que el titular dio su consentimiento, por ejemplo, recopilación de direcciones o mails de un portal de búsqueda de empleo, lo cual contraviene el consentimiento que prestó el titular de los datos para su tratamiento. En el mismo sentido, la publicación de sentencias condenatorias por internet, cuestión que fue solucionada, pero que muchos ciudadanos demandan, alegando un derecho a conocer a las personas que han cumplido condena para elegir sus relaciones. Una cuestión muy controvertida en cuanto a DDFF que se tratará junto con el denominado *derecho al olvido* o derecho de supresión de información personal.

casos y con el sistema actual, es sino imposible, sí muy difícil, al igual que la imposición de la sanción o la posibilidad de petición de una indemnización por daños.

Los datos obtenidos de una fuente accesible al público no necesitan para su tratamiento del consentimiento del titular de los datos, pero sólo se considera su tratamiento como legítimo y, por tanto, legal, cuando el interés para su uso, bien por un titular de un fichero, bien por una persona (física o jurídica) a la que se le proporcionen esos datos, sea el mismo que el interés por el que esas fuentes de datos son públicas. El principal asunto es discernir qué se entiende por interés legítimo. La respuesta se encuentra en las finalidades, que deben ser determinadas, explícitas y legítimas por parte del responsable del tratamiento. Los datos de fuentes accesibles al público no son datos de libre acceso, no son datos de libre tratamiento. Un punto importante a señalar es que los datos personales obtenidos de una fuente accesible al público se incorporan a un fichero; este nuevo fichero, donde se introducen los datos, ya no tiene el carácter de fuente accesible al público³⁴⁰. Es lo que se referencia en la Resolución 00862/2008 que sancionó a un banco español por haber utilizado los listados de un Colegio Oficial de Ingenieros para publicitar un producto financiero entre los colegiados³⁴¹. El nuevo fichero sobre el que se realiza el tratamiento de datos personales debe adecuarse completamente a la normativa sobre protección de datos, en especial sobre el consentimiento y finalidad de los datos que se introducen y tratan en él. El responsable del fichero debe acreditar que los datos provienen de una fuente accesible al público y que su interés para su tratamiento es legítimo. Si no es así, si no puede probar su procedencia, se considerará vulnerado el principio de consentimiento consagrado en la LOPD.

6.3.3 Las fuentes de datos personales accesibles al público.

³⁴⁰ DE LA SERNA BLIBAO, obra citada, página 270.

³⁴¹ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Resolución 00862/2006 Banco de Sabadell"]. http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2008/common/pdfs/PS-00002-2008_Resolucion-de-fecha-17-07-2008_Art-ii-culo-5.4-y-5.5-LOPD.pdf

En detalle, las fuentes de datos personales que la LOPD y su Reglamento considera de acceso público, tienen los siguientes comentarios:

A. El censo promocional.

Antes de la LOPD, la legislación sobre el uso de datos personales contenidos en el Censo Electoral era manifiestamente ilegítima. Sobre la base de su consideración como fuentes accesibles al público y sobre el RD 1332/1994 de 20 de junio, para el desarrollo de la Ley de 1992 (LORDAT). La AEPD zanjó todo el conflicto sobre la base del artículo 41.2 de la LO 5/1985 de 19 de junio, de Régimen Electoral General, por lo cual quedaba prohibida cualquier información particularizada sobre los datos personales contenidos en el Censo Electoral, a excepción de los que se solicitan por conducto judicial. Que el Censo esté expuesto públicamente no significa que su utilización pueda ser indiscriminada. Por ello, la LOPD habla de censos promocionales, evitando cualquier referencia al Censo Electoral. El censo promocional se reguló en el artículo 31 LOPD. Sólo el Instituto Nacional de Estadística (INE) podría elaborar censos promocionales; las CCAA pueden tener una figura similar de censo promocional, pero no pueden tener competencias sobre los datos personales contenidos en el censo de habitantes y ciudadanos españoles³⁴². Los ficheros generados por el INE (Instituto Nacional de Estadística) son de naturaleza pública, y será de aplicación la regulación de la Administración Pública competente. Los datos contenidos en el censo promocional

³⁴² Como interesante y reciente se aporta como referencia el procedimiento sancionador de la AEPD a las entidades ASSEMBLEA NACIONAL CATALANA y ÒMNIMUM, con Resolución R/02762/2015, y resultado una sanción muy importante de 240.000 euros a la Asamblea Nacional Catalana (ANC) y con otros 200.000 euros a Òmnium Cultural por la masiva encuesta realizada ante la consulta (considerada ilegal) convocada el 9 de noviembre de 2014. En total 440.000 euros de sanción cuyas razones se exponen en una de las Resoluciones más largas y fundadas que se han producido, 71 páginas. Entre otras razones y resumidamente, la AEPD argumenta que las entidades sancionadas no cumplieron con la normativa según la cual el titular ha de dar su consentimiento por escrito para el tratamiento de datos que revelan ideología, afiliación, religión o creencias. Los datos se habían obtenido por medio de los datos del Censo de población, pero eran tratados sin consentimiento de los titulares para esas finalidades y además se trataron datos especialmente protegidos por entidades que no formaban parte de las AAPP.

serán sólo el nombre, apellidos y domicilio que constan en el Censo Electoral. Si se desea la inclusión de otros datos, se deberá solicitar a los órganos encargados de la elaboración del censo promocional y contar con el consentimiento del titular de los datos. Los titulares de los datos personales pueden pedir su exclusión de cualquier elaboración de censo promocional. La finalidad del censo promocional debe ser el reparto de publicidad, documentos comerciales o actividad análoga; para su elaboración se puede solicitar el pago de una contraprestación económica. En el plazo de un año desde su emisión el fichero elaborado perderá su carácter de fuente accesible al público. Los encargados de la elaboración del censo promocional tienen que actualizarlo cada trimestre. Los titulares de los datos personales podrían ejercer sus derechos de exclusión en el plazo de 10 días para listados de consulta telemática y en las siguientes ediciones para listados en otro soporte. Los listados con fines promocionales no estuvieron exentos de controversia. En el año 2014 se promulgó la Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios junto con otras leyes complementarias. Por esta ley se derogó un conflictivo artículo de la anterior Ley de Comercio Minorista, el artículo 39. Pero ninguna ley en 16 años ha regulado este asunto de forma inequívoca. La Disposición Transitoria Segunda de la LOPD dictó que se desarrolle por la vía reglamentaria la cuestión de los censos promocionales, con fines de prospección comercial y publicitaria, tarea que todavía no se ha realizado. Se siguen únicamente las regulaciones en materia de protección de datos para estos asuntos.

B. Las listas de profesionales.

Estos listados solamente contienen los datos de una persona física por su pertenencia a un grupo profesional. Los datos son el nombre, apellidos, título, profesión, grado académico, dirección profesional y la indicación de porqué su pertenencia al grupo profesional en cuya lista se incluyen. Se puede incluir un dato telefónico profesional, fax y dirección de mail. Otros datos contemplados como de posible inclusión son el

número de colegiado, fecha de incorporación al grupo profesional y su situación dentro del colegio (alta o baja, ejerciente o no ejerciente, por ejemplo) Se encuentran en esta categoría no sólo las personas que pertenecen a Colegios Oficiales de las diferentes profesiones colegiadas, sino también las personas que no cuenten con colegiación, pero formen un grupo profesional. Se diferencian dos tipos de ficheros en esos listados. Por una parte, ficheros considerados como fuentes accesibles al público, cuya finalidad es cumplir con las actividades profesionales del grupo. Por otra parte, están los ficheros privados con finalidad de cumplimiento de otras funciones del grupo. Tienen dos regímenes jurídicos diferentes, por tanto, al tratarse de ficheros públicos o privados. La LOPD y el Reglamento en otros artículos realizó matizaciones a este tipo de ficheros. Algunas son las que incluyeron el artículo 6.4 LOPD y los artículos 34 y ss. del Reglamento, por los cuales se permitía la oposición del titular al tratamiento de sus datos siempre que existan razones fundadas (por ejemplo, a que sean públicos por razones de seguridad) y también el artículo 28.2 y 45 del Reglamento, por los que el titular podría oponerse a que sus datos fueran utilizados para fines publicitarios o de prospección comercial. Como puede apreciarse, la voluntad del titular de los datos tiene prioridad sobre cualquier finalidad, por lo que los datos no pueden utilizarse indiscriminadamente, aunque sean publicados por razones profesionales. Además, estos datos profesionales tendrían sólo esa finalidad, la profesional, no otras.

C. Los repertorios telefónicos y las *Guías* de servicios de comunicaciones electrónicas.

El artículo 3 j) LOPD consideró que los repertorios telefónicos serían fuentes accesibles al público; el artículo 7 del Reglamento lo reflejó así y se remitió a su normativa específica, la Ley 32/2003, de 3 de noviembre Ley General de Telecomunicaciones (LGT), desarrollada por Real Decreto 424/2005 de 15 de abril, de las condiciones para

la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (RSU).

El artículo 34 LGT se titula expresamente *Protección de los datos de carácter personal*. Por esta norma, las empresas que explotan redes públicas o servicios de comunicaciones electrónicas, tienen la obligación de garantizar la protección de datos personales de los usuarios, según la legislación vigente, pero además la propia LGT y el RSU también incluyeron normas en este sentido para protección de los usuarios y sus derechos en materia de protección de datos personales. En todos los casos, la entidad reguladora que conoce de reclamaciones en esta materia será la AEPD y se aplicará su régimen sancionador³⁴³. La actividad empresarial de las telecomunicaciones es uno de los pocos sectores económicos que tiene una regulación específica.

7. Los Principios (que son derechos y obligaciones en la práctica) de la Protección de Datos de Carácter Personal.

La LOPD en su Título II reflejó los principios generales de la protección de datos personales. Para la doctrina, los principios generales de protección de datos constituyeron el contenido esencial del derecho a la protección de datos personales. Por otro lado, los principios generales no regularon con exactitud las conductas, ni del responsable del fichero o tratamiento, el obligado a cumplir con la LOPD, ni de los titulares de datos³⁴⁴.

³⁴³ Véase MARTÍN RETORTILLO BAQUER, LORENZO; , "Comentario al artículo 35 LGT", *Comentarios a la Ley General de Comunicaciones; Ley 32/2003 de 3 de noviembre*, Madrid, 2004. . El tema de las listas denominadas *Robinson* o de exclusión comercial es de sumo interés, aunque no son una solución definitiva a los contactos comerciales no deseados. La AEPD tuvo estas situaciones protegidas, pero eso no evitó las molestias, pues muchas compañías no cumplen con el compromiso de exclusión, al actuar con llamadas o mails *aleatorios* o generados por un sistema de llamadas o de envíos de mensajes automatizados.

³⁴⁴ HERRÁN ORTIZ, A., *El derecho a la protección de datos personales en la sociedad de la información.*, Bilbao, 2003, pág. 53. La autora resumió su visión: "Los principios generales de protec-

Desde una perspectiva constitucional³⁴⁵, la LOPD debería haber dispuesto otra sistemática para aportar mayor claridad al derecho fundamental que desarrolló. Se apuntó como explicación a esta falta de rigor legislativo en 1999 la inexistencia de un referente en la propia CE del derecho a la protección de datos personales y la inexistencia de jurisprudencia y doctrina suficiente, lo cual, no era así en la realidad internacional, como se ha analizado en los epígrafes anteriores. De hecho, está claro que otros derechos fundamentales y libertades públicas se tratan de forma ordenada y definida. Los legisladores quizá no estuvieron bien asesorados y tenían prisa, pero doctrina y ejemplos prácticos existían. En cualquier caso, en este análisis se van a nombrar como los menciona la LOPD y el Reglamento, con la salvedad apuntada de que se trata de *obligaciones del responsable* del fichero o tratamiento y son *derechos del titular*

ción de datos constituyen el contenido esencial del derecho a la protección de datos, y configuran un sistema de tutela que garantiza una utilización racional y razonable de los datos personales. Por ello a través de la configuración de estos principios el legislador aspira a constituir un sistema preventivo de tutela de la persona frente al tratamiento de sus datos, estableciendo un saludable equilibrio entre los avances de la sociedad de la información y el respeto a la libertad de los ciudadanos” la práctica de la ley los llega a confundir por su aplicación.

³⁴⁵ DÍAZ REVORIO, FRANCISCO JAVIER; , "Comentario al artículo 5 LOPD. Derecho de la Información en la recogida de datos. Una perspectiva constitucional.", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.*, Madrid, 2010, pág. 433-451. “quizá hubiera sido preferible una mayor claridad y una técnica más depurada dese la perspectiva constitucional, en el sentido de especificar en un artículo previo los elementos del derecho fundamental a la protección de datos, que se irían desarrollando de forma sistemática y ordenada en los siguientes artículos. Acaso la misma cabecera del Título II podría referirse más propiamente a los elementos configurados del derecho de protección o disposición de los datos personales y comenzar con un artículo general que definiera el derecho y los elementos o facultades que comprende, antes de desgranar cada una de ellas. Abrir el Título con el artículo dedicado a la calidad de los datos implica un cierto “salto lógico” ya que, dado que el Título I contiene sólo disposiciones generales, y en las definiciones no se hace referencia al derecho de protección de datos, el legislador pasa a regular la calidad de los datos, la información y el consentimiento sin enunciar siquiera la relación de estos elementos con el derecho fundamental que se regula. En realidad, y como sugiere el título de la propia Ley, el legislador parece más preocupado por la regulación de los datos y su tratamiento y transferencia, que por el desarrollo de un derecho fundamental autónomo y sus elementos configuradores.” página 432 y siguientes.

de los datos, la AEPD y la jurisprudencia así lo confirma. Las sanciones a la falta de calidad en el tratamiento de datos personales, que se definieron en la LOPD como un principio, fue un resultado gravoso de su aplicación como derecho y obligación, por tanto, se trata de una norma con resultado de sanción. No es sólo un principio orientativo, es un derecho del titular de los datos personales que se nombra como principio en la nominación del Título II LOPD y que se regula en su artículo 4 extensamente como norma, con peor o mejor sistemática y es una obligación *de hacer*, que el titular puede exigir al responsable del fichero o tratamiento de sus datos personales³⁴⁶.

7.1. La calidad de los Datos.

Fue el primero de los principios que mencionó la LOPD en el artículo 4. Junto a éste, se mencionan el principio de finalidad definido por la legitimidad, la determinación y la explicitud, siendo máximo exponente de la calidad de datos. Los datos deben, a su vez, ser adecuados, no excesivos, exactos e íntegros. La STS 672/2014, de 19 de noviembre (FJ 4.6) consideró el principio de calidad y los principios que derivan de éste (pertinencia, actualidad, cancelación de datos innecesarios y recabación por medios lícitos) como básicos para el tratamiento automatizado de datos personales bajo la exigencia de adecuación, pertinencia y proporcionalidad a los fines para los que ha-

³⁴⁶ ALEXY, R., "Los derechos fundamentales y el principio de proporcionalidad", *Revista Española de Derecho Constitucional*, nº 91, 2011, pág. 11-29. Es la base de la teoría de los principios, esa distinción entre reglas (normas) y principios: "Las reglas son normas que exigen algo en forma definitiva. Ellas son, por lo tanto, mandatos definitivos. Su forma de aplicación es la subsunción. Si una regla es válida y las condiciones para su aplicación son satisfechas, entonces debe hacerse exactamente lo que ella exige, ni más ni menos. Si esto se cumple, entonces la regla ha sido satisfecha, si no se cumple lo que ella estipula, entonces la regla no ha sido satisfecha. Por el contrario, los principios son mandatos de optimización. Como tales, ellos exigen que algo sea realizado en la mayor medida posible, de acuerdo a las posibilidades fácticas y jurídicas existentes" El texto del artículo se remite a la obra del mismo autor, ALEXY, R., *Teoría de los derechos fundamentales (Theorie der Grundrechte, 1986)*, Madrid, 1993.

yan sido recabados y tratados. Este principio-norma no tiene serias diferencias con la nueva regulación europea, que se analiza en el epígrafe correspondiente.

7.1.1 La pertinencia del tratamiento.

Del texto legal destacó la cuestión de la pertinencia de los datos recabados. Se generó una fuerte relación entre la finalidad para la que se recopilan los datos y la legitimidad del tratamiento, condicionada por la adecuación³⁴⁷. Se prohibió en la LOPD cualquier tratamiento de datos que no sea necesario para la finalidad que se autoriza por el titular de los mismos, aunque éste preste consentimiento informado. Este punto es sumamente importante, porque la protección de los datos personales se sitúa por encima del consentimiento del afectado, el derecho fundamental es más relevante que la voluntad (o supuesta voluntad) del individuo. Las empresas encontraron en la información personal una fuente de datos importantísimos para su actividad, que les permitía labores de promoción más eficaces y proporcionar servicios, productos y precios que sean efectivos. ¿Es perjudicial para los DDFF de un ciudadano que sus datos se usen con esa finalidad? La Ley y el Reglamento entraron en ese punto en serias lagunas y controversias, entre los artículos 15, 51.2 y 16 LOPD, no definiendo con claridad qué actividades estaban o no limitadas. Se refirieron claramente a las actividades de telecomunicaciones, pero no quedó clara la finalidad, límite para el tratamiento de los datos de servicios continuados, como si se quisiera dar una especie de

³⁴⁷ APARICIO SALOM, JAVIER; , "Comentario al artículo 4. Principios de la LOPD. La Calidad de datos.", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, 2010, pág. 324-340. El autor propone un ejemplo clarificador: En una situación de prestación de servicios continuados, la empresa que presta estos servicios obtiene mucha información derivada del consumo que realiza el usuario. Esa información debe estar limitada a la actividad de liquidación, facturación y pago de servicios. Sin embargo, la información del usuario permite obtener datos sobre su comportamiento en compras y consumo, así como su perfil económico. En igual opinión GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 170 y ss. . En esta obra y en las anteriores que la autora ha publicado mantiene su opinión sobre los principios de la protección de datos.

salida en forma de laguna abierta a interpretación para el uso no informado de datos personales, con una finalidad obvia de carácter comercial. Esta laguna legal fue muy bien aprovechada por los nuevos avances tecnológicos, con máquinas tan efectivas de análisis y generación de perfiles a través de programas informáticos que se han denominado *inteligencia artificial*³⁴⁸. Los avances tecnológicos, como ya se ha apuntado, no tienen que ser negativos en sus resultados. Lo que se quiere prevenir es el abuso de derecho, no respetando ni los derechos a la protección de datos, ni otros tantos derechos, fundamentales o no.

La adecuación del tratamiento a la finalidad autorizada por el titular, se reguló en el artículo 4.2 de la LOPD y el artículo 8.2 y 3 del Reglamento. La finalidad que se permitió por el titular de los datos y que reguló a su vez la LOPD y su Reglamento, es la que respeta la actividad para la que ha sido permitido su tratamiento, no otra incompatible. Como actividad compatible la propia LOPD consideró que pueden ser actividades históricas, estadísticas o científicas (art. 4.2 final) que desarrolló el artículo 4.5 LOPD, el cual consideró excepcionales los casos de mantenimiento de datos para estas finalidades y se remitió a una regulación específica. El Reglamento, en su artículo 9.1. dejó una puerta abierta al mantenimiento de los datos para el cumplimiento de la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias. En el punto 2 del mismo artículo 9 del Reglamento se estableció otra vía de excepción por la cual la AEPD podría acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos.

7.1.2 El deber de actualización y rectificación.

³⁴⁸ La inteligencia artificial, se recuerda, se nutre del tratamiento masivo de datos o *big data*.

El deber de actualización y rectificación se reguló en los artículos 4.3, 4.4 de la LOPD y 8.5 del Reglamento. Son los artículos que más específicamente atendieron al principio de calidad de datos, que se realiza con su mantenimiento actualizado³⁴⁹. Se distinguió entre los tratamientos consentidos por el interesado y los no consentidos por el mismo, realizándose también una distinción entre los tratamientos impuestos por las AAPP o la Ley en general y los tratamientos consentidos por el titular. En el caso de tratamiento consentido por el titular, una parte de la doctrina consideró que la relación entre titular de los datos y responsable de su tratamiento es de tipo contractual, basándose en el artículo 1.256 del Código Civil (CC a partir de ahora) el cual establece que el cumplimiento de los contratos no puede quedar al arbitrio de una sola parte contratante. Ocurre entonces, que el responsable necesita los datos exactos de la otra(s) parte contratante, para cumplir con sus obligaciones. El interesado debe ser la parte contratante con más interés en que sus datos sean correctos. Ambas partes están obligadas a la actualización de los datos y a su mantenimiento correcto. Para esta visión del tratamiento de datos consentido por el titular, el deber de actualización se configuró como una obligación derivada del consentimiento para el tratamiento de los datos personales y de la buena fe contractual del artículo 1.258 CC. También consideró que, al ser *una parcela de libertad* (expresión muy acertada) a la que el titular de los datos renuncia para asumir el cumplimiento del contrato, el consentimiento otorgado para el tratamiento de sus datos debe ser interpretado de forma restrictiva. La falta de comunicación de las actualizaciones de datos personales que se produzcan, afectan a ambas partes, pero especialmente al responsable del fichero el cual no puede utilizar los datos personales para las finalidades que se expusieron en la recogida y que autorizó el titular³⁵⁰.

³⁴⁹ APARICIO SALOM, JAVIER; , "Comentario al artículo 4. Principios de la LOPD. La Calidad de datos.", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, 2010. TRONCOSO REIGADA, ANTONIO; , "Comentario artículo 4 LOPD El principio de Calidad de los datos", *Comentario a la Ley de Protección de Datos de Carácter Personal*, , 2010.

³⁵⁰ Obra citada de APARICIO SALOM, página 333. "no podrá servirse de los datos para los propósitos que pretendía y que convino con el interesado y, por ende, impedirá, asimismo, a este último la satisfacción del interés que manifestó al facilitar la información al responsable y autorizar el tratamiento."

En esta visión del principio de calidad de datos, que se puede calificar dentro de civilista más que de Derecho administrativo, se considera que el tratamiento no regula expresamente las consecuencias del incumplimiento de la obligación, por tanto, no existe responsabilidad contractual de ninguna de las partes, ni del interesado en el caso de que no comunique cambios o actualizaciones de sus datos personales, ni del responsable del tratamiento si no las realiza, salvo que la actualización resulte esencial para el cumplimiento de lo acordado en un contrato, como por ejemplo, los contratos bancarios o de seguros, en los cuales la obligación de comunicación de cambios en los datos personales es esencial para su cumplimiento. Por tanto, el titular de los datos, sería la parte obligada a informar de cualquier cambio en sus datos, pues es quien mejor los conoce en cada momento, mientras que el responsable del tratamiento no tiene porqué saber de estos cambios, y, por tanto, deberá, según esta interpretación de la norma, quedar exento de cualquier responsabilidad y culpabilidad si la prestación no se desarrolla conforme a lo pactado contractualmente. La obligación del responsable del fichero o tratamiento no puede incluir una investigación de los datos personales de un titular, sino que se puede entender en el límite de conocer los cambios en la información tratada cuando se tenga conocimiento de dichas modificaciones; por tanto, no supone un incumplimiento de la LOPD la constancia de algún dato inexacto en el tratamiento si el responsable no ha tenido noticia de dicha inexactitud. Sin embargo, según la LOPD, el responsable del tratamiento tendría *la obligación* de actualizar la información que tiene del titular de los datos personales, no es obligado el titular de los datos a proporcionar dicha actualización. El artículo 8.5 del Reglamento añadió, además, que si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por este. Es una presunción, siempre interpretable, que libera al responsable del tratamiento de la obligación de investigar y actualizar los datos del titular.

Si el tratamiento se basa en una imposición legal, la ley suele establecer la obligación de comunicar los cambios al titular de los datos personales, por lo que el responsable del tratamiento no tiene obligación de actualizarla por su iniciativa.

7.1.3 La cancelación de datos.

La cancelación de los datos innecesarios, como cumplimiento del principio de calidad, se consideró obligatoria según el artículo 4.5 LOPD y 8.6 del Reglamento, con la reseña por parte de este último artículo de que se autoriza al responsable del tratamiento el mantenimiento de los datos que sean necesarios para el cumplimiento de obligaciones legales durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado. Una vez cumplido el periodo al que se refieren los párrafos anteriores, los datos sólo podrían ser conservados previa *disociación* de los mismos, sin perjuicio de la obligación de bloqueo, prevista en la LOPD y en el Reglamento. Si no se realizaban estas obligaciones de cancelación de datos innecesarios, se estaría ante un incumplimiento de los artículos mencionados y también del artículo 6.1 LOPD, como un tratamiento sin consentimiento del titular ni autorización legal. La cancelación de datos personales cuando se haya cubierto la finalidad para la que fueron recabados forma parte de la lógica y fomenta, no sólo la calidad del tratamiento de los datos personales, sino también la seguridad del mismo.

7.1.4 Recogida de datos por medios fraudulentos, desleales e ilícitos.

Por último, el artículo 4.7 prohibió la recogida de datos por medios fraudulentos, desleales o ilícitos, siendo una expresión sumamente ambigua³⁵¹. El Reglamento no aclaró tampoco qué se puede considerar bajo estas expresiones, pues lo reitera casi textual en el artículo 8.1. pero no las explica. la LOPD expresó tres conductas prohibidas diferentes: el uso de medios fraudulentos, el uso de medios desleales y el uso de medios ilícitos. Estas expresiones no son sinónimas, ni deben concurrir conjuntamente

³⁵¹ Se puede enmarcar dentro de la doctrina civilista en las obligaciones contractuales lógicas que se expresan el artículo 7 y 1.104 del CC, en cuanto a la diligencia debida y a la buena fe.

los tres supuestos para considerar una conducta contraria a la LOPD, sino que basta la concurrencia de uno de ellos. Las expresiones deben ser interpretadas de conformidad con otros artículos de la LOPD³⁵²

7.2. El derecho a ser informado.

En el Título II se trató como principio de la LOPD el importantísimo derecho del titular de los datos personales a la información en la recogida de sus datos por cualquier responsable de su tratamiento. El titular de los datos otorgará su conformidad al tratamiento después de haber sido informado sobre la intención del responsable del tratamiento o del fichero para tratarlos, esa es su finalidad. Si no se conociera el tratamiento y la finalidad que explican la razón de la recogida de datos, el titular no podría otorgar debidamente su consentimiento. Como ya se comentó, existen dos su-

³⁵² “El uso de medios fraudulentos sucede cuando, mediante el engaño o fraude, alguien consigue que la persona facilite sus datos.” Lo deduce así del contenido del artículo 44.4 LOPD, que tipifica como infracción muy grave “el uso de estos medios para la obtención de los datos” y del Diccionario RAE, que define “fraudulento” como “engañoso, falaz”. Medios fraudulentos se consideran aquellos que producen un “engaño o confusión” en el titular de los datos; sin tal engaño o confusión el titular de los datos no hubiera expresado su voluntad, por lo que, de haber conocido la realidad, no se hubiera producido el consentimiento. La voluntad está viciada por el engaño. El uso de medios desleales es explicado desde la definición de la RAE de la palabra “desleal”, “deslealtad”, y se define como “la falta de observancia de la confianza que alguien debe a otra persona.” Es lo contrario la fidelidad o lealtad. Estos significados “implican la existencia de un deber o una obligación (jurídica o moral) que vincule a la persona desleal con quien sufre esta circunstancia.” Debe existir una relación de confianza o jurídica (o ambas) El incumplimiento de esta obligación se genera por un abuso de confianza de la parte que incumple. En el caso de la aportación de datos, “la deslealtad sólo existirá cuando se permite voluntariamente el acceso a la información en base a la confianza que vincula a dos personas”. La prohibición del artículo 4.7 es para la obtención de datos “mediante el engaño, el abuso de confianza o la vulneración de normas, constituyendo tres prohibiciones claramente distinguibles.” Los medios ilícitos para acceder a la información personal son aquellos que la RAE define como “no permitido legal o moralmente”. Se usan medios prohibidos por una regla jurídica o moral para obtener datos de carácter personal.

puestos para acceder a datos personales. El primero a través del propio titular, la persona física que otorgaría el consentimiento para tratarlos; el segundo sería por fuentes accesibles al público, caso en el cual el consentimiento se recabaría con posterioridad para que el titular ejerza sus derechos de acceso, rectificación, oposición y/o cancelación, especialmente estos últimos si no desea que sus datos sean tratados por el responsable del fichero o tratamiento en cuestión. El deber previo de información para el primer caso quedaría sustituido por el deber posterior de información en el segundo caso. El responsable del fichero o del tratamiento tendría un deber de *hacer* anterior a cualquier actividad que desee o necesite realizar con datos personales.³⁵³ Debería informar al titular, porque ese es su derecho, de quién tiene sus datos y con qué finalidad, por tanto, informa de la existencia de un fichero, de la finalidad del tratamiento de los datos y de los posibles destinatarios o cesiones de datos personales. El responsable del fichero o tratamiento responde de esta obligación, en cualquier caso. El Reglamento resultó de todos modos muy controvertido con esta cuestión³⁵⁴, pues el artículo 18 del Reglamento fue anulado por la STS 4057/2010, de 15 de julio de 2010; STS 4047/2010, de 15 de julio de 2010 y STS 4050/2010, también de 15 de julio de 2010. Los argumentos del TS para anular este artículo del Reglamento,

³⁵³ Se remite a la Sentencia del TC 292/2000 ya comentada en otro epígrafe. Igualmente se apunta que los datos personales recabados de fuentes accesibles al público tendrán la misma operativa de información, pero *a posteriori*, no en el momento de ser recabados. También se apunta a la posibilidad de que los datos sean recabados por imperativo o habilitación legal para que los datos sean tratados sin consentimiento de su titular.

³⁵⁴ Texto del anulado Artículo 18 del Reglamento de la LOPD, acreditación del cumplimiento del deber de información:

1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.
2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.”

se basaron en el principio de libertad de forma, que se refleja en el artículo 5 de la LOPD y, en general, en todo el sistema jurídico español, para cumplir con las obligaciones y con el derecho de información del titular de los datos personales, sin requerimientos específicos y posibilitando que los medios para probar que el titular ha sido informado sean múltiples en sus formas (escrita, verbal, telemática, grabación de voz, por ejemplo). La obligación del responsable estribó en la idea de que la información sobre el tratamiento de los datos sea *expresa, precisa e inequívoca*, pero sin hacer referencia a la forma. La obligación de acreditar el cumplimiento del deber de información no varía en la práctica, pero no existe la obligación de constancia documental que sí exigía el Reglamento. Las empresas deberían guardar en cualquier caso la prueba de que el titular fue informado sobre el tratamiento de sus datos³⁵⁵.

Las Sentencias del TS supusieron en su momento una serie de declaraciones sobre cuestiones y recursos presentados ante este Tribunal por empresas de sectores financieros y empresas que gestionan archivos de personas deudoras a entidades de crédito (ficheros de solvencia patrimonial); como se reflejaron en la prensa³⁵⁶, las empresas fueron la Asociación Nacional de Establecimientos Financieros de Crédito o más conocida por sus siglas ASNEF, la empresa Bureau de Crédito, S.A. y la Federación de Comercio Electrónico y Marketing Directo, por sus siglas FECEMD. Afectaron a más artículos del Reglamento, como se verá. El interés de estas empresas, bajo siglas de asociaciones o federaciones, eran introducir datos personales sin prueba del deber de

³⁵⁵ Alguna doctrina anterior había marcado la falta de precisión en los términos “adecuados, pertinentes y no excesivos” que la LOPD utilizó. Véase los comentarios de GUERRERO PICÓ, M., *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Navarra, 2006, pág. 238.

³⁵⁶ Una referencia puede ser la noticia en el diario Expansión, cuyo link se aporta a título de comentario, no de análisis. El titular es desorbitado y exagerado. “El Tribunal Supremo revoluciona el marco de protección de datos en España”

<http://www.expansion.com/2010/07/27/juridico/1280227228.html> a 25 de octubre de 2015.

información³⁵⁷, lógicamente, para evitarse el coste y el trabajo de recabar el consentimiento para el tratamiento de datos personales de un sector de población que había producido impagados a entidades de crédito o que eran objetivo de tratamientos de datos para marketing. El TS planteó también dos cuestiones prejudiciales ante el Tribunal de Justicia de las Comunidades Europeas (en adelante TJCE)³⁵⁸ sobre la aplicación directa del artículo 7.f) de la Directiva 95/46/CE, cuestión que el TJCE cierra considerando los efectos del citado artículo como directos.

El artículo 5 LOPD no aclaró si el derecho a la información del titular de los datos, se trata de un requisito previo o de un contenido esencial del derecho fundamental en sus cinco apartados, los cuales hablan del contenido, forma y requisitos de la información en los dos casos mencionado: cuando los datos son recabados del propio interesado titular en los tres primeros puntos y cuando los datos son obtenidos de otros medios en los dos últimos. No se entra a considerar el contenido de un derecho subjetivo, sino que se enumeran genéricamente deberes y obligaciones cuyo destinatario no se especifica ni se define, se empleó el término *interesado* al mencionar al titular del derecho fundamental, con cierto carácter pasivo, como sujeto de un deber de información que corresponde al responsable del fichero, término que sólo se mencionó también en el punto 4 del artículo 5 LOPD. Como se expuso, el artículo del Reglamento que lo desarrolla resultó derogado después de las Sentencias del TS y del TJCE.

En cuanto al contenido del artículo 5 LOPD, se podría apreciar que los tres primeros puntos contienen requisitos materiales y formales exigibles a la información que se recaba del propio titular, como requisitos de calidad de la información y su forma. En

³⁵⁷ Las empresas tenían además otros intereses, como la inclusión de datos personales en listados de impagados antes de tener una sentencia firme declarativa que diera fuerza de certeza legal a la deuda reclamada.

³⁵⁸ Sentencia del TJCE de 24 de noviembre de 2011. Texto completo en <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62010CJ0468> a 25 de octubre de 2011. También la AEPD publica esta sentencia en http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_justicia/common/14_Sentencia_de_24_de_noviembre_de_2011._Asuntos_C-468-10_y_C-469-10._ASNEF_y_FECEMD_v_Administraci-oo-n_del_Estado.pdf

los dos siguientes se señalan las excepciones, las cuales son muy débiles ante la fuerza de las obligaciones. El contenido, por tanto, se resumiría en el deber de información del responsable del tratamiento o del fichero ante el titular de la existencia de un fichero o tratamiento de datos personales. (artículo 5.1.a); de la finalidad para recabar los datos y su destino (artículo 5.1.a); de los destinatarios de la información (artículo 5.1.a); del carácter obligatorio o facultativo para la respuesta del titular a las respuestas que se le planteen. (artículo 5.1.b); de las consecuencias de la obtención de los datos o de la negativa a suministrarlos. (artículo 5.1.c). También de los importantes derechos de acceso, rectificación, cancelación y oposición (derechos ARCO, se recuerda, artículo 5.1.d); de la identidad y dirección física del responsable del tratamiento o de su representante en España. (artículo 5.1.e) y por último e importante la actividad del cesionario³⁵⁹, en caso de que se produzca cesión de datos, obligatoria o no obligatoria. (artículo 12.2 del Reglamento, que continúa en vigor).

Los requisitos de forma que debía cumplir la información para el titular de los datos personales o aspectos que tienen más que ver con la manera en la que se recaba la información se manifiestan en el artículo 5.1, que consagró la expresión frecuentemente utilizada de modo *expreso, preciso e inequívoco*. Cualquier expresión de consentimiento con efectos jurídicos tiene esta forma, no solamente para el derecho a la protección de datos. La información para otorgar cualquier consentimiento con efectos jurídicos debe ser siempre clara y explícita. Otras exigencias lógicas, que pertenecen a cualquier campo del Derecho y su ejercicio, serían el artículo 5.2 LOPD, para exigir que en los cuestionarios de petición de datos figuren las advertencias del punto 1, de forma claramente legible. Las excepciones a esta obligación no son tales, sino solamente una flexibilización que se refleja en el artículo 5.3 LOPD, pues la obligación sigue vigente en todos los casos, lo único que dice ese punto es que cuando fuera obvio su utilización no sería necesario informar. Se está hablando de situaciones obvias de claridad, por ejemplo, para servicios de emergencia médica en la que la salud del titular se encuentre en riesgo.

³⁵⁹ Esta cesión obligatoria son los casos que la ley impone, por ejemplo, para las AAPP, como datos para recaudación impositiva o Seguridad Social.

Los puntos 4 y 5 del artículo 5 LOPD describieron la información que debe tener el titular cuando sus datos fueran tratados por responsables de fichero o de tratamiento obtenidos de fuentes que no son el interesado. El consentimiento del titular no se otorgó en el momento de recabarse los datos personales, por tanto, se debía esperar a que el titular tuviera conocimiento del tratamiento de los datos para que otorgase su consentimiento informado. La LOPD, como ya se ha comentado, obligó a facilitar al titular la información de que sus datos, obtenidos por otras fuentes que no son él mismo, son tratados y por quién, para lo que se solicitaba su consentimiento en algunos casos (se flexibiliza la obligación) y en otros no se exige este deber de información (casos en los que se exime la obligación de informar). El artículo 5.4 marcó un plazo para facilitar al titular la información de tres meses desde el registro de los datos, con la excepción de haber sido informado con anterioridad. No existía la obligación de facilitar información a los titulares de datos personales en los supuestos que refleja el artículo 5.5. LOPD. En cualquier caso, se debía respetar el contenido esencial del derecho a la protección de datos, aun cuando estas excepciones fueran situaciones que hiciesen imposible realizar el *derecho-deber* de información y, por tanto, obtener el consentimiento del titular para el tratamiento de sus datos personales. Son situaciones enumeradas como los mandatos judiciales o legales, los tratamientos de datos personales para fines científicos, históricos y estadísticos, en los que se recomienda su anonimización; los casos en que sea imposible llevar a cabo la obligación de informar, o exija esfuerzos desproporcionados; esto se debía someter al criterio de la AEPD o del organismo autonómico competente, para que considerasen esta cuestión en función del número de interesados, la antigüedad de los datos o las medidas compensatorias y los ya comentados datos personales que proceden de fuentes accesibles al público y cuya finalidad sea la publicidad o prospección comercial; en este caso, cuando se produzca la llegada de la información publicitaria, se informará al titular de la fuente de los datos, la identidad del responsable del fichero o tratamiento y de los derechos ARCO. Existía una vinculación clara entre este artículo 5 LOPD, *derecho-deber* de información, el artículo 6 y el artículo 15 de la LOPD, como se expondrá a continuación.

7.3. El Consentimiento del Afectado.

El consentimiento del titular de los datos para su tratamiento se convirtió, como se puede deducir de esta exposición, en la base de todo el derecho fundamental a la protección. Es el denominado *principio del consentimiento*, pero realmente es un derecho del titular y una obligación del responsable del fichero o tratamiento antes de cualquier tratamiento de datos o con posterioridad en determinados casos. *El consentimiento es una declaración de voluntad hacia el responsable del tratamiento o del fichero para que pueda tratar sus datos de acuerdo con la información presentada.* En el artículo 6.1 LOPD se estableció que el consentimiento será inequívoco; el Reglamento, que dedicó un Capítulo, el II del Título I, con el epígrafe Consentimiento para el tratamiento de Datos y deber de información, sistematizado como Sección 1ª, lo reflejó en el artículo 12 y siguientes, vinculando sistemáticamente consentimiento e información. El consentimiento inequívoco se puede presumir de todo consentimiento dentro del Derecho³⁶⁰. En el caso de la Protección de datos se marca el calificativo de *inequívoco* como un sinónimo de indubitado, sin dudas³⁶¹. Como gran parte de la terminología en esta materia, es una traducción de la Directiva 95/46/CE, en su artículo 3.h). Y la propia LOPD estableció una definición clara de consentimiento del

³⁶⁰ La Doctrina civilista así lo contempla y realiza estudios sobre esta cuestión que pueden ser muy interesantes y empleados en materia de protección de datos. Pero esta tesis se centra en el análisis de la protección de datos como derecho fundamental, por ello se remite este asunto a la doctrina y no se refleja en la profundidad que requiere. Se realiza un apunte especial a las teorías alemanas sobre la voluntad (*Willenstheorie*) cuyo representante más destacado es SAVIGNY y las teorías declaracionistas (*Erklärungstheorie*) con pensadores como KOHLER.

³⁶¹ FERNANDEZ LÓPEZ, JUAN MANUEL; "Comentario al artículo 6. Principio de Consentimiento", *Comentario a la Ley Organica de Protección de Datos de Carácter Personal.*, Madrid, 2010, pág. 453-472. Apunta igualmente el autor en su texto las dudas que le suscitaba ya en ese momento la transferencia de datos a EEUU bajo la doctrina de *puerto seguro* que posteriormente se vió afectada por Sentencias del TJCE y el TS.

afectado o titular de los datos en el artículo 3 h)³⁶², por lo que no es necesario recurrir al Derecho Civil para otorgar validez al consentimiento informado bajo los parámetros generales, sino que la LOPD los define así: *Consentimiento del interesado: toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos que le conciernen*. Por tanto, el consentimiento se otorga por una *libre manifestación de voluntad*, exteriorizando su facultad de libre decisión, *sin coacción ni limitaciones, inequívoca*, sin dejar lugar a dudas y *concreta* para el caso requerido, *específica*, para tratamientos concretos e informados, *con una finalidad limitada*. Una cuestión complicada se presentó en el asunto de la prueba del consentimiento tácito. Cuando el consentimiento es expreso, por cualquier medio (firma digital, firma en papel, grabación de voz, entre otros posibles) no existen dudas. Pero qué ocurre cuando se debe probar la existencia del consentimiento tácito. El artículo 12.3 del Reglamento obligó al responsable del fichero o tratamiento a probar y aportar dicha prueba de consentimiento del titular de los datos, por cualquier medio admisible en Derecho. La AN en numerosas Sentencias y la AEPD así lo confirmaron³⁶³. El consentimiento es de suma importancia para la eficacia del derecho a la protección de datos personales, se encuentra en el núcleo material del derecho fundamental como derecho de autodeterminación informativa y control de información personal³⁶⁴.

³⁶² Este artículo de la LOPD tuvo muchas enmiendas en su tramitación. La desordenada redacción del Título II LOPD dio lugar a serios debates sobre su contenido. El Reglamento tiene una sistemática más limpia y lógica, haciendo más comprensibles los principios y los derechos de la ley para los ciudadanos.

³⁶³ Las Resoluciones de la AEPD no han variado hasta la fecha en la exigencia al responsable del fichero o tratamiento de datos personales de la prueba en la existencia del consentimiento del afectado. No se está ante una cuestión civil, por la que la prueba recae en quien alega, sino ante una cuestión administrativa que se rige por sus propias normas, en este caso, la LOPD

³⁶⁴ MURILLO DE LA CUEVA, P., "La protección de los datos de carácter personal en el horizonte del 2010", *Anuario de la Facultad de Derecho*, nº 2, 2009, págs. 131-142, pág. 141. Marca la incoherencia entre el artículo 6.1. y sus obligaciones contrastado con el artículo 14 del Reglamento que permite la presunción en determinados casos.

7.3.1 Excepciones a la obligación de recabación del consentimiento.

El artículo 6.2 LOPD reunió los supuestos de excepción a la obligación de recabación del consentimiento. Se agruparon en los supuestos de datos de titulares para el ejercicio de las funciones de las AAPP, datos personales necesarios para formar parte de contratos, precontratos, negocios, relaciones laborales, porque sin esos datos es imposible su realización; datos imprescindibles para proteger un interés vital del titular en los términos del artículo 7.6. LOPD y de nuevo, datos de fuentes accesibles al público. El artículo 10.2 del Reglamento, bajo el epígrafe supuestos que legitiman el tratamiento o cesión de datos, recogió una serie de situaciones que se pudieran considerar excepciones a la obligación de consentimiento para el tratamiento de datos personales. Esta sistemática se consideró poco afortunada por la doctrina, pues es un artículo anterior al capítulo II que fue dedicado al consentimiento del afectado³⁶⁵. El artículo 10 LOPD se encuentra en el capítulo I, dedicado a la calidad de los datos; que las excepciones se formulen antes que las normas generales es una falta sistemática, cuando no un error o falta de capacidad legislativa. Los supuestos, dispersos, son los siguientes:

7.3.2 Supuestos de habilitación para el tratamiento y cesión sin consentimiento

La norma de protección de datos consideró que se habilitaba el tratamiento y cesión sin el consentimiento del titular cuando una norma con rango de ley o una norma de derecho comunitario (europeo) lo autorizara. (artículo 10.2.a) También en el supuesto de que el tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario, con prevalencia de los dere-

³⁶⁵ DÍAZ REVORIO, FRANCISCO JAVIER; , "Comentario al artículo 5 LOPD. Derecho de la Información en la recogida de datos. Una perspectiva constitucional.", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.*, Madrid, 2010, pág. 436 y ss.

chos y libertades fundamentales del titular de los datos, según el artículo 1 LOPD (artículo 10.2.a) 2º párrafo). Por último, por mandato legal, cuando el tratamiento o la cesión fueran necesarios para que el responsable del tratamiento cumpliera un deber que le imponga una norma (artículo 10.2.a) 3º párrafo).

Se distinguiría entre las normas que sí son totalmente obligatorias, como Reglamentos y Tratados, con efectos tanto a nivel vertical como horizontal dentro de nuestro sistema, para las cuales no es necesaria la transposición de estas normas y son de obligado cumplimiento en todos los Estados Miembros desde su entrada en vigor, de las Directivas comunitarias que no tienen este rango normativo, pues solamente tienen efecto directo vertical, obligando a los Estados Miembros a su trasposición legal en el plazo que indiquen; durante su trasposición, el derecho interno es el referente legal. Los ciudadanos tienen derecho a reclamar daños y perjuicios al Estado que no ha cumplido en plazo. La AN en muchos casos se refiere a la Directiva 95/46/CE para argumentar sus decisiones.

7.3.3 Supuestos de tratamiento y cesión sin consentimiento.

Son tres los supuestos que la LOPD regula y en los que no sería necesario el consentimiento del titular de los datos. El primero se refiere a las funciones de las AAPP y su necesidad de tratamiento de datos personales en el ámbito de sus competencias, atribuidas por una norma con rango de ley o una norma de derecho comunitario (artículo 10.3.a) El segundo supuesto se produciría en el caso de que sean necesarios para la celebración, mantenimiento o cumplimiento de un contrato o precontrato, la existencia de una relación comercial, laboral o administrativa de la que sea parte el titular de los datos personales (artículo 10.3.b) y por último cuando fueran necesarios para mantener un interés vital del titular (artículo 10.3.c) Estos casos estarían claros en su configuración, correspondiendo a la redacción del artículo 6.2 LOPD. El artículo 7.6. LOPD regularía supuestos de tratamiento de datos especialmente protegidos en casos de vital importancia, como en la situación que pudiera encontrarse el titular u

otra persona vinculada se encontraran física o jurídicamente incapacitados para otorgar el consentimiento. El punto 3 del artículo 6 LOPD trató del supuesto de revocación de consentimiento, que se delimitó a la causa justificada y a la falta de efectos retroactivos. La revocación no debía necesitar causa justificada por parte del titular. Esta redacción fue criticada desde la doctrina, alegando que, si el consentimiento se considera libre, la revocación también debería serlo.

La revocación del consentimiento fue tratada en el artículo 17 del Reglamento. El titular podría ejercer la revocación de su consentimiento *a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento*. Se presentaron alternativas para que el titular pudiera ejercer su derecho de revocación del consentimiento por medio del envío de cartas prefranqueadas, llamadas a un número gratuito o servicios de atención al público sin coste alguno (artículo 17.1) El titular de los datos no debía soportar coste alguno cuando deseara revocar el consentimiento otorgado. El plazo para el cese del tratamiento sería de 10 días desde la recepción de la revocación (artículo 17.2.), teniendo en cuenta, además, la obligación de bloqueo de los datos que ordena el artículo 16.3 LOPD, la comunicación de la revocación a los cesionarios (en el mismo plazo, se entiende, artículo 17.4) y la confirmación de que la revocación se ha recibido y realizado el cese del tratamiento de forma expresa por el responsable del tratamiento (artículo 17.3., se entiende que también en el mismo plazo de 10 días)

7.3.4 El derecho de oposición.

El punto 4 del artículo 6 LOPD estableció que en los casos en los que no fuera necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no dispusiera lo contrario, éste podría oponerse a su tratamiento cuando existieran motivos fundados y legítimos relativos a una concreta situación personal. *En tal supuesto, el responsable del fichero excluiría del tratamiento los datos relativos al afectado*. Se consideró el texto otra fuente continua de con-

troversia por la doctrina, pues siendo una transposición de la Directiva 95/46/CE, el derecho de oposición se trasformó en algo que no se entendió bien dentro del derecho español. La LOPD lo mencionó, pero no lo definió; fue el Reglamento de nuevo, en su artículo 34, la norma de referencia para aclarar el enunciado de la LOPD. El Reglamento dedicó todo un Capítulo al derecho de oposición, el capítulo IV del Título III, que tuvo como epígrafe *Derechos de acceso, rectificación, cancelación y oposición*. Son los artículos 34 a 36 del Reglamento. El derecho de oposición se definió en el artículo 34 del Reglamento como el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en el supuesto de que no fuera necesario su consentimiento para el tratamiento, también como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justificara, siempre que una Ley no dispusiera lo contrario; en otros casos, cuando se tratara de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 del Reglamento, cualquiera que fuera la empresa responsable de su creación y cuando el tratamiento tuviera por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 del Reglamento.

Una parte de la doctrina consideró que el Reglamento no debería regular estos supuestos junto con sus excepciones, pues era una cuestión reservada a la ley³⁶⁶. Esta opinión también la compartió VILLAVERDE MENÉNDEZ³⁶⁷, quien consideró que en el Reglamento pudiera invadir materias propias de la Ley, siendo la LOPD, y no la norma reglamentaria, la que debe regular el ejercicio del derecho de oposición en su *calidad de facultad integrada* en el contenido constitucional del derecho fundamental a la protección de los datos personales. El artículo 35 del Reglamento formuló una norma-

³⁶⁶ FERNANDEZ LÓPEZ, JUAN MANUEL; "Comentario al artículo 6. Principio de Consentimiento", *Comentario a la Ley Organica de Protección de Datos de Carácter Personal.*, Madrid, 2010, pág. 472 y ss.

³⁶⁷ VILLAVERDE MENÉNDEZ, IGNACIO; "Comentario al Artículo 6. Derecho de oposición. ", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal.* , Madrid, 2010, pág. 502.

tiva de procedimiento para el ejercicio del derecho de oposición; este derecho se ejercería por el titular de los datos mediante solicitud dirigida al responsable del tratamiento, debiendo resolverse su petición en el plazo de 10 diez días. Siempre se respondería al afectado, aunque no se dispusiera de sus datos, es decir, el titular reclama información sobre datos que el responsable no tendría dentro de sus ficheros y, por tanto, no los habría tratado. Para el caso de que sí se traten datos del titular, se procedería a la exclusión de los tratamientos en el mismo plazo. Si alguna de estas circunstancias no se cumpliera, el titular de los datos podría acudir a la AEPD para reclamar su tutela. Antes de acudir a la AEPD, el titular debe solicitar sus derechos ante la empresa u organismo responsable que sea titular del fichero en que se supongan tratados los datos de carácter personal³⁶⁸. En torno a este asunto, consentimiento y oposición al tratamiento de datos, es llamativa la reiteración de fallos en los sistemas de comunicación de las empresas, que envían publicidad a personas que no sólo dejaron de ser clientes, sino que, además, manifestaron claramente su voluntad de no recibir más notificaciones de ningún tipo remitidas por la misma organización. Serían circunstancias habituales de reclamación de tutela a la AEPD frente a diferentes empresas denunciadas³⁶⁹.

³⁶⁸ Derechos ARCO; en este link se especifica el derecho de oposición http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/oposicion-ides-idphp.php

³⁶⁹ Del estudio de las diferentes Resoluciones de la AEPD se desprende que, en todas ellas, las multas son cuantiosas. El perfil de las empresas multadas suele ser la gran o mediana empresa. La pequeña empresa no suele ser denunciada, aunque existen casos. En ellos, la AEPD suele ser comprensiva ante la pequeña empresa, salvo que exista un ánimo que roce lo delictivo.

http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2015/common/pdfs/PS-00082-2015_Resolucion-de-fecha-08-09-2015_Art-ii-culo-6.1-LOPD.pdf de esta Resolución se extrae el texto de las Sentencias que se menciona a continuación y que se puede leer en otras muchas Resoluciones.

http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2015/common/pdfs/PS-00129-2015_Resolucion-de-fecha-11-09-2015_Art-ii-culo-6-LOPD-22.1-LSSI.pdf Aquí la AEPD trata muchos artículos de la LOPD, porque el caso no está exento de importancia y gravedad. La multa impues-

En cuanto a las Sentencias sobre el derecho de oposición, la AEPD priorizó en sus argumentaciones a dos resoluciones: la SAN 3938/2006, de 20 de septiembre, y la SAN 1036/2009, de 4 de marzo.

En la SAN 3938/2006 de 20 de septiembre (FJ 6), la Sala consideró que el consentimiento debe ser inequívoco, pues “*se trata de una garantía fundamental, legitimadora del régimen de protección establecido por la Ley*, en desarrollo del Art. 18.4 de la Constitución, dada la notable incidencia que el tratamiento automatizado de datos tiene sobre el derecho a la privacidad en general, y sobre los derechos al honor y a la intimidad y a la propia imagen, y que sólo encuentra, como excepciones al consentimiento del afectado, aquellos supuestos que, por lógicas razones de interés general, puedan ser establecidos por una norma de rango de Ley”

En la SAN 1036/2009, de 4 de marzo (FJ 4), la AN interpretó que “es de interés reseñar que el apartado 1 del artículo 6 LOPD exige el consentimiento inequívoco del afectado para el tratamiento de sus datos de carácter personal. El adjetivo *inequívoco* que califica al consentimiento, significa según el Diccionario de la Real Academia Española *que no admite duda o equivocación* y, por contraposición, a equívoco, lo que no puede entenderse o interpretarse en varios sentidos o que no puede dar ocasión a juicios diversos.” La AN consideró que sólo el titular puede otorgar el consentimiento para el tratamiento de sus datos “pues es él y no un tercero quien tiene el poder de disposición y control sobre sus datos personales, aun cuando no se requiere que se produzca de forma expresa o por escrito, pero sí debe reunir los requisitos previstos en el artículo 3.h) y 6.1 de la LOPD”.

La orientación que encontró en la AEPD el responsable del fichero o tratamiento para cumplir con sus obligaciones, en especial en cuanto al consentimiento del titular, no es amplia ni clarificadora. La *Guía del Responsable del Fichero* dedicó sus páginas a

ta de 50.000 Euros por infracción del artículo 6.1 LOPD; otra de 1.000 Euros por información del artículo 21.1 LSSI, que no está incluida en este análisis, pero sí relacionada. Ambas Resoluciones son recientes, del año 2015.

definir qué obligaciones tiene dicho Responsable³⁷⁰. Para una persona ajena a la formación jurídica, es una ardua tarea intentar entender cuáles son sus obligaciones. Sería todo mucho más sencillo si la propia AEPD tuviera su formulario o formularios para la generalidad de los casos y para los más complicados se realizaría un estudio por parte de sus servicios jurídicos y con su aprobación. Así se evitarían la mayoría de las complicaciones empresariales en ese sentido. En cuanto al derecho de oposición en relación con la revocación del consentimiento, la *Guía* no fue extensa en sus explicaciones para determinar *qué es la oposición* al tratamiento de los datos. Más bien nombró reiteradas veces el derecho de oposición, pero no lo aclaró. La AEPD, para contribuir con mayor y mejor eficacia a la protección de datos, podría también en este caso realizar una serie de documentos obligados en idioma comprensible; tiene un Canal³⁷¹, para el responsable de ficheros en el que se encuentra información, que debería aportar procedimientos claros, no sólo la enumeración de las obligaciones. La AEPD publicitó el derecho de oposición³⁷² como derecho del titular de los datos en el Canal del Ciudadano; serían también conveniente que existiera una orientación mayor para el obligado a cumplir los derechos del titular, la persona física o jurídica responsable del tratamiento.

7.4. El consentimiento de los menores de edad

³⁷⁰ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Guía del Responsable del Fichero"]. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

³⁷¹ Canal del Responsable del Fichero <https://www.agpd.es/portalwebAGPD/canalresponsable/index-ides-idphp.php>

³⁷² http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derechos/oposicion-ides-idphp.php Este derecho, como los de acceso, rectificación, oposición y cancelación (ARCO) se encuentran explicados dentro del Canal del ciudadano, siendo obligado su cumplimiento para el titular de los datos al Responsable del fichero o tratamiento. Existen igualmente formularios para su ejercicio destinados al titular, pero no se especifica claramente su procedimiento para el responsable.

Existe un debate doctrinal que excede el objeto del presente estudio, pero que se considera interesante su alusión. El profesor PÉREZ LUÑO aludió a la carencia de regulación dentro de la LOPD del consentimiento en los casos de tratamiento de datos pertenecientes a titulares menores de edad³⁷³. De nuevo fue el Reglamento quien suplió esta ausencia legislativa en el artículo 13, estableciendo que podrá procederse al tratamiento de los datos de los *mayores de catorce años* con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores. En ningún caso podrían recabarse del menor datos que permitieran obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. Podrían recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de obtener la autorización del tutor legal del menor. En todo caso, correspondió al responsable del fichero o tratamiento articular los procedimientos para garantizar que se comprobó de modo efectivo la edad del menor y la autenticidad del consentimiento prestado, en su caso, por los padres, tutores o representantes legales. El comentario, que se apunta como referencia y como espléndido discurso, merece un marco más acorde con ese tema. Este texto se dirige hacia la práctica empresarial y ciudadana. El asunto de menores se tratará sólo a un nivel de casos en los que impliquen a menores en algunas prácticas empresariales. PÉREZ LUÑO, expuso que con esa regulación se trató de evitar los efectos negativos de los perfiles de personalidad de menores de edad elaborados en función de las informaciones contenidas en bases de datos personales. Dichos perfiles podrían considerarse como la reputación o fama, que es expresión de la dignidad y el honor y que puede ser valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas. La vida cotidiana de los menores se ve afectada por una serie de valoraciones familiares, socia-

³⁷³ PÉREZ LUÑO, A., "Comentario al Artículo 6 LOPD. El consentimiento de los menores.", *Comentario a la Ley Orgánica de Protección de Datos.*, Madrid, 2010, pág. 473-494.

les, escolares, entre otras posibles, sobre su conducta, que pueden ser tomadas en consideración para las más diversas circunstancias, presentes o futuras en la vida del menor, tales como el ingreso en un centro escolar o universitario, la concesión de una beca o la admisión en determinadas instituciones o colectivos.³⁷⁴ La Directiva 95/46/CE tampoco contempló este asunto de suma importancia en la actualidad. El GT29 elaboró a lo largo de estos años varios informes y Dictámenes sobre el consentimiento de los menores de edad. Destaca en el ámbito de las empresas las Recomendaciones para la creación del Código de Conducta sobre comercialización directa de 2003, con una importante revisión en 2010. Son un conjunto de buenas prácticas, una autorregulación para el tratamiento de datos de menores y la comunicación con ellos. Otras materias abordadas a nivel europeo serían la geolocalización de menores, la protección de los menores en las redes sociales, en el ámbito escolar, prácticas publicitarias con menores, entre otras materias que afectan a todo el espacio territorial europeo (EEE). La AEPD suplió también la carencia de regulación de estos supuestos de menores aportando información muy valiosa³⁷⁵. El menor de 14 años debía obtener siempre el consentimiento de sus padres o tutores legales para el tratamiento de sus datos, así lo reguló el Reglamento y en el informe jurídico de la AEPD que se referencia. Los menores se encuentran especialmente expuestos al uso de información personal, ya no sólo de sí mismos, también para obtener datos de su entorno familiar y social, con fines comerciales, de ocio o de operativa por *internet*, que no siempre es inocente. Sólo hay que leer u oír la incidencia que determinados usos de dispositivos, junto con las redes sociales, produjeron en determinados casos de menores, que son

³⁷⁴ Véase PÉREZ LUÑO, obra citada, página 493-494.

³⁷⁵ Desde informes jurídicos hasta videos informativos destinados a menores, como la página www.tudecideseninternet.es, desarrollada para ser una herramienta en la educación de los menores para proteger sus datos. En la "Guía para el Ciudadano". También se hace mención de los menores y sus derechos, además de recomendar otra Guía específica para menores: "Recomendaciones, Derechos de niños y niñas, Deberes de los padres y madres AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Recomendaciones. Derechos de niños y niñas. Deberes de los padres y madres."].

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2008/recomendaciones_menores_2008.pdf.

delictivos y rebasan con mucho el tema de esta tesis. Su estudio pertenece más al derecho penal, pues las consecuencias no se detienen con sanciones administrativas. Esas conductas son delitos en toda su extensión, tanto de adultos contra menores, como de menores entre sí, generando algo que pasa de la broma al delito. Además, como señala la AEPD en los textos comentados y en sus informes jurídicos, muchas veces son los padres, quiénes al emplear *internet* para comunicarse, ponen en riesgo a sus hijos, a través de *blogs* o redes sociales con información personal de menores. Otras leyes entran en consideración, como la Ley Orgánica 1/1996 de 15 de enero, de Protección Jurídica del Menor y también la ya comentada en este texto, Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, además de las leyes penales correspondientes si nos encontramos frente a un delito. Los avances tecnológicos y la facilidad de su uso por menores rebasan de nuevo la previsión de la AEPD para los menores y cualquier otra expectativa que hoy se pueda tener que será igualmente superada por la realidad³⁷⁶.

En cuanto a la incidencia en relaciones con empresas, especialmente colegios, la AEPD elaboró informes de consultas aclaratorios en temas como publicación de fotos de menores en las páginas web de colegios, inclusión de listados públicos e información académica a los padres; como ejemplos³⁷⁷.

³⁷⁶ Una de esas situaciones en que la realidad supera a las previsiones normativas es la enorme conflictividad entre padres divorciados por la exposición de datos del menor en perfiles de redes sociales de los propios padres, asunto ya comentado. Como ejemplo, véase la noticia

<http://www.abc.es/familia-padres-hijos/20150715/abci-legalidad-fotos-internet-201507141355.html>

³⁷⁷ Se apunta especialmente una conocida Resolución de la AEPD, la R/01349/2008, sobre el caso de una menor de 14 años que contrata servicios con Telefónica Móviles en el año 2008 y además la empresa incluye a la menor en el ASNEF por impagado. Se le impone a la empresa una cuantiosa multa por infracción del artículo 6 LOPD de 40.000 Euros y otra multa por infracción del artículo 4.3 LOPD de 30.000. Esta Resolución fue recurrida. El listado de Resoluciones que la AEPD recomienda sobre materia de menores se encuentra en

http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/menores/otros_textos/index-ides-idphp.php

7.5. La práctica empresarial frente a los principios de la protección de datos.

En la práctica, los responsables del tratamiento, en su mayoría, no tienen el más mínimo sentido de lo que se denomina calidad de datos. No tienen intención de maldad ni de incumplimiento, simplemente no entienden los conceptos de datos *adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas*. Existe también, una distancia de comprensión entre el pequeño empresario o autónomo y la gran empresa, tan abismal como real, sin tener que ver con la formación profesional recibida por los usuarios y responsables de tratamiento, resultando múltiples incidencias de calidad de datos en ambas tipologías de empresa. En la gran empresa, la cancelación de datos obedece no sólo a cuestiones de cumplimiento de la LOPD, sino también a razones técnicas o empresariales de diverso calado económico, pues mantener datos tiene costes importantes en infraestructuras y personal, por lo cual, si existen datos innecesarios, se procede a su borrado o destrucción. Si existe mantenimiento de datos en esta tipología de empresas también tiene sentidos comerciales o de estudios de mercado, por ejemplo. Para las PYMES no se puede hablar, en general, de un mantenimiento de los datos de calidad, con actualizaciones, y pensar en la cancelación de datos les resultaba a muchos empresarios o profesionales algo desconocido, apilando documentación sin concierto alguno, sin cuidado, por ejemplo, encima de una mesa, con nombres y apellidos de todos los implicados en casos incluso de repercusión penal (despachos de abogados). Otro ejemplo del mal tratamiento de datos personales se produjo en más de una ocasión con datos clínicos en un contenedor de la basura o en la papelera sin destruir, o datos de clientes de aseguradoras formando parte de bases de datos que no estaban en la finalidad propuesta al titular para su consentimiento. Estos son ejemplos de conducta que provienen de los posibles responsables del tratamiento o de fichero³⁷⁸.

³⁷⁸ Las PYMES y profesionales consideran los datos personales como un patrimonio, una forma de conocimiento. Los consultores tienen casos muy comentables, como un responsable de contabilidad de una empresa mediana, importante a nivel de Comunidad Autónoma que mantenía datos en soporte de pa-

Por parte de los titulares, se puede hablar, en la mayoría de casos, de falta total de concienciación respecto a qué datos deben aportar a quién y dónde. Los titulares extienden sus datos en cualquier situación, sin pensar en las consecuencias, muy al contrario, muchas son las personas que se sienten muy bien por difundir su imagen en los medios de comunicación, por ejemplo, sin trabas. Aportan documentación sin saber su finalidad, firman y aceptan consentimientos sin leer para cientos de empresas y no piensan en la calidad de los datos aportados, en muchos casos, ni razonan si su DNI está actualizado o en actualizar el empadronamiento, que es obligatorio en cualquier cambio de residencia. Las dificultades no son sólo culturales, también son de voluntad de entendimiento. Falta la voluntad de los propios teóricos interesados, los cuales parece que sólo la Ley tiene interés en la protección de sus propios datos, y, por tanto, de mantener el derecho fundamental reconocido que es la protección de datos personales. Estas dificultades, siguen sin solución; por una parte, existen ciudadanos que reivindican la protección del sistema jurídico frente al tratamiento incontrolado de datos, por otra, la sociedad de la información y las comunicaciones imposibilita la autodeterminación informativa total y completa de los titulares³⁷⁹.

pel con más de 25 años de antigüedad. Era imposible para el responsable pensar en la destrucción de esa enorme cantidad de datos en papel, especialmente de nóminas, pues lo consideraba inapropiado e ilógico. Discutir con esta persona no fue posible, se tuvo que esperar a su jubilación para llevar a cabo un cambio en los procedimientos. Otro caso de responsable de administración en una empresa de medianos-altos ingresos por facturación del sector agropecuario consideraba adecuada la cancelación de datos a través de la destrucción de papel en la barbacoa de verano, en la casa particular de su responsable de tratamiento. Vemos también casos de duplicidad de bases de datos, muy personales y protegidos especialmente (salud, raza, religión, sexualidad) en muchos casos, guardados en los lugares más pintorescos, por ejemplo, una cabaña en la montaña, como en el caso de varios abogados conocidos.

³⁷⁹ MURILLO DE LA CUEVA, P., "La protección de los datos de carácter personal en el horizonte del 2010", *Anuario de la Facultad de Derecho*, nº 2, 2009, pág. 131-142. "Mientras todo esto ha ido sucediendo los problemas a los que desde el primer momento se han tenido que enfrentar, primero, quienes reivindicaban la articulación de una protección jurídica contra el acopio y la utilización incontrolados de datos personales por terceros y, después, aquellos a quienes se ha encomendado la responsabilidad de aplicar las normas en las que se ha ido plasmando esa garantía, han permanecido inmutables. Esos problemas son, entre otros, el desconocimiento que la mayor parte de las personas tienen sobre

Al margen de la LOPD, los beneficios empresariales para mantener una calidad de datos personales, a través de procesos técnicos y de aprendizaje de los usuarios en sus procesos de tratamiento, son muy beneficiosos vistos desde una perspectiva avanzada, cumpliendo la legalidad y los DDFF. Se ahorran costes directos evitando tener información innecesaria, duplicada e inexacta, que sólo conduce a errores de gestión y a gastos, como, por ejemplo, el envío incorrecto de documentación o el coste de infraestructuras señalado. Se genera una sensación de seguridad en los clientes, con lo que se acentúa la fidelización. También se mejora la imagen corporativa al mejorar el servicio. Un titular de datos que se siente apreciado en una empresa será un cliente fidelizado. La autorregulación podría generar una mejor comprensión y gestión empresarial de datos personales, evolucionando los conceptos de DDFF a elementos integrados en la sociedad, comenzando con el respeto a los otros individuos que conforman el espacio social y siguiendo con el respeto a las normas fundamentales que ordenan el sistema jurídico. Esta cuestión se ampliará en posteriores epígrafes.

8. La vertiente más conflictiva: los Datos especialmente protegidos. El artículo 16 de la Constitución. Derechos fundamentales y realidad.

Los artículos 7 y 8 LOPD establecieron una regulación especial a los datos *especialmente protegidos* y *datos de salud*. El texto mencionó el artículo 16 CE, según el cual *nadie podrá ser obligado a declarar sobre su ideología, religión o creencias*, lo que se denominó como *datos especialmente protegidos*. Cuando en relación con estos datos

los peligros derivados del acceso por terceros a los datos que les identifican o permiten identificarlos cuando no afectan directamente a su vida íntima. Ignorancia que les lleva a no adoptar las cautelas que sí observarían si fueran conscientes de los resultados a que puede conducir la utilización de esa información y a no reaccionar frente a su utilización irregular. La relativa complejidad del lenguaje utilizado por el legislador, tributario en buena parte de terminología y expresiones procedentes de Directivas europeas, no es una ayuda para superar esta dificultad. Como tampoco lo es la tendencia de parte de los especialistas y de las instituciones de garantía a servirse de conceptos difíciles de comprender.”

se procediese a recabar el consentimiento de un titular, se advertiría al interesado acerca de su derecho a no prestarlo, debiendo ser el consentimiento expreso y por escrito para otorgarlo en los casos de tratamiento de datos. El artículo 7 LOPD reiteró en su redacción que sólo mediante el consentimiento expreso y por escrito del afectado podrían ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Las excepciones estuvieron en los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos, precisará siempre el previo consentimiento del afectado³⁸⁰.

El artículo 16 CE (nadie podrá ser obligado a declarar sobre su ideología, religión y creencias) se repitió textualmente en el artículo 7.1 LOPD. Esta tipología de datos junto con la libertad sindical forman un primer grupo de datos especialmente protegidos. El artículo 7.3 LOPD reguló un segundo grupo de datos especialmente protegidos, los relativos a la salud, al origen racial y a la vida sexual. La diferencia entre ambos grupos reside en el modo del consentimiento. Mientras que para el primer grupo (ideología, creencias, religión y afiliación sindical) se requería el consentimiento expreso y por escrito, para el segundo grupo (origen racial, salud, vida sexual) se precisó que el consentimiento sería expreso, sin requerir forma escrita obligatoria. El artículo 7.4 LOPD prohibió la creación de ficheros cuya única finalidad sea almacenar datos personales sensibles, se reitera, los referentes a ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual³⁸¹.

³⁸⁰ El antecedente a la regulación que estableció la LOPD se encontraría en la Directiva 95/46/CE, la cual estableció en el artículo 8.1. un régimen especial de prohibición de tratamiento para los datos personales que pudieran revelar el origen racial o étnico, las preferencias o prácticas religiosas, las opiniones o militancias políticas, ideas filosóficas, pertenencia a sindicatos, datos relativos a la sexualidad o a la salud. Los denomina categorías especiales de datos o datos sensibles y debieran ser protegidos por mayores garantías.

³⁸¹ El artículo 7.5 LOPD contiene una curiosidad, por nombrar así una forma de legislar peculiar. Los datos sensibles de infracciones penales o administrativas, debieron contar sin duda con menor conside-

Se exceptuó de la obligación de otorgar el consentimiento por escrito para el mantenimiento de ficheros cuya titularidad sean partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, fundaciones y entidades sin ánimo de lucro que tuvieran por finalidad objetivos en la política, la filosofía, la religión o la sindicalidad, en cuanto a datos relativos a sus asociados o miembros. Pero la cesión de estos datos sería siempre con el consentimiento previo del afectado. Los datos de origen racial, salud y vida sexual sólo podrían ser recabados, tratados o cedidos cuando, por razones de interés general, así se disponga por ley o, como ya se señaló, el afectado consienta expresamente.

También se excepcionó de la prohibición de tratamiento de datos sensibles del artículo 7.6 LOPD cuando el tratamiento de estos datos sea necesario para cuestiones médicas, como prevención o diagnóstico sanitario, tratamiento médico, gestión de servicios sanitarios, bajo el secreto profesional de personal sanitario o personal equivalente en cuanto al deber de secreto. De lógica fue la excepción de tratamiento de datos sensibles para salvaguardar la vida (el interés vital) del titular o de otra persona que en ese momento esté incapacitado para dar su consentimiento. Esta cuestión se volvió a reiterar en el texto del artículo 8 LOPD, que remitió a la legislación estatal o autonómica sobre sanidad en cuanto a tratamiento y cesión de datos de salud.

El nuevo RGPD estipula en el artículo 9.1. la prohibición de tratamiento de categorías especiales de datos personales biométricos, datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la filiación sindical, el tratamiento de datos genéticos, datos relativos a la salud, a la vida sexual o a la orientación sexual de la persona física. Las excepciones se desarrollan en los puntos posteriores del mismo artículo, siendo similares supuestos de excepción que los incluidos en la actual LOPD y su Reglamento, con mención expresa de los datos genéticos y biométricos³⁸².

ración que los otros datos sensibles para el legislador, pues se permitía que fueran normas reguladoras de tipo reglamentario, que especificó el artículo 20 LOPD, quienes las determinaran en cuanto a su inclusión en ficheros de las AAPP.

³⁸² Es una larga lista de excepciones que se transcriben por si son de interés en su novedad legislativa:

-
- a. Cuando el interesado otorgue su consentimiento explícito, salvo que el Derecho de la Unión o de los Estados miembros establezca que la prohibición de tratamiento de alguno de los datos especificados en el artículo 9.1. no puede ser levantada por el interesado.
 - b. Cuando el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos del interesado o del responsable del tratamiento en los ámbitos laborales, en la Seguridad Social o en la protección social.
 - c. Cuando sea necesario realizar un tratamiento de datos para el interés vital del interesado, en caso de que no esté capacitado para otorgar su consentimiento.
 - d. Cuando el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
 - e. El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
 - f. el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
 - g. El tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
 - h. el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
 - i. El tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,
 - j. El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

Este tipo de datos, que tienen una especial relevancia respecto a la intimidad y la libertad de la persona, son objeto de especial atención por parte de la normativa sobre protección de datos personales. Si nos atenemos, sin embargo, a las consecuencias del tratamiento indebido de conjuntos dispersos de datos unificados por los sistemas actuales de las tecnologías de la información, cualquier grupo de datos que conforme una identificación del individuo en cualquiera de sus facetas puede tener resultados imprevistos para su intimidad o para su desarrollo social, en definitiva, para su libertad y sus DDFF. Por ejemplo, una simple foto con nombre y apellidos en una situación determinada o en un lugar específico (manifestación política o sindical, fiesta gay o club nocturno, procesión de Semana Santa o de fiestas patronales, hospital rodeado de amigos en conductas determinadas y explícitas) se convierte en una fuente de datos que no se había previsto, sobre salud, vida sexual, ideología, religión o sindicalidad; por supuesto, origen étnico (nadie puede ocultar su tipología racial evidente) Una simple foto puede causar estragos para el titular de esos datos en un futuro, pues se toma en un momento en que no se tiene conciencia de que se aporta información para otros fines que no son el acto presente. Bien lo reflejó la *Guía del Ciudadano* de la AEPD³⁸³ cuando manifiesta que la publicación de una foto (que no es un *dato especialmente protegido* de forma específica en la LOPD) puede causar daños a la imagen, reputación o intimidad de su titular, pues los datos en *internet*, cuya disposición para cualquiera es bastante fácil y que escapan al control de la persona que los *subió*, son muy difíciles de eliminar con posterioridad. Si las imágenes son de

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

³⁸³ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Guía para el ciudadano. El derecho fundamental a la protección de datos."]. pág. 30 y ss.

menores o de discapacitados, la cuestión se complica aún más. Por eso, un simple dato de imagen, una foto, se transforma con facilidad en dato sensible con imprevisibles consecuencias en la práctica.

Las consecuencias del tratamiento de datos también pueden violar el artículo 15 CE, el cual establece que *todos tienen derecho a la vida y a la integridad física y moral, sin que, en ningún caso, pueden ser sometidos a tortura ni a penas o tratos inhumanos o degradantes*. Como se apuntó en los comentarios relativos al consentimiento de los menores, el uso de grabaciones, páginas web, grupos sociales y demás herramientas que sirven para comunicarse, se convierte en instrumentos de degradación personal de mofas o de comentarios insultantes o degradantes; estos usos se pueden encontrar dirigidos a cualquier ciudadano, convirtiéndose en una auténtica tortura para las personas objetivo de estas acciones³⁸⁴.

³⁸⁴ Hay casos en casi todos los ámbitos personales: trabajo, deporte, escuela, universidad, en menores y en personas de edad, sin diferenciación de ingresos económicos, situación social o personal, como salud, estado civil. Se comentarán algunas de estas circunstancias. Una prueba específica que se practica actualmente y que apunta la AEPD: para ser eficaz en una red social la persona titular de los datos debe identificarse cuanto más mejor. Las empresas de redes sociales (Facebook, fijémonos) utilizan esos datos para ofrecernos productos a través de anuncios dirigidos a lo que denominan perfil y que, como ya se ha apuntado en esta tesis, comienzan a ser conductas; vemos que los *banners* (la publicidad) está completamente dirigida a nuestra edad, nuestros intereses, nuestra tipología sexual (mujer, hombre, heterosexual, gay, lesbianas, etc.) nuestro nivel de estudios, nuestros contactos y comentarios. Cualquier ciudadano puede realizar una prueba muy divertida: al cambiar determinados aspectos de su perfil social va a cambiar la publicidad. Si el estado civil aportado es soltero/a, aparecerá muy posiblemente la publicidad de conocidas agencias de contactos afectivos y que cambiará al señalar casado/a. Si se añade con hijos, aparece una publicidad relativa a los hijos y sus edades (diferentes artículos de consumo en función de la edad) Si cambiaba los intereses o los gustos, la publicidad cambiaba también. Se añade a título de comentario que Facebook no gozó del reconocimiento de los inversores hace unos años, cuando salió a bolsa en EEUU, precisamente porque no dejaba de ser una empresa de alquiler de espacios publicitarios en páginas web o *banners*. Con el paso de los años, se consolidó como una buena inversión por la información masiva que aporta sobre conductas o tendencias sociales, lo cual es denominado por las nuevas tendencias económicas como el “oro del siglo XXI”

Las estrategias de la denominada *viralidad informativa* se encargan de propagar la información que contienen las redes sociales. Si no se desea por el usuario la exposición de información es necesario mucho tiempo y dedicación, pues la protección de información no se establece hasta este momento por defecto. Para las empresas publicitarias es muy importante que se difundan los denominados *me gusta (likes)*, e incluso ofrecen motivaciones o premios para quien lo realiza. Como bien definió la *Guía del ciudadano* de la AEPD, quien se registra en una red social cree que es de forma gratuita, pero no sabe que el precio del uso de toda esa infraestructura (sensacional y muy costosa) es la información personal, los datos que proveen de suficiente información conductual como para poder tener un negocio muy lucrativo sobre esa base. Esa es la transacción. En otro epígrafe también se ha comentado levemente acerca de la valiosa información que se aporta a los servicios de inteligencia en general con todos los datos volcados en las redes sociales. La pregunta se centra en el dudoso tratamiento de datos que otras organizaciones realizan al margen de los Estados democráticos.

Los artículos comentados de la LOPD y del RGPD vinculan directamente el derecho a la protección de datos personales con la CE, en su artículo 16, pero también con el artículo 14, por el que empieza el Capítulo II, Derechos y Libertades, con casi idéntica denominación que el Título I, del que forma parte, De los Derechos y Deberes Fundamentales. El texto del artículo 14 CE estableció que *los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social*. El régimen especial de protección de los datos sensibles se podría ampliar a la protección contra la discriminación, y, por tanto, a la protección del derecho fundamental de igualdad con facilidad. Con ello, en estos momentos actuales, que los constitucionalistas no pudieron analizar, se proveería de protección jurídica efectiva a múltiples situaciones. El punto más llamativo, el artículo 17 CE, que en una sola frase enunció que *toda persona tiene derecho a la libertad y a la seguridad*, es de suma trascendencia. Para la CE la seguridad y la libertad se desarrollan como derechos vinculados. Ante las intromisiones provocadas por el uso de los medios informáticos y de teleco-

municaciones, esa seguridad se presenta completamente mermada (en parte por el propio titular de los datos personales, que no está exento de responsabilidad) y la libertad está seriamente condicionada.

Lo más curioso es que la protección de todos estos DDFF y libertades públicas expuestos, más todas las posibles transgresiones de los DDFF del Título I de la CE³⁸⁵, se encuentran en las competencias de la AEPD, como primera instancia ante posibles agresiones a través de los nuevos medios de comunicación e información. No es el TC, no son los Tribunales ordinarios, es una Agencia bajo el Derecho Administrativo, cuya organización dependería del poder político. Es el organismo de protección y casi regu-

³⁸⁵ Gozan de especial protección, por eso ante su transgresión recaban la tutela establecida en el artículo 53.2 CE, por un procedimiento basado en los principios de preferencia y sumariedad ante los Tribunales ordinarios. Los artículos 53.2 y 161 de la CE protegen igualmente estos derechos y libertades con el Recurso de Amparo ante el TC. Se puede interponer Recurso de Inconstitucionalidad contra las leyes y normativas con fuerza de Ley que vulneren los derechos y libertades del artículo 16, según el artículo 53.1 y 161.1. a) CE. Sólo por Ley puede regularse el contenido de estos artículos del Título I CE (artículo 53.1) Además, el artículo 16 está dentro de los derechos cuyo desarrollo normativo sólo puede realizarse por Ley Orgánica con mayoría absoluta del Congreso (artículo 81.2 CE) No se pueden regular estos contenidos por Decreto-Ley (artículo 86.1 CE) Todos los derechos establecidos en el Capítulo II del Título I CE gozan de vinculación directa de las AAPP (sin mediación del legislador) como dictamina la STC 80/1982. El artículo 168 CE establece además la vía de reforma agravada para este tipo de derechos, con la aprobación de 2/3 de votos del Congreso de los Diputados y del Senado, disolución de las Cortes Generales, celebración de elecciones generales, nueva ratificación de la propuesta por otros 2/3 de ambas Cámaras y la ratificación de la propuesta por Referéndum. Se va a comentar algo que se considera por esta tesis importantísimo dentro del Derecho Constitucional español. La CE se considera en la línea del llamado “indiferentismo ideológico”, pues admite cualquier ideología, con el único límite del orden público. En otros ordenamientos, como la Constitución alemana, se prohíben expresamente las ideológicas contrarias a los principios constitucionales. La CE permite la defensa pública de ideologías contrarias al ordenamiento español, “inconstitucionales”, siempre que se respeten los supuestos punibles o no se incurra en ellos. El TC constata esta línea en numerosas Sentencias, alegando que España no impone una militancia o ideología a favor de la CE y el Ordenamiento Jurídico Español. La CE, por todo ello, ampara también a quien la niega o la ataca, con el límite de la lesión efectiva de bienes o derechos. La CE permite, por tanto, las ideologías contrarias a la democracia. Se citan como ejemplos las siguientes Sentencias del TC: 13/2001, 48/2003, 235/2007, 12/2008, 101/1983, 122/1983, y se menciona la Ley Orgánica 6/2002.

lación, porque como se ha visto ya en los epígrafes anteriores, es la AEPD la que muchas veces suplió las ausencias de la LOPD y su Reglamento, en un primer nivel.

La LOPD no trató solamente de proteger al titular de los datos en los supuestos del artículo 16.2. CE. Y reiterando la idea, toda aportación de datos, en especial la visual, convierten un grupo de datos, que aisladamente no están catalogados como de especial protección constitucional, en datos sensibles y trascendentes en cuanto al daño que sufre la persona cuando se utilizan para transgredir y agredir a otro, con ánimo o sin ánimo de realizar el daño. El transgresor que vulnera la protección de datos ejerce generalmente su derecho fundamental a la libertad, sea libertad de expresión, sea libertad de información, sea de comunicación en la sociedad, sería larga la lista de ejemplos que se dan en la actualidad. La cuestión se complica si es el propio titular quien puso en riesgo la protección de sus datos personales, que pueden llegar a ser sensibles con facilidad a través de la tecnología. En ese caso, ejerce una libertad sin saber las consecuencias futuras de su conducta, ni tan siquiera puede prever qué resultado tendrán todos esos datos ni por quién serán tratados para qué finalidad.

8.1. La ponderación como sistema de solución de conflictos entre DDFF

Ante esta situación, completamente cambiante e inestable, se tiene una contradicción evidente entre las normas entre sí (DDFF y normativa a aplicar) y entre la realidad y el derecho. La doctrina del derecho conoce ese fenómeno jurídico como *antinomía o contradicción normativa*, la cual se produciría cuando en un mismo sistema de normas existen incompatibilidades imputables a la misma situación de hecho o fáctica³⁸⁶. Esas incompatibilidades no podrían ejercerse al mismo tiempo en la misma

³⁸⁶ PRIETO SANCHÍS, L., "Observaciones sobre las antinomias y el criterio de ponderación", , nº 11, 2000. "Suele decirse que existe una antinomia o contradicción normativa cuando dentro de un mismo sistema jurídico se imputan consecuencias incompatibles a las mismas condiciones fácticas, es decir, cuando en presencia de un cierto comportamiento o situación de hecho encontramos diferentes orientaciones que no pueden observarse simultáneamente. Por ejemplo, una norma prohíbe lo que otra

realidad. La cuestión de las antinomias en el Derecho se considera muy antigua y su frecuencia estuvo en relación con la voluntad y capacidad legisladora. La personificación del Estado como algo supremo y omnipotente, infalible, en el que muchos creen, se transformaría en esa suerte de fe, más que de razón y comprensión concluyendo que lo absoluto no existe. El Derecho positivo, el derecho regulador, sería un conjunto de actos de producción normativa a lo largo del tiempo, que reflejaría en el futuro los intereses e ideologías de sus creadores, *humanos y falibles*. Aunque las antinomias se pueden presentar como patologías para un jurista, serían una consecuencia natural – irremediable- del dinamismo del sistema jurídico, en su vertiente positiva, al igual que en su vertiente negativa de análisis supondrían la consecuencia también natural de una irracionalidad legislativa, pues muchas antinomias podrían evitarse, evitando generar legislativamente normas contradictorias con otras anteriores o eliminando del sistema jurídico a las normas que se contradicen. Esas contradicciones se encontrarían presentes en todos los sistemas jurídicos y frente a todos los derechos, en especial los DDFF. Para el análisis de esta tesis, el derecho fundamental a la protección de datos se encontraría en -aparente- antinomia o confrontación frente a otros DDFF. En la resolución de las antinomias, la doctrina del Derecho utiliza las herramientas más diversas, como son las que PRIETO SANCHÍS enumeró, como criterio jerárquico, por el cual la ley superior deroga a la inferior; también el criterio cronológico, en el que la ley posterior deroga a la anterior y el criterio de especialidad, en el que la ley especial deroga a la ley general. Los dos primeros criterios no se podrían aplicar cuando la antinomia se produjese en la misma norma³⁸⁷. Tomando el criterio de especialidad se

manda, o permite no hacer lo que otra ordena, etc.; desde la perspectiva del destinatario del Derecho, el caso es que no puede cumplir al mismo tiempo lo establecido en dos normas: si cumple la obligación vulnera una prohibición, si ejerce un derecho o un permiso incurre en ilícito.” A pie de página, el autor cita a CAPELLA “con lo que el resultado de la acción –dado que la norma permisiva es un compromiso de no interferencia de la autoridad- puede aparecer una contradicción normativa entre la prescripción de sancionar al contraventor y ese compromiso de no interferencia”

³⁸⁷ El autor deja de lado el problema de contradicciones dentro de una norma como la Constitución, pues es una tesis que no quiere analizar en este análisis de referencia. Entonces, para Prieto Sanchís,

puede diferenciar en este punto entre las *antinomias contingentes o en concreto*, que son externas o propias del discurso de aplicación y *las antinomias en abstracto*, internas o propias del discurso de validez, la cuales se distinguirían porque al pretenderse aplicar una de ellas nacería un conflicto con la otra.

En el caso de las antinomias contingentes, en concreto o externas, *no se definiría abstractamente la contradicción por la norma ni existiría otra para su resolución*. Sólo cuando el caso concreto fuera detectado, podría el sistema jurídico advertir la concurrencia o contradicción de las normas, y sólo en ese momento se provee a la solución, en favor de una u otra, solución que no vincularía al sistema, porque en otro caso distinto y en otro momento temporal pudiera tener otro resultado. En esos casos, La colisión normativa se descubre y se resuelve ante el caso concreto, y los casos son imposibles de determinar a priori³⁸⁸.

En el caso de las antinomias internas o en abstracto se produce una *superposición conceptual entre las normas*, por la que al aplicar una se genera el conflicto con la otra. En este caso, el sistema jurídico tendría la posibilidad de aproximar con antelación una solución, sin estar siempre a la espera del caso concreto³⁸⁹.

Esta tipología de conflictos normativos se presentaría como frecuentes en constituciones que tienen un importante contenido sustantivo y densidad material que no

queda el criterio de especialidad para resolver ciertas antinomias, lo cual puede no resultar cuando no es posible una relación de especialidad entre dos normas teóricamente contradictorias.

³⁸⁸ Se cita a GÜNTHER: como “razones *prima facie* relevantes” en base a la descripción completa de la situación.

³⁸⁹ PRIETO presenta un ejemplo muy actual, sin que tenga como tema la protección de datos, pero muy gráfico: “una antinomia es interna o en abstracto cuando los supuestos de hecho descritos por las dos normas se superponen conceptualmente, de forma tal que, al menos, siempre que pretendamos aplicar una de ellas nacerá el conflicto con la otra. Por ejemplo, una norma que prohíbe el aborto y otra que permite el aborto terapéutico se hallan en una posición de conflicto abstracto, pues la especie de abortos terapéuticos forma parte del género de los abortos; en consecuencia, o una de las normas no es válida o la segunda opera siempre como regla especial, es decir, como excepción constante de la primera.” Se utiliza por el autor el ejemplo de KELSEN en un constitucionalismo denominado clásico por la doctrina.

existía en otros momentos del constitucionalismo más clásico. Como ejemplo, el conflicto mencionado entre el derecho al honor del artículo 18 CE, que se pudiera extender al Derecho a la protección de datos en el mismo artículo, y el derecho a la libertad de expresión consagrada en el artículo 20 CE. Ambas normas serían válidas y coherentes en un plano abstracto e interno, pero entran en colisión frecuentemente en el plano real o externo. Es más, sólo en cada caso concreto muchas veces se acierta con una solución, que no tiene porqué ser aplicada en otro momento, aunque el supuesto sea similar. Algunos conflictos pueden verse como necesarios, por ejemplo, la contradicción entre el artículo 9.2 CE y el artículo 14 CE, cuyo texto apunta a la igualdad ante la ley³⁹⁰.

Se pretende extender estas ideas de la doctrina jurídica para el Derecho a la protección de datos pues, en primer lugar, los avances tecnológicos, el medio o la herramienta que sirve de base al tratamiento de datos personales, no son previsibles desde el presente, ni lo fueron muchas veces en el pasado. *En abstracto* se podría concebir soluciones a situaciones básicas y en concreto, de forma eficaz y eficiente, sería posible si se involucraran en la solución los profesionales adecuados, aportando una de las cuestiones que el legislador parecía ignorar, cual es el fuerte componente de conocimientos técnicos necesarios para la protección de los datos. Esta idea se extenderá ampliamente en el epígrafe dedicado a la autorregulación en materia de protección de datos.

³⁹⁰ Texto del artículo 9.2 CE: Corresponde a los poderes públicos promover las condiciones para la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social. Texto del artículo 14 CE: Los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social" PRIETO afirmo: "Lo que ocurre con el principio de igualdad es que la CE no suministra la descripción de las situaciones de hecho que imponen, como razón definitiva, un tratamiento jurídico igual o desigual; no sabemos, desde la CE, qué personas y circunstancias, ni a efectos de qué, han de ser tratados de un modo igual o desigual. Esto no se puede resolver en abstracto, sino en presencia de los casos de aplicación.

Por otro lado, el conflicto entre DDFF resultaría irremediable, pero ello no significa que el conflicto fuera negativo, sino que podría ser interpretado como un signo de evolución social, de avance de nuestra civilización e incluso de la evolución como especie, como seres humanos³⁹¹. El ciudadano ejercería sus DDFF como bienes jurídicos “cuya protección resulta necesaria para lograr el pleno desarrollo de la personalidad, y cuyos perfiles se revelan atendiendo a las circunstancias reales de la vida humana.” Es la denominada por la doctrina como *nueva concepción* de los DDFF, en la que la libertad se asienta como la infraestructura de todos los DDFF, el modo en que se ejercen por sus titulares *en la sociedad*, la cual aportaría el respeto a su ejercicio con el instrumento de la norma jurídica. Los DDFF son bienes jurídicos que necesitan de protección para desarrollarse por sus titulares, no deberían considerarse en una sociedad avanzada como *esferas de libertad vacías de contenido*³⁹². Su ampliación a todos los seres humanos se convertiría en una tendencia imparable con los vehículos comunicativos y tecnológicos actuales.

El conflicto solamente debería tener una solución ante el caso concreto. Porque se está hablado de principios y en estos casos los principios “se caracterizarían porque nunca son mutuamente excluyentes en el plano abstracto y, si llegasen a serlo, se convertirían en reglas; (dejarían de ser principios, derechos fundamentales) sus eventuales contradicciones no desembocan en la declaración de invalidez de uno de ellos, ni tampoco en la formulación de una cláusula de excepción en favor de otro, sino en el establecimiento caso por caso de *una relación de preferencia condicionada*, de

³⁹¹ “Siempre que deseemos construir igualdades de facto habremos de aceptar desigualdades de iure”, afirmo PRIETO en cuanto al artículo 9.2 y el artículo 14 CE. La interpretación de su afirmación no se dirigiría hacia un resultado negativo. Aun siendo cierto que a lo largo de la Historia toda crisis o situación conflictiva tuvo un precio en cuanto a bienestar, vidas humanas, o derechos, no quiere decirse que en la actualidad la especie humana, a través de nuestra civilización, no fuera capaz de superarse, eliminando la ecuación que propuso PRIETO.

³⁹² DE DOMINGO, T., *¿Conflictos entre derechos fundamentales?*, Madrid, 2001, pág. 364 y ss. Los antecedentes a la evolución de la concepción de los DDFF son la consideración jurídica de la dignidad humana, el reconocimiento del libre desarrollo de la personalidad, la dimensión institucional de los DDFF, la garantía del contenido esencial, entre otras manifestaciones.

manera que en ocasiones triunfará un principio y otras veces su contrario.”³⁹³ Esta es la *fisionomía de principios* que se consideraría como operante entre DDFF cuando en su aplicación entrase en conflicto con otros derecho o bienes constitucionales; también cuando se limitasen estos principios por el legislador. Su visión significa admitir que “entre el derecho y su límite se entabla un verdadero conflicto, de manera que sus respectivos supuestos de hecho presentan un ámbito de validez parcialmente coincidente; y que dicho conflicto no puede resolverse mediante un criterio de especialidad.” Otras posiciones son las que consideran que los DDFF están perfectamente delimitados desde la CE, existiendo unos límites inquebrantables, funcionando como reglas a las que sería de aplicación el criterio de especialidad³⁹⁴.

PRIETO SANCHÍS pareció no compartir la doctrina que pasó a denominar *teoría estrecha del supuesto de hecho de los derechos fundamentales*. Sería una visión por la cual se podría “dibujar con precisión el contenido efectivo de cada derecho fundamental o las modalidades específicas de su ejercicio, excluyendo del ámbito protegido aquellas conductas que sean *además* otra cosa (...) o que entren en colisión con normas generales”³⁹⁵.

³⁹³ Obra citada, página 14-15. “O bien la ley o medida limitadora penetra en el recinto prohibido y entonces es inválida, o bien no lo hace y entonces el asunto nada tiene que ver con el régimen de los derechos”

³⁹⁴ El autor cita a I. de OTTO, “La regulación del ejercicio de los derecho y libertades”; Martínez Pujalte, “La garantía del contenido esencial de los derechos fundamentales”; Gavara de Cara, “la garantía del contenido esencial de los derechos fundamentales”, ente otros autores. Recoge en esa nota a pie de página una frase de Martínez Pujalte: “más allá de los contornos que los delimitan no puede existir protección constitucional del derecho fundamental y, en cambio, dentro de ellos la protección constitucional es absoluta”.

³⁹⁵ PRIETO SANCHÍS, L., “Diez argumentos sobre los principios”, , nº 26, 1996. El análisis sería un resumen de diferentes tendencias sobre el concepto de principio o derecho fundamental, desde la perspectiva de varios autores, con una conclusión lógica: “la existencia de principios en un sistema jurídico no convierte a éste en ningún sucedáneo de la moralidad. Los principios, si son llamados generales del Derecho, reproducirán sin más el mérito o el demérito del ordenamiento que reflejan y del que se inducen; y si son principios explícitos, constitucionales, legales o jurisprudenciales, tendrán el valor moral que se deduzca del juicio crítico o racional sobre el contenido de los mismos. Definicionalmente,

En el sistema jurídico existen normas que conviven en su vertiente abstracta, pero que en determinados supuestos fácticos se contradicen y no resultarían eficaces los medios para la resolución de las antinomias, las cuales suelen ser frecuentes en la esfera constitucional, puesto que en los DDFF no existen los criterios de jerarquía de los derechos ni tampoco la prelación de los mismos por cronología. Las Constituciones actuales son textos con predominio de contenido material de principios y derechos sustantivos, no son documentos donde se vierten contenidos morales o de filosofía política.³⁹⁶

El derecho a la protección de datos, como derecho fundamental, se encuentra dentro de estas contradicciones; la práctica empresarial y ciudadana frente a la protección de datos personales supone cada día una serie de incidencias sin límite, como igualmente entran en conflictos e incidencias los medios tecnológicos por los cuales se desarrollan gran parte de las actividades que atañen a los mencionados derechos, tanto al derecho a la protección de datos, como a todos los derechos implicados en cualquier conducta, expresión de la misma, intereses tanto empresariales como privados, valoraciones de esa misma conducta con incidencias en todos los derechos y en todos los planos de la personalidad individual, aunque también con fuerte incidencia en valoraciones colectivas (valoración, por ejemplo, de la imagen de una empresa deter-

los principios no garantizan la conexión del Derecho con la moral en el sentido de una moral buena o correcta, sino acaso únicamente la conexión con la llamada moral social mayoritaria o del grupo hegemónico, siempre más o menos presente en el orden jurídico". Contrastó sus ideas con las de ALEXY, R., *Teoría de los derechos fundamentales (Theorie der Grundrechte, 1986)*, Madrid, 1993. considerando la teoría amplia del supuesto de hecho en función del problema entre DDFF del autor alemán, el cual debería ser tratado como un conflicto entre bienes constitucionales, "como un conflicto entre unas razones que abogan en favor de la libertad individual y otras que lo hacen en favor de su restricción" Al resultado del conflicto se llegaría por la ponderación.

³⁹⁶ Citas en página 19, obra citada de PRIETO SANCHÍS. "documentos con un fuerte contenido material de principios y derechos sustantivos que no responden a un esquema homogéneo y cerrado de moralidad y de filosofía política". El autor, a pie de página, consideró que tiene una concepción amplia de los derechos (se supone que habla de los derechos fundamentales), y, por tanto, consideró preferible entender que "todo tipo penal puede representar en principio un límite a la libertad constitucional"

minada en *internet* y en los medios, que tiene una incidencia directa en su desarrollo empresarial y en el trabajo de sus empleados)

*La ponderación es una forma de razonamiento o razonabilidad, de forma proporcionalizada.*³⁹⁷ *Es aplicable a normas que son iguales en grado y que están en conflicto.* Si existiera prelación o jerarquía, no estarían en conflicto, puesto que ya tendrían un criterio para resolverlo. Entre DDFF no existe jerarquía. El TC lo afirmó en varios de sus pronunciamientos, conjugando DDFF o libertades en conflicto y ponderando su eficacia recíproca, generando un orden de preferencia en cada caso concreto³⁹⁸. Ningún principio se declararía inválido porque está en ese momento en conflicto, sino que ambos principios o DDFF se preservan en lo abstracto, aunque en cada caso concreto se reconozca la primacía de uno sobre otro. La tarea de ponderación se atribuye a los jueces, al menos en el ámbito constitucional de derechos fundamentales y libertades públicas. El legislador no debería ponderar, pues la posible ponderación legislativa no elimina el conflicto entre principios a través de una norma general, pues si así fuera, se tendría un poder constituyente, al atribuir a una norma un rango mayor que a otra; ese poder constituyente no pertenece al legislador ordinario. La ponderación se muestra en la práctica, en los casos concretos, en los que se somete a un juicio conductas de particulares o de poderes públicos. El legislador se mueve dentro de la Constitución, no la valora, no la interpreta. El juez ordinario, no sólo el juez constitucional, puede ponderar, pues *“detrás de toda regla late un principio constitucional.”*³⁹⁹

³⁹⁷ Obra citada de ALEXY, página 161. la ponderación como una regla: “cuanto mayor sea el grado de la no satisfacción o de afectación de un principio, tanto mayor tiene que ser la importancia de la satisfacción de otro”

³⁹⁸ Obra citada de ALEXY, página 170, se cita a GUASTINI, *“Los principios del derecho positivo”*, Esta “jerarquía móvil es un concepto muy acorde con el derecho a la protección de datos personales. No resulta de un *ajuste a medida* para resolver un conflicto. Se trata de solucionar con el sentido común lo que un gran surtido inefectivo de normas no consigue, con las herramientas de los derechos fundamentales, los principios que informan un sistema de normas efectivas y respetadas.

³⁹⁹ Página 22, obra citada de PRIETO SANCHIS. En otra visión de la doctrina, el legislador sí es intérprete y pondera la norma. En estas ideas se ha optado por la doctrina del autor Prieto Sanchís.

La ponderación no se muestra sólo en la práctica como sentido común o racionalidad, tiene una cuidada elaboración en la Teoría del Derecho y la Jurisprudencia del Tribunal Constitucional. En la STC 66/1995, de 8 de mayo, el Tribunal estableció cuatro puntos definitorios para generar una ponderación adecuada⁴⁰⁰. En primer lugar, que la medida enjuiciada presente un fin constitucionalmente legítimo como fundamento de la interferencia en la esfera de otro principio o derecho. En segundo lugar, que se acredite la adecuación, aptitud o idoneidad de la medida objeto de enjuiciamiento en orden a la protección o consecución de la finalidad expresada. En tercer lugar, que se demuestre la necesidad de la intervención lesiva para un derecho o principio constitucional. Se debe demostrar que no existe otra medida a tomar que resulte menos gravosa o restrictiva. Aquí los jueces ejercen un *juicio de ponderación argumentado*, que excede un tanto del papel neutral o pasivo que le da el sistema jurídico democrático. Por último, que exista un juicio de proporcionalidad en sentido estricto, lo cual resume los requisitos anteriores. Los jueces deben acreditar la existencia de *un equilibrio entre los beneficios que se obtienen al limitar un derecho fundamental para obtener beneficios protegiendo otro, aun dañándolo o lesionando ese derecho, para la consecución de una finalidad legítima*.

El juicio de ponderación es, sin duda, un *juicio valorativo y con carácter discrecional*. Ello no sería sinónimo de irracionalidad o subjetivismo. Este asunto podría ser una vía de salida para el *decisionismo y la subjetividad* en detrimento de la potestad legislativa y, por tanto, de la representación de la voluntad popular, del pueblo soberano, que es el protagonista de las decisiones legislativas. Este punto es referenciado con HABERMAS y su consideración de los DDFF como bienes o valores que han de ser pon-

⁴⁰⁰ La STC 66/1995 atendió un Recurso de Amparo promovido por la Federación de Banca, Ahorro, Seguros y Oficinas de la Unión General de Trabajadores (FEBASO-UGT) contra la Sentencia de la Sala de lo Contencioso-Administrativo del TSJM (Tribunal Superior de Justicia de Madrid, de 04 de junio de 1992, sobre prohibición de concentración; dicha Sentencia confirmaba la Resolución de la Delegación del Gobierno de Madrid, de 25 de mayo de 1992. Los convocantes desean realizar una manifestación en la Plaza de Canalejas de Madrid y la Delegación del Gobierno no se lo admite, por constituir una zona de tráfico denso de vehículos y además estar en obras, por lo cual se produciría un colapso total de la circulación en todo el Centro de Madrid.

derados en cada caso concreto, convirtiendo al Tribunal en un *negociador de valores*, en una suerte de *instancia autoritaria* que “invade las competencias del legislador y que aumenta el peligro de juicios irracionales porque con ello cobran primacía los argumentos funcionalistas a costa de los argumentos normativos”⁴⁰¹.

Esta teoría, compartida por parte de la doctrina, implica que se tenga una delimitación tan rigurosa de los DDFF que no sería necesaria la ponderación. Los conflictos serían solo apariencia, porque siempre existe un derecho o un principio como solución, que excluye a otro conflicto o principio⁴⁰². Más sólo sería una criticable comprensión de las antinomias externas, las situaciones externas en su argumentación, propias del discurso de aplicación. No existe una prelación en los DDFF, por tanto, sólo existirá una *adecuación* para solucionar y/o regular cada caso concreto. La ponderación hace posible un *juicio para buscar la norma más acertada*⁴⁰³ Esto no lo acep-

⁴⁰¹ SANCHÍS analiza a HABERMAS, J., *Factividad y validez*, Madrid, 1998, pág. 332-333. “Se trata de hallar entre las normas aplicables prima facie aquella que se acomoda mejor a la situación de aplicación, descrita de la forma más exhaustiva posible desde todos los puntos de vista”. Por ejemplo, se comenta el Recurso de Amparo constitucional. Este recurso consiste en una “argumentación deontológica que sólo permita para cada caso una única solución correcta, lo que implica concebir los derechos como auténticos principios, no como valores que puedan ser ponderados en un razonamiento teleológico”

⁴⁰² Se citan los autores siguientes: MARTÍNEZ PUJALTE, “La garantía esencial de los Derechos Fundamentales”; CIANCIARDO, “El conflictivismo en los Derechos Fundamentales”; RODRÍGUEZ-TOUBES MUÑOZ, “Principios, fines y Derechos Fundamentales”. El conflicto “no puede ocurrir –y si ocurre será sólo una apariencia superable- que un mismo caso quede comprendido en el ámbito de dos principios o derechos tendencialmente contradictorios; siempre habrá uno más adecuado que otro El autor hace una crítica a Habermas desde el plano de la aplicación de la norma, que no puede ser igual que el plano de la validez en abstracto. Un principio o derecho fundamental no sea más o menos que otro, tajantemente, sin posibilidad de variación, sino que será “adecuado o inadecuado para regular el caso concreto”. y, al parecer, incluso podemos encontrarlo sin recurrir a las valoraciones propias de la ponderación.”

⁴⁰³ “La ponderación no representa un esfuerzo para la armonización de lo tendencialmente contradictorio, tarea que no hace ninguna falta, sino un juicio orientado a determinar qué norma debe regular un caso que, en principio, puede ser subsumido también en otra norma de sentido contrario. Un juicio orientado, pues, a la búsqueda de la norma más adecuada, por más que esa búsqueda permita distintas argumentaciones no irracionales y permita, por tanto, soluciones dispares.” Importante frase del autor

taría la teoría haberniana, pues se basa en una “*defensa de la unidad de solución correcta*”.

Es precisamente para los casos en que es necesario la prevalencia de un derecho fundamental ante otro derecho fundamental donde la ponderación adquiere su máximo nivel⁴⁰⁴. Así lo expresó también ALEXY, con la diferenciación entre casos potenciales y casos actuales, reales, en los que se dirime la posición de un derecho fundamental. Será en la práctica siempre donde se apreciaría la eficacia de los DDFF, pues en otro caso, estaríamos en un listado de derechos sin más pretensión que la retórica, sin aplicación práctica y, por tanto, ante un Estado sin libertad⁴⁰⁵. La ponderación se

español citado. Muy aplicable al tema del derecho fundamental a la protección de datos y todos los derechos que se implican en su regulación. El profesor PRIETO SANCHIS también generó una abundante bibliografía sobre las tesis de DWORKIN, y su distinción entre principios y normas. Su sistemática se dirigiría al derecho anglosajón, menos orientada al derecho europeo, con todas sus distinciones sistemáticas. Se eligió este trabajo de Prieto Sanchís como referencia por considerarlo muy aplicable al derecho fundamental a la protección de datos, pero existen otros trabajos del profesor interesantes y representativos de su obra, que se mencionan en la bibliografía.

⁴⁰⁴ Se puede concluir que “no hay riesgo de anarquismo jurídico”, porque, según PRIETO SANCHÍS, “La virtualidad de la perspectiva adoptada -por él- es que en la zona de penumbra donde resulta discutible si una conducta está o no en principio incluida dentro del contenido de un derecho, se impone un ejercicio de justificación o ponderación, esto es, de racionalidad antes que de autoridad”

⁴⁰⁵ PECES-BARBA, G., “Crítica a Prieto Sanchis en su obra “Principios y normas”. Problemas de razonamientos jurídicos.”, , Madrid, 1992.

http://e-archivo.uc3m.es/bitstream/handle/10016/11676/sobre_Peces_1993.pdf?sequence=1 En esta pequeña obra que se referencia, concluye el autor que estos razonamientos sobre principios y normas le parecían una excelente construcción desde un positivismo renovado que denomina “normativismo realista, capaz de integrar en el viejo esquema kelnesiano, corregido y remozado, la función de las normas principales y su papel en el funcionamiento de la maquinaria jurídica” aunque el autor añadió que no creía que fuera suficiente una reflexión racional de los juristas y de los operadores jurídicos. Añadió la necesidad de un “progreso sobre las expresiones desnudas de la fuerza, y los modernos sistemas democráticos suponen un evidente progreso en la racionalidad de sus ordenamientos jurídicos iluminados por la ética pública de la modernidad” No todo es bienaventuranza en las palabras de esta crítica. Añade un comentario al final, en la página 436, que también incumbe a la realidad: el poder no puede ignorarse. Y lo expresa con las siguientes palabras: “en última instancia, no pueden sustraerse (los ordenamientos jurídicos mencionados en la frase anterior) al papel decisivo de la voluntad de los

reitera en todas las resoluciones judiciales, ofreciendo una actividad constatable de adecuación de las normas a la realidad y al caso concreto. Muchas de las manifestaciones del ejercicio de la ponderación por los Tribunales se manifestarán en otros momentos de esta exposición sobre los conflictos entre derechos fundamentales.

8.2. La proporcionalidad, la idoneidad y la intervención mínima como principios para el ejercicio de otros derechos y libertades frente a la protección de datos personales.

Para el sistema jurídico español, como el TC dictaminó en múltiples resoluciones, ningún derecho fundamental puede considerarse absoluto; con el respeto a las garantías constitucionales, un derecho fundamental podría limitarse en su ejercicio para protección de otro derecho fundamental o bien constitucionalmente protegido, límite siempre en referencia al caso concreto, no siendo posible la limitación realizada para un caso aplicable para todos los casos similares ni establecer generalidades⁴⁰⁶. El

que tienen poder de decisión, y van a escoger los argumentos definitivos en que fundar la orientación de la norma." Véase también GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 115. La autora citó a Sanchís en varias de sus obras, se toma como referencia la más reciente.

⁴⁰⁶ En este sentido las STC 110/1984, de 26 de diciembre y STC 143/1994, de 9 de mayo. Véase también MURILLO DE LA CUEVA, P., "La protección de los datos de carácter personal en el horizonte del 2010", *Anuario de la Facultad de Derecho*, nº 2, 2009, pág. 131-142, pág. 139-140. "No deja de ser cierto que siempre que se positiviza un derecho o una institución se produce su incorporación a un conjunto en el que les rodean otros derechos e instituciones que los delimitan y con los que pueden entrar en conflicto. Dejan, pues, de ser absolutos y se transforman, como todos los derechos e instituciones, en categorías circunscritas dentro de unos confines cuya determinación puede, en ocasiones, ser difícil, pero que no dejan de existir por esa razón. No es, pues, desconocida la hipótesis de la devaluación de los derechos en general ni, vistas las particulares circunstancias que acompañan al derecho a la protección de datos en particular, está excluido que la padezca. Y, sin embargo, las amenazas a la dignidad, a la identidad, a la libertad y a la intimidad de las personas que justifican este derecho y explican su recepción en las Constituciones, en las leyes y en la jurisprudencia no han desaparecido. Al contrario,

principio de proporcionalidad realizaría una función limitadora objetiva, para que ninguno de los DDFF reconocidos fuera sacrificado completamente en beneficio de otro. Junto con el principio de proporcionalidad, la ponderación de DDFF se realizaría adecuadamente, pasando a ser la reserva de ley establecida en el artículo 53.1 CE una *reserva de ley proporcionada*⁴⁰⁷.

La idoneidad exige que los medios -proporcionales- sean también los correctos para conseguir el fin perseguido por la norma. El legislador suele adoptar medios adecuados para los fines que desea realizar. Igualmente es considerado el criterio de intervención mínima como indispensable dentro del sistema, pues debe elegirse el recurso menos perjudicial e invasivo de otros derechos para obtener un resultado. Con ambos conceptos se llegaría a lo que ALEXY denominó *optimización relativa a las posibilidades fácticas*, que consiste en *ahorrar costos que pueden ser evitados*. Es en este punto donde ponderación y proporcionalidad se incluyen bajo la Teoría de los Derechos Fundamentales con la misma regla comentada para el principio de ponderación: “Cuanto mayor sea el grado de la no satisfacción o afectación de uno de los princi-

todo apunta que se han incrementado exponencialmente de la mano de las posibilidades crecientes que ofrece la tecnología, entre las que destaca la facilidad creciente de establecer sistemas de video-vigilancia que se hacen, ya no con datos personales más o menos desagregados, sino con imágenes de los afectados en los ámbitos más variados: domicilio, trabajo, vía pública, establecimientos comerciales, lugares de ocio, etc. O los mecanismos que, incorporados a documentos de identidad, hacen posible el seguimiento y localización de individuos y naturalmente, la definitiva superación de la protección que en otro tiempo y respecto de otros peligros podían ofrecer las fronteras estatales.” Murillo de la Cueva se adelantó de nuevo a los legisladores en materia de protección de datos en el año 2009, como la realidad de los hechos ha mostrado. También se recuerda la Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983 que se adopta por nuestro TC en la STC 292/2000 tan claramente. En Alemania se traspasó el principio de proporcionalidad desde las AAPP al Derecho Constitucional. Véase también MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, Madrid, 1996, pág. 118 y ss.. El TC lo considera un principio del Estado de Derecho importantísimo para realizar una ponderación adecuada STC 85/1992, de 8 de junio, FJ4.

⁴⁰⁷ MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, Madrid, 1996, pág. 119.

prios, tanto mayor debe ser la importancia de la satisfacción del otro”⁴⁰⁸. En este sentido, la doctrina estableció también tres sub-principios al principio de proporcionalidad: adecuación, intervención mínima y proporcionalidad en sentido estricto⁴⁰⁹.

La conexión evidente entre el principio de proporcionalidad, la teoría de los principios y los DDFF condujo a la afirmación de que todos los conceptos mencionados se encontrarían íntimamente unidos, aunque sólo fuera por la discusión generada en la doctrina. Algunos autores serían partidarios de lo que denominan *primera tesis de necesidad*, esto es, en torno a una cuestión teórica-normativa y otros autores se centrarían en la existencia de una *conexión necesaria entre los derechos fundamentales y el principio de proporcionalidad o la teoría de los principios*⁴¹⁰. Fue la positividad de los DDFF lo que relacionaría a esos con el principio de proporcionalidad a través de lo que denominaron *test de positividad*. ALEXY rechazó este punto, pues consideró que los DDFF tienen una doble naturaleza. Serían, por una parte, un derecho positivo a nivel constitucional, pero, además, poseerían lo que se denominó la *dimensión ideal*, pues fueron plasmados en la Constitución para transformar los Derechos Humanos en Derecho positivo, a través de la intención del legislador constituyente⁴¹¹. En otra vertien-

⁴⁰⁸ ALEXY, R., *Teoría de los derechos fundamentales (Theorie der Grundrechte, 1986)*, Madrid, 1993, pág. 218.

⁴⁰⁹ MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, Madrid, 1996, pág. 120 y ss.

⁴¹⁰ ALEXY, R., "Los derechos fundamentales y el principio de proporcionalidad", *Revista Española de Derecho Constitucional*, nº 91, 2011, pág. 11-29, pág. 23. El autor cita entre otros a JESTAEDT, M; LERCHER, P; KLEMENTJ.H.

⁴¹¹ ALEXY, R., "Los derechos fundamentales y el principio de proporcionalidad", *Revista Española de Derecho Constitucional*, nº 91, 2011, pág. 11-29, pág. 25. "El carácter ideal de los derechos humanos no se desvanece una vez ellos hayan sido transformados en derecho positivo. Al contrario, los derechos humanos permanecen conectados con los derechos fundamentales como razones en favor o en contra del contenido que ha sido establecido a través de la positivización y como razones exigidas por la textura abierta de los derechos fundamentales. Por lo tanto, la dimensión ideal de los derechos humanos sobrevive, a pesar de su positivización. En respuesta a esto, podría ser elevada la objeción de que la presencia de la dimensión ideal destruye el carácter positivo de los derechos fundamentales. Éste, sin embargo, no es el caso. La tesis de la doble naturaleza exige que se tengan en cuenta seriamente tanto

te, MEDINA GUERRERO, recordó que la Constitución sería una norma peculiar, integrada por *preceptos abiertos e incompletos*, haciendo de la misma una norma flexible en cuanto a los DDFF, por lo que a pesar de la eficacia directa e inmediata de los DDFF consagrados en la CE, resultaría imprescindible la intervención del legislador para conseguir la eficacia de los mismos. Se vinculó la ley y los DDFF a través del ejercicio de regulación del legislador (*decisión política*) pero también el Tribunal Constitucional controlaría la producción normativa a través de la interpretación (*razonamiento jurídico*)⁴¹². *Tanto legislador como Tribunal Constitucional estarán sujetos al principio de proporcionalidad*. El TC utilizó el principio de proporcionalidad de forma fragmentaria a lo largo de su jurisprudencia, la cual se empleó en otras posteriores con mucha frecuencia y que podría ser una forma recurrente de trasladar estos razonamientos a otros DDFF⁴¹³. Hasta la STC 66/1995, de 8 de mayo, el TC no estableció un razonamiento claro respecto al principio de proporcionalidad y los subprincipios de adecuación, indispensabilidad y proporcionalidad en sentido estricto, como medios para conseguir un fin. Con ello, el TC *vinculó la proporcionalidad con la ponderación*, pues a una limitación o restricción de los DDFF le debería acompañar la proporcionalidad en sentido estricto, para que se deriven de su limitación más ventajas que perjuicios⁴¹⁴. Este poder de limitación del TC no debería entorpecer la libertad de configuración política del poder legislativo; por este razonamiento, el principio de proporcionalidad no debería aplicarse estrictamente. Como afirma MEDINA, *el principio de proporcionalidad reclama su utilización proporcionada*⁴¹⁵ y tampoco de-

a la dimensión ideal, así como a la dimensión real del derecho. Ella exige, además, que sea otorgada una prioridad *prima facie* a la dimensión positiva o autoritativa”

⁴¹² MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, Madrid, 1996, pág. 25-26.

⁴¹³ MEDINA GUERRERO menciona las siguientes: STC 90/1983 FJ 2; STC 3/ 1983 FJ 4; STC 46/1984 FJ 2; STC 209/1988 FJ10; STC 158/ 1993 FJ2 entre otras. Obra citada, p. 126 127.

⁴¹⁴ Véase MEDINA GUERRERO, obra citada, p. 136 en cita de la STC 66/1995 FJ5. “la restricción es proporcionada en sentido estricto si es ponderada o equilibrada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto”

⁴¹⁵ Véase MEDINA GUERRERO, obra citada, p. 137-145, el autor cita la STC 19/1998 FJ 8.

bería el TC adoptar el papel que corresponde al legislador. Es sumamente difícil conciliar el mandato constitucional para la optimización de los derechos, el control de la constitucionalidad de los mismos y la libertad de configuración que tiene el legislador como representante de los ciudadanos, además de conciliar los intereses públicos y los privados, lo que genera una tarea ardua y de difícil control. MEDINA se decantó porque sea el poder y el proceso político quienes desarrollasen esa tarea de ponderación y proporcionalidad de los DDFF, siempre bajo el límite de los límites: *la garantía del contenido esencial de los DDFF*, consagrada por abundante jurisprudencia del TC y doctrina española. Se inició en la STC 11/1981, de 8 de abril (FJ 8) y desde entonces continúa estableciendo las garantías y limitaciones de los DDFF, su contenido esencial⁴¹⁶. Ello no debería resultar un perjuicio de la labor del legislador, como bien el TC en la STC 67/1984, de 7 de junio (FJ 2) adelantó. El contenido esencial no debería ser un todo *petrificado*, sino que, como cualquier otra cuestión, el contenido esencial sería también objeto de interpretación en función de los tiempos, de la sociedad del momento, manteniendo el sentido de la propia CE.

Respecto al derecho a la protección de datos personales, la proporcionalidad, la idoneidad y la intervención mínima se hacen indispensables para regular unas situaciones cambiantes en la realidad, por lo que la normativa constitucional se relacionaría con su finalidad. A diferencia del principio de igualdad, también de carácter relacional, la proporcionalidad, en estrecha relación con la idoneidad y la intervención mínima, se verían siempre en relación al medio y al fin que perseguía la norma constitucional. El lugar del principio de proporcionalidad dentro de la doctrina sobre los DDFF se encuentra en *su función de límite de los límites* que los poderes públicos pudieran imponer al ámbito material⁴¹⁷.

⁴¹⁶ Véase MEDINA GUERRERO, obra citada, p. 154-156. El contenido esencial de los DDFF es un límite a la capacidad de restringir los DDFF. La STC 11/1981, de 8 de abril, establece los mecanismos para delimitar el mencionado contenido esencial de los DDFF.

⁴¹⁷ GONZÁLEZ BEILFUSS, M., *El Principio de Proporcionalidad en la Jurisprudencia del Tribunal Constitucional*, Cizur Menor, 2003, pág. 112.

Se utilizó por la doctrina del TC el denominado en el derecho español *test de proporcionalidad* alemán (*Verhältnismäßigkeitsprüfung*) sobre todo en Sentencias con incidencia penal⁴¹⁸. En cuanto a la colisión con otros derechos, quedaría por resolver por la doctrina las definiciones adecuadas para la proporcionalidad, la idoneidad y la intervención mínima, porque se presentarían en confusión con otros aspectos. Se aportan como recientes referencias las STC 35/2016, de 3 de marzo y 38/2016, de 3 de marzo, las cuales reconocen el uso del test de proporcionalidad en el análisis de los recursos de constitucionalidad resueltos.

8.3. La protección de datos y otros DDFF, en referencia a los datos especialmente protegidos del artículo 16 CE.

⁴¹⁸ Existe una serie de trabajos analíticos desde la perspectiva del test de proporcionalidad; aparte de los mencionados autores anteriores, se podría cuestionar por la doctrina las definiciones de los conceptos, de proporcionalidad, idoneidad e intervención mínima, generándose la posibilidad de que los tres aspectos comentados sean la expresión de la realidad normativa adecuada a los tiempos, más que una doctrina inalterable en el tiempo. Son más bien conceptos de la racionalidad argumentativa para adecuar las situaciones a los DDFF consagrados, que se pueden utilizar, se piensa, en otros aspectos de la realidad, tanto del Derecho como en otras disciplinas. Véase la crítica de SÁNCHEZ GONZÁLEZ, S., "De la imponderable ponderación y otras artes del Tribunal Constitucional", *Teoría y Realidad Constitucional*, nº 12/13, 2003. No estando de acuerdo con la línea del autor, lo cierto es que presentó las posibles debilidades del test de proporcionalidad y de la ponderación, que unidos podrían formar un marco más acorde con los poderes políticos del momento. En otros sentidos PERELLÓ DOMÉNECH, I., "El principio de proporcionalidad y la jurisprudencia constitucional", *Jueces para la democracia*, nº 28, 1997. Y de la misma autora PERELLÓ DOMÉNECH, I., "Notas sobre el concepto de razonabilidad y su uso en la jurisprudencia constitucional", *Jueces para la democracia*, nº 46, 2003. Como reciente trabajo, las ideas de BINDI, E., "Test de proporcionalidad en el age of balancing", *UNED Revista de Derecho Político*, nº 96, 2016, pág. 291-330. La conclusión de la autora se basa en las ventajas de los controles realizados por los Tribunales Constitucionales sobre las decisiones de los órganos representativos, frente a los riesgos que son innegables, como pudieran ser los usos del principio de proporcionalidad como instrumento de lo que denomina *age of balancing* (edad del equilibrio) para sofocar la autonomía de la política democrática, al ser los Tribunales Constitucionales objeto de *un déficit democrático* y legitimador, con un alto nivel de discrecionalidad en la utilización de los elementos decisorios.

Se van a tratar en este punto de análisis las confluencias entre el derecho a la protección de datos personales y otros derechos fundamentales. Sin ánimo exhaustivo, como visión general del espacio legislativo y jurisprudencial (en especial consideración a las STC) en cuanto a la realidad que acompaña al tratamiento de datos personales.

8.3.1 Los libros bautismales y la protección de datos.

El asunto, ya no tan en debate tras el ATC 20/2011, de 28 de febrero, en el que no admitió a trámite el Recurso de Amparo plateado por la AEPD después de la STS 4646/2008, de 19 de septiembre, es sumamente interesante. Los hechos fueron, en un escueto resumen, los siguientes: El 23 de mayo de 2006, la AEPD admitió la reclamación de tutela de derechos (TD/00046/2006) por la que se ordenaba al Arzobispado de Valencia anotar en el libro de bautismo la solicitud de cancelación realizada por el interesado. A esta reclamación de tutela suceden varias más. Con fecha 10 de octubre de 2007, la Audiencia Nacional (por su Sección Primera de la Sala de lo Contencioso-Administrativo) desestimó el recurso interpuesto por el Arzobispado contra la resolución de la AEPD. El 19 de septiembre de 2008, el TS estimó el recurso de casación interpuesto por el Arzobispado contra la anterior sentencia, anulando la Resolución inicial de la AEPD. Para el 12 de noviembre de 2008, la Sección Sexta de la Sala de lo Contencioso-Administrativo del Tribunal Supremo dictó providencia por la que inadmitió el incidente de nulidad de actuaciones promovido por la AEPD. Las partes recurrieron al TC, pero el 28 de febrero de 2011, el ATC no admitió a trámite el recurso de amparo 9929-2008, promovido por la AEPD, al respecto del contencioso que mantenía desde hacía años con el Arzobispado de Valencia (y con la Iglesia Católica, IC a partir de ahora), respecto a la cancelación de datos en los Libros de bautismo, en el Auto del TC 20/2011, de 28 de febrero. El mencionado ATC consideró que la AEPD adolecía de falta de legitimación activa para interponer el recurso, puesto que no era titular (en este caso) del derecho a la tutela judicial efectiva, ni (en ningún caso) del dere-

cho a la protección de datos personales. El TC estimó que sólo los titulares de los derechos, el Defensor del Pueblo y el Ministerio Fiscal estarían legitimados⁴¹⁹. El TC no entró en el fondo del asunto. No valoró, como sí lo hizo en otras ocasiones. Por tanto, para este análisis se toman solamente en consideración los argumentos de la AEPD y del TS.

Se debe distinguir en este asunto la diferencia entre apostasía de la IC (de la fe, por tanto, asunto de creencias y otras normas que no son puramente jurídicas, pues afectan a ámbitos del alma, para el creyente), del derecho fundamental a la protección de datos personales, generándose varias cuestiones. En las reclamaciones interpuestas ante la AEPD se solicitaba la eliminación de la inscripción como católicos en los Libros Bautismales. Ninguna se basó en el uso ilegítimo del dato del bautismo, su tratamiento sin consentimiento expreso, su cesión sin consentimiento, su tratamiento automatizado o no automatizado, la posesión ilegal de los datos personales, la negación de acceso a los datos del titular, o cualquier otra razón que tuviera como argumento la normativa de protección de datos. El fondo del asunto no pudo ser claramente diferenciado y delimitado por los titulares de datos personales; muchos de ellos argumentaban mal su petición, no se limitaban a la simple cancelación o a la cuestión de protección de datos, sino que añadían algo más: sus intenciones emocionales de no formar parte de la IC, de no formar parte de los bautizados, de no incluirse su nombre como católicos, cuestión que debían dirimir con la propia IC, no con la AEPD. La STS resolvió con toda claridad *que la normativa sobre protección de datos tenía como objeto jurídico la protección de datos personales frente a intromisiones, preferentemente de la informática, no se podría utilizar para dejar constancia de creencias o convicciones de los ciudadanos* (FJ 4). El TS no consideró la petición de cancelación de los Libros de Bautismo como parte del derecho fundamental a la protección de datos personales.

⁴¹⁹ Un solo magistrado manifestó un voto particular (Pablo Pérez Tremps) por el que entendía que la AEPD sí tenía a su juicio capacidad para interponer el Recurso de Amparo, pues cumple una especial función institucional en la defensa del derecho fundamental a la protección de datos personales.

Los reclamantes muy posiblemente querían ejercer un derecho que se encuentra dentro del artículo 16 CE, como es la libertad religiosa, el cual tuvo su desarrollo en la Ley Orgánica 7/1980, de 05 de julio, la cual reconoció el derecho de todo ciudadano a cambiar de confesión o a abandonar la que tenía, e incluso manifestarse o no sobre este asunto que forma parte de la vida íntima y privada. Si se tratara de libertad religiosa, los poderes públicos deben tutelarlos. La apostasía, sin embargo, tiene sus propias normas dentro de la IC (en el *Código de Derecho Canónico*). Pero los reclamantes de tutela ante la AEPD quisieron formalizarlo a través de la norma civil y no a través del procedimiento previsto por la propia IC, llamándolo cancelación de los datos de los Libros de Bautismo, tratando estos Libros como ficheros. Este término utilizado fue el más definitorio. ¿Son los Libros y Registros mantenidos durante siglos por la IC ficheros en sentido legal para la normativa sobre protección de datos de carácter personal?; ¿Son los datos personales allí inscritos susceptibles de cancelación?; ¿Es la IC considerada como responsable de dicho fichero y de su tratamiento? ¿Se aplica la normativa de la LOPD a los Libros de la IC?

Desde un punto de vista puramente de protección de datos se deben considerar los siguientes elementos para concluir en una solución. Por una parte, la limitación al derecho a la protección de datos frente al Tratado Internacional con la IC. Por otra parte, la libertad religiosa expresada en la IC como organización independiente del Estado Español. En otro apartado, decidir sobre si es posible calificar como fichero, según la normativa de protección de datos, de los archivos y libros de la IC (no sólo de bautismo, también de matrimonios, defunciones, confirmaciones, y cualquier otro tipo de datos, que sólo la IC puede tratar) Y, por último, si existe un tratamiento en cuanto al mantenimiento de estos Libros y Registros.

La AEPD varió sus argumentaciones con el paso de los años. En el Informe Jurídico anteriormente referenciado se dice: “debe recordarse que, conforme a lo señalado en reiteradas sentencias de la AN, (...) los Libros Sacramentales han de ser considerados ficheros de datos de carácter personal”. En concreto, se referencia la SAN 4728/2007, de 10 de octubre de 2007 (FJ 3), en la cual se afirma que “Los Libros de Bautismo, por tanto, en la medida en que recogen datos de carácter personal -al menos el nombre y

apellidos del bautizado y el hecho mismo de su bautismo- con arreglo a criterios preestablecidos que permiten su tratamiento, tienen la consideración de fichero y están sujetos, en cuanto tales, a la legislación en materia de protección de datos. Con arreglo a lo expuesto, no puede negarse que, por ejemplo, la expedición de una partida de bautismo sea una forma de tratamiento de datos personales y que éstos, al estar contenidos en el Libro de Bautismo con arreglo a criterios preestablecidos, determinen que éste tenga la consideración legal de fichero. En definitiva, cuando el legislador ha querido excluir del ámbito de aplicación de la LOPD determinados ficheros lo ha dicho expresamente (artículo 2.2 LOPD), sin que en dichas excepciones se comprendan los Libros y Registros de la Iglesia Católica”. Como se consideraron ficheros, se deberían atener a la normativa de calidad de los datos, por ello, si el sentido de su mantenimiento era dejar constancia de la pertenencia a la fe católica de un individuo, y el titular de los datos ya no lo es por apostasía, debería haberse modificado su contenido (se argumentó por el Informe Jurídico con el artículo 4.3 LOPD, los datos personales deben ser exactos, adecuados y no excesivos). Además, se consideró una forma de apostasía por las Autoridades Eclesiásticas, elemento que no se negó por parte de los interesados. Sin embargo, el TS no consideró los Libros de Bautismo (y con ello todos los Libros y Registros de la IC) como ficheros, sino como un listado, *una acumulación* de datos personales (FJ 4), que no facilitaba su búsqueda, acceso o identificación, y para el TS no cumplían los requisitos ni del artículo 3.b), que definía el concepto de fichero ni del artículo 2.c) de la Directiva 95/46/CE, con el mismo contenido; muy al contrario de la opinión mantenida por la AEPD al respecto en ese momento, que consideró que con el nombre y apellidos del titular junto con la fecha y lugar del acto en cuestión (sea bautismo, matrimonio, acto más que controvertido por su eficacia civil, confirmación o cualquier tipo de acto religioso) se podía localizar fácilmente al titular⁴²⁰. La STS y la IC argumentaron que sólo el titular de los datos

⁴²⁰ El TS argumenta que “no cabe aceptar que esos datos personales, a que se refiere la Sala de instancia, estén recogidos en los Libros de Bautismo, como un conjunto organizado tal y como exige el art. 3.b) de la LO15/99, sino que resultan son una pura acumulación de estos que comporta una difícil búsqueda, acceso e identificación en cuanto no están ordenados ni alfabéticamente, ni por fecha de nacimiento, sino sólo por las fechas de bautismo, siendo absolutamente necesario el conocimiento previo

del acto religioso puede acceder a los mismos por el archivo parroquial, ningún tercero puede hacerlo. Se podría oponer que podían acceder miembros de la IC a esos archivos parroquiales, y seguro que no tenían control de accesos ni gestión por parte del Estado Español, al menos en este momento. Por ello, si estos Libros y Registros fueran ficheros, no se debería solicitar la cancelación de datos personales, sino que serían ilegales, deberían desaparecer⁴²¹.

Además, los datos de la IC tuvieron el carácter de datos históricos para la argumentación del TS, no de estado civil de la persona, pues si fuera así, los casados por la IC que tuvieran una convalidación de matrimonio civil en función del Tratado entre la Santa Sede y el Estado Español, ya mencionado, que en un determinado momento se divorcian, no modifican sus datos en los Libros y Registros de la IC. La AEPD sí reconoció este aspecto, tratando a los Libros de Bautismo como fichero, pero no entró a considerar a los Libros de Matrimonio.

El TS también basó su pronunciamiento en la autonomía de la IC y en la inviolabilidad de sus Archivos. Se podrían diferenciar en este asunto varios conceptos⁴²². Uno de ellos fue la autonomía de la IC en función del Tratado (o Acuerdo) entre el Estado Español y la Santa Sede, de 3 de enero de 1979. Es un Tratado internacional, por el que

de la Parroquia donde aquel tuvo lugar, no resultando además accesibles para terceros distintos del bautizado, que no podrían solicitar ajenas partidas de bautismo". Junto con los datos del bautizado, nombre o nombres y apellidos, figuran también en los Libros parroquiales los datos personales de padres, padrinos, testigos y autoridad competente, lugar y fecha de administración del Sacramento, día y lugar del nacimiento. Si no son suficientes datos personales, podemos comentar en este momento que una simple IP es considerada dato personal, o que un listado de alumnos con aprobado o suspenso también lo es. Además del bautismo, pueden figurar en estos libros otros Sacramentos, como ya se ha dicho: matrimonio canónico, confirmación, apostasía, defunción, entre otros datos.

⁴²¹ El TS no los consideró ficheros, pues en función del artículo 7.4 LOPD estarían prohibidos, recordemos su texto: "Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual"

⁴²² GONZÁLEZ MORENO, BEATRIZ; , "Comentario del artículo 7 LOPD. La Ley Orgánica de protección de datos y los Libros de Bautismo.", *Comentario a la Ley Orgánica de Protección de Datos Personales.* , Madrid., 2009.

se reconoció la eficacia civil a Instituciones o ritos religiosos que se encuentran regulados por un ordenamiento jurídico de igual entidad que el estatal con efectos en un ámbito distinto⁴²³. Por esta norma, el Estado Español debía respetar y proteger con carácter inviolable los Archivos, Registros y documentos de entidades eclesiásticas. Serían de aplicación las normas internacionales del Convenio de Viena sobre obligaciones de las partes contratantes, cuyo artículo 27 dispone que *una parte no puede invocar las disposiciones de su derecho interno como justificación del incumplimiento de un Tratado*. Además, el mandato del artículo 10.2 CE obligaba a que el Tratado entre la Santa Sede y España se cumpliera. La finalidad de los Libros o Registros de la IC y su naturaleza canónica resultaba evidente, pues su fin era la prueba de los Sacramentos administrados, según el Derecho Canónico, por las parroquias correspondientes. Resultaban probados, a través de estos archivos, hechos que se inscribieron, los cuales no se consideraron prueba de la adhesión personal a la fe católica ni a la pertenencia actual a la Iglesia. Se defendió por el TS que, como tales registros de la administración de Sacramentos, son inviolables frente al Estado Español y frente a los particulares, porque en el propio Acuerdo entre el Estado y la Santa Sede se reconocía a la IC el derecho a ejercer su misión apostólica y se le garantizaba el libre y público ejercicio de las actividades que le son propias y en especial las de culto, jurisdicción y magisterio⁴²⁴.

Entre la doctrina que se interesó por este asunto, se encuentran publicaciones que argumentaban en contra de la aplicación de la norma de protección de datos personales a los Libros y Registros de la IC⁴²⁵. La cuestión continua aún abierta en el año 2017

⁴²³ Obra citada, página 622.

⁴²⁴ Obra citada, página 623.

⁴²⁵ OTADUY, JORGE; "Iglesia Católica y Ley Española de Protección de Datos: Falsos conflictos. "]. <file:///D:/Downloads/95-08.OtaduyEst.pdf> Es sacerdote y profesor de Derecho Canónico de la Universidad de Navarra. Los estudios del profesor de Derecho Canónico se basan, lógicamente, en probar la no aplicación de la norma de protección de datos personales a los Libros y Registros de la IC. Se generaron en el tiempo de la polémica cuestión, por lo que sirven de base, prácticamente, a los argumentos del TS, o por lo menos, son similares. Los textos del profesor no admiten dudas intelectuales. Véase

tanto para la AEPD, que sigue recibiendo peticiones de cancelación de datos personales por ciudadanos españoles, como para la doctrina⁴²⁶. Existe, sin lugar a dudas, una garantía reforzada por la legislación de protección de datos hacia datos sensibles o especialmente protegidos, entre los que se encuentran los de naturaleza religiosa, en especial desde un punto de vista de derechos fundamentales. Por esta razón, se puede seguir analizando los argumentos utilizados por el Tribunal Supremo en torno a una cuestión concreta, entre otras cuestiones se podría plantear, ¿Puede explicar la confesión religiosa qué sucede con los datos de las personas que han decidido abandonar esa religión y estaban incluidos en cualquier tipo de soporte y tratamiento? El hecho de que estos Libros tengan como misión identificar, desde hace siglos, quién estaba bautizado y quién no, ya sería requisito suficiente para argumentar a favor de su carácter de fichero. Se podría añadir su estructuración como tal, aunque no sea un fichero automatizado, sino un fichero en papel, en Libros perfectamente ordenados por fecha y nombres, al igual que contienen infinidad de datos localizables y que no se evita la asimilación de una persona con la fe católica.

En el Estado aconfesional, Social, Democrático y de Derecho, que tiene reconocida una laicidad positiva (STC 46/2001, de 15 de febrero), desde un punto de vista de ciudadanía, la IC debería adoptar una serie de medidas para que los datos personales fueran disociados, evitando la posible identificación de los titulares de datos personales. Si la IC no lo realizase, podría darse la situación de que estos archivos canónicos se encuentren dentro de los supuestos contemplados en el artículo 7.4 LOPD, por el cual se prohibiría expresamente su existencia. Este resultado sería mucho peor para la IC que la simple cancelación de datos personales, o como se sugiere, la disocia-

también OTADUY, JORGE; , "La Iglesia Católica ante la Ley Española de Protección de Datos."]. [file:///D:/Downloads/ICn90\(529-555\).pdf](file:///D:/Downloads/ICn90(529-555).pdf)

⁴²⁶ PELAYO OLMEDO, J., "La adscripción religiosa como dato especialmente protegido. El caso del registro butismal en España."]. <http://revistas.uned.es/index.php/derechopolitico/article/view/15740/13691> El autor es también profesor y experto en asuntos canónicos. La pregunta de este autor es la siguiente: "¿qué sucede cuando el individuo ejerce su derecho a abandonar la confesión religiosa y sus datos se mantienen en un archivo interno de la confesión?"

ción⁴²⁷. No cabe la menor duda de que existen suficientes razones para que el TS no viera correctamente en su Sentencia la existencia de ficheros en estos depósitos de datos, pues las definiciones de la LOPD y su Reglamento se aplicaron a *depósitos de datos* mucho menos estructurados y organizados que los comentados. Simplemente se podría contemplar que la sociedad civil demanda una serie de actuaciones, que, sin ánimo de ingerir en la IC y sus múltiples aspectos positivos, deberían ser consideradas con fuerza y antelación a una acción civil suficientemente bien argumentada y sostenida en el Derecho Español, sin implicaciones religiosas (apostatas o no apostatas, otras cuestiones de odio o de revancha a la IC, eso no sería ni concluyente ni efectivo) que podrían cambiar la doctrina del TS. Además, la decisión del TC de no admitir a trámite el Recurso de Amparo de la AEPD no impide que otros presenten Recurso con buenos argumentos.

La cuestión religiosa y la protección de datos se aborda novedosamente en el RGPD en el artículo 91 en cuanto a *normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas*. Cuando en un Estado miembro, iglesias, asociaciones o comunidades religiosas apliquen, en el momento de la entrada en vigor del RGPD, un con-

⁴²⁷ Obra citada, páginas 166 a 168. El autor expone que “en un Estado aconfesional o de laicidad positiva (cita esta contradicción entre ordenamientos español, de protección de datos, vs. canónico) no puede servir para que un Tribunal estatal justifique que el alta en la entidad (bautismo) es un hecho cierto, exacto e histórico, pues sería reconocer que si la entidad no tiene previsto un procedimiento de abandono el derecho a abandonar la confesión religiosa puede que nunca llegará a ser efectivo.” (...) “A diferencia de otros supuestos, el bautismo tiene enorme trascendencia religiosa y jurídica para el ordenamiento católico. Por el bautismo no sólo se otorga en el ordenamiento canónico la consideración jurídica de persona con capacidad de derecho y deberes, sino que además se constituye en requisito jurídico previo para la consecución de otros sacramentos, específicamente del matrimonio canónico. Por ello, desde el punto de vista civil, insistimos en que sería más idóneo que la IC adoptará una medida completa de disociación de los datos, de tal modo que no se conculque el derecho a la protección de datos y en caso de necesidad, por cambio de opinión del interesado, pueda recuperarlos.” (...) “Lo más grave es que esta situación, si no se solventa, podría llevar a situar a este tipo de archivos dentro del apartado 4 del artículo 7 LOPD, donde se prohíbe expresamente su existencia. Una consideración que (...) tiene consecuencias jurídicas más graves e indeseadas que la mera cancelación o rectificación de los asientos.”

junto de normas relativas a la protección de las personas físicas en lo que respecta al tratamiento, tales normas podrán seguir aplicándose, siempre que sean conformes con el RGPD. Además, las iglesias y las asociaciones religiosas que apliquen normas generales de conformidad con el apartado 1 del artículo 91 estarán sujetas al control de una autoridad de control independiente, que podrá ser específica, siempre que cumpla las condiciones establecidas en el capítulo VI del RGPD. ¿Se podría generar, como posibilidad, una Autoridad independiente de protección de datos personales para cuestiones de índole religiosa, cumpliendo la normativa del RGPD? Aun cumpliendo la nueva normativa europea, se plantean dudas razonables respecto a la Autoridad de control independiente que podrá ser específica en directa conexión, no con el Derecho Constitucional o con el Derecho Europeo, sino con normativas de índole religiosa, que podrían ser cuestionables. Se generarían entonces ámbitos de aplicación normativa de un derecho fundamental, como lo es la protección de datos, al margen de las normas establecidas por los poderes del Estado o de la UE, pues no se aplicarían, como no se aplican en la actualidad, las normas sobre protección de datos a los registros de las comunidades religiosas, sean de la tendencia que fueran. A la espera de las decisiones de la AEPD, podría ser una alternativa la modernización de las normas sobre los documentos de la IC, junto con la creación de una Autoridad independiente que cumpla la normativa de protección de datos dentro del territorio europeo, formada por las distintas sensibilidades e intereses agrupados para un fin común, cual fuese la protección de los DDFF, tanto a la protección de datos como a la libertad religiosa.

8.3.2 La videovigilancia, los sistemas de grabación y visualización de imágenes.

Se considera videovigilancia la captación, grabación y/o tratamiento de imágenes con fines de observación y seguridad, para proteger a personas o bienes. En entornos empresariales tiene una especial utilización, pues la empresa verifica a través de las

imágenes, que se graban o no en diferentes dispositivos, el cumplimiento del trabajador de sus obligaciones laborales y la seguridad de las instalaciones ante acciones ilícitas de terceros (robos, atracos, daños a personas y bienes) o de su propio personal. La videovigilancia y la captación de imágenes, tanto privada, en sentido de hogares o instalaciones para uso personal, como empresarial, repercute sobre los derechos de las personas, lo que obligó a los legisladores y Tribunales a fijar garantías para su práctica. La LOPD, su Reglamento y la Instrucción 1/2006, de 8 de noviembre de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia por sistemas de cámaras o videocámaras, resultó aplicable a los casos en que el uso de la videograbación o videovigilancia afectase a personas que pudieran ser identificadas o identificables, pues se considera la imagen un dato de carácter personal. La Ley Orgánica 4/1997, de 4 de agosto, reguló la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. Para el ámbito privado, la Ley 5/2014, de 4 de abril, de Seguridad privada (en adelante, LSP), aportó una normativa que afectó a la protección de datos personales, derogando la norma anterior de 1992.

Junto a estos usos de videovigilancia regulados, existen otros nuevos métodos de captación y tratamiento de imágenes por medio de videocámaras o webcams. En estos casos, también se aplicó la LOPD cuando existiese captación, grabación, transmisión, conservación o almacenamiento de cualquier tipo de imágenes que permitieran la identificación de una o varias personas. Además, dicho tratamiento de datos personales por grabación de imágenes debe contar con suficiente legitimación, por lo que el titular de los datos tiene que prestar su consentimiento para el tratamiento de imágenes, o como excepción, una norma con rango de ley eximiría de consentimiento al responsable del fichero o tratamiento, como sería el caso del artículo 20 del Estatuto de los Trabajadores o la tipología prevista por la LSP. Por el contrario, no se aplicaría la normativa de protección de datos cuanto se tratase de imágenes captadas y tratadas en un ámbito doméstico, siempre y cuando no trasciendan a otros. Tampoco se

aplica la protección de datos a los medios de comunicación, en un ejercicio legítimo del artículo 20 de la CE⁴²⁸.

Las imágenes deben captarse y tratarse en proporcionalidad a la finalidad, informando de su captación y/o grabación al titular, siempre teniendo en cuenta antes de su utilización la existencia de medios menos invasivos. No se permite captar ni grabar imágenes en espacios públicos desde instalaciones privadas, salvo que sea imprescindible para la finalidad de vigilancia pretendida. Las imágenes sólo se pueden conservar por un tiempo imprescindible para cumplir con la finalidad autorizada, después se debe proceder a su destrucción definitiva.

Entre las obligaciones del responsable del fichero o tratamiento, la LSP estableció que los ficheros deberían ser inscritos como tales en la AEPD (Ficheros de Videovigilancia) no se consideraba fichero a la simple visualización de imágenes en tiempo real, si no existían grabaciones de tales momentos; para estos casos, no fue necesaria la inscripción, pero sí se mantenían las obligaciones de la normativa de protección de datos mencionada. Después de la entrada en vigor del RGPD, la cuestión de inscripción de ficheros no se apreciaría como necesaria, pero no se tiene en este momento la decisión de la AEPD, que quizá, por el tipo de dato de imágenes, podría establecer algún sistema de control o certificación.

⁴²⁸ En este punto existen actualmente peticiones de discreción al respecto, por el uso abusivo de imágenes de personas, que, siendo anónimas, se encuentran con su imagen en programas y redes sociales, por el efecto descrito de transmisión de información por redes sociales. Se trataría últimamente de mitigar este exceso, por normativa deontológica profesional, después de los últimos atentados en Francia y en Bélgica, solicitando a los medios de comunicación respeto por las situaciones y las imágenes de videovigilancia que muchas veces, argumentando una noticia, serían excesivas, por su falta de respeto a las víctimas y a su dolor o circunstancia (visionado de cadáveres expuestos, personas heridas sangrando o mutiladas, tratadas por los servicios de emergencia en situaciones íntimas; personas corriendo ante el pánico que produce la situación, como ejemplos) Se trataría de imágenes que no aportan nada a la noticia, sólo intrusión en la intimidad y el dolor de otros, no es una censura informativa. Algunos medios advierten de este tipo de imágenes e incluso las muestras con rostros *pixelados*, para respetar la identidad de las personas implicadas y su momento de dolor.

La LSP mantuvo el deber de información al titular de los datos. Se debería informar a todas las personas que resultase videovigiladas o grabadas que entrasen en recintos con instalaciones de videovigilancia. La Instrucción 1/2006 AEPD aportó un *distintivo informativo* (bien conocido, pues se encuentra en entidades bancarias, farmacias, centros comerciales, por ejemplo) obligatorio. Este distintivo se debe colocar en los accesos del espacio afectado. Además, se informa a los afectados de la existencia de un fichero o tratamiento de datos, la finalidad y los destinatarios, los derechos ARCO (acceso, rectificación, cancelación y oposición), junto con la identidad y dirección del responsable del fichero o tratamiento. La información puede constar en el propio distintivo de videovigilancia o en otros soportes, siempre y cuando el titular tenga acceso a esa información. En estos aspectos, también se espera un cambio normativo a favor de una certificación de control de procedimientos.

En cuanto a la cancelación de imágenes, la AEPD estableció en la Instrucción 1/2006, el plazo de un mes, como máximo, para que se cancelasen las imágenes obtenidas por videograbación. Es el mismo criterio que se estableció en la Ley Orgánica 4/1997, para la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. Excepcionalmente se conservarían las imágenes que gravasen delitos o infracciones a disposición de la Autoridad competente.

A. Los Servicios de videovigilancia y la seguridad privada.

En los principios del siglo XXI se abarataron sensiblemente los sistemas de videograbación y captación de imágenes, por lo que la seguridad privada también se extendió en su uso por la población en general. La cuestión de videovigilancia no estaba específicamente regulada. Sólo existieron referencias como en la Disposición Adicional Novena de la Ley Orgánica, 4/1997, de 4 de agosto, de utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos (LO 4/1997), en donde se estableció un mandato por el que el Gobierno debía elaborar en el plazo de un año, es decir, agosto de 1998, la normativa correspondiente para adaptar los principios inspiradores

de dicha norma al ámbito de la seguridad privada⁴²⁹. La AEPD suplió durante años esta carencia normativa hasta el año 2014, con la Ley 5/2014, de 4 de abril, de Seguridad Privada (LSP) que reguló esa materia para evitar el ejercicio de tratamientos de datos personales de forma indiscriminada y omnipresente, legitimando el tratamiento de datos por las empresas de seguridad privada.

El artículo 5.f) LSP, definió como actividades de seguridad privada la instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia; El artículo 6 LSP consideró que la fabricación, comercialización, venta o entrega de equipos técnicos de seguridad electrónica, así como la instalación o mantenimiento de dicho equipos, siempre que no estuvieran conectados a centrales de alarma o centros de control o de videovigilancia, son y pueden ser actividades complementarias de la actividad de seguridad privada. Según el artículo 6.4. LSP, los prestadores de servicios de seguridad privada que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, no conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia, quedarían excluidos del ámbito de aplicación de la legislación de seguridad privada. El artículo 6.4 LSP estableció que las empresas de seguridad privada que se dediquen a la instalación o mantenimiento de aparatos, dispositivos y sistemas de seguridad que no incluyesen la conexión a centrales receptoras de alarmas o a centros de control o de videovigilancia, sólo estarían sometidas a la normativa de seguridad privada en lo que se refiere a las actividades y servicios de seguridad privada para las que se encontrasen autorizadas. Por tanto, se reguló la instalación y mantenimiento de sistemas de videovigilancia cuando estén conectados a centrales de alarmas con sistemas de videovigilancia, reservando esta actividad a los profesionales. Las empresas deberían estar convenientemente autorizadas o haber presentado declaración responsable, estar inscritas en el Registro Nacional de Seguridad Privada o Registros autonómicos correspondientes (artículo 18 a 20 LSP); el contrato de presta-

⁴²⁹ Sobre esta cuestión téngase en cuenta la Ley 23/1992, de 30 de julio, de Seguridad Privada y su Reglamento de desarrollo, la cual, no pudo prever el fenómeno tecnológico, por lo que no contenía normas sobre tratamiento de datos captados por cámaras.

ción del servicio deberá celebrarse por escrito comunicándose su celebración al Ministerio del Interior o, en su caso, al órgano autonómico correspondiente con antelación a la iniciación de la actividad (artículo 9 LSP) según lo que se determine reglamentariamente, entre otras normativas para el sector profesional.

La AEPD definió la actividad hasta la nueva LSP de 2014, otorgando legitimación al tratamiento de datos personales. La videovigilancia se definía explícitamente en el artículo 42 LSP⁴³⁰, el cual se remitió a la LO 4/1997 de utilización de videocámaras

⁴³⁰ El artículo 42 define ampliamente los servicios de videovigilancia:

1. Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.

Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales.

No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras cuyo objeto principal sea la comprobación del estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. Estas funciones podrán realizarse por personal distinto del de seguridad privada.

2. No se podrán utilizar cámaras o videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en su normativa específica, previa autorización administrativa por el órgano competente en cada caso. Su utilización en el interior de los domicilios requerirá el consentimiento del titular.

3. Las cámaras de videovigilancia que formen parte de medidas de seguridad obligatorias o de sistemas de recepción, verificación y, en su caso, respuesta y transmisión de alarmas, no requerirán autorización administrativa para su instalación, empleo o utilización.

4. Las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad. Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales.

5. La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de

por las Fuerzas y Cuerpos de Seguridad en lugares públicos en su artículo 6.1. en cuanto a cumplimiento de los principios de idoneidad e intervención mínima con medios proporcionales a los objetivos necesarios de protección de las personas y bienes.

Lo más resaltable de la normativa implicada en los sistemas de videovigilancia y en su caso, videograbaciones, serían su única finalidad: *la seguridad en cuanto a la protección de personas y bienes que puede ser también una actividad preventiva de daños o para detectar los mismos*. Otras finalidades no son admisibles. El artículo 42 LSP regula los supuestos en los que el uso de videocámaras o cámaras en general no está dentro de los servicios de la videovigilancia y que podrían realizarse por personas que no pertenecen a un servicio de seguridad privada (conserjes de un edificio, personas de control de accesos para aparcamientos, por ejemplo) A estos servicios también sería de aplicación las normas de protección de datos, estando restringido el acceso al visionado y tratamiento de datos exclusivamente a las personas autorizadas.

Un punto importante respecto a la videograbación y videovigilancia sería la cesión de imágenes. El artículo 8.4 LSP estableció la prohibición expresa a las empresas y personal de las mismas para transmitir este tipo de datos personales a otros, con la excepción de las autoridades judiciales y policiales. Especialmente en conexión con los DDFF, el personal de empresas de seguridad o la propia empresa no podrían ejercer ningún tipo de control sobre opiniones políticas, sindicales o religiosas o sobre la expresión de tales opiniones, ni proceder al tratamiento, automatizado o no, de datos relacionados con la ideología, afiliación sindical, religión o creencias. Son los datos especialmente protegidos de la LOPD. El artículo 15 LSP estableció la cesión de datos de videograbación a los Cuerpos y Fuerzas de Seguridad del Estado, admitiendo también el acceso a los sistemas de videovigilancia en tiempo real cuando fuera necesario para el cumplimiento de su función preventiva o represiva de acciones delictivas. Se trata de la excepción de Seguridad pública que apareció también en la LOPD.

carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.

6. En lo no previsto en la presente ley y en sus normas de desarrollo, se aplicará lo dispuesto en la normativa sobre videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad.

La LSP en su preámbulo expresó las motivaciones que promueven a la Ley, “la seguridad no es solo un valor jurídico, normativo o político; es igualmente un valor social. Es uno de los pilares primordiales de la sociedad, se encuentra en la base de la libertad y la igualdad y contribuye al desarrollo pleno de los individuos. Los Estados, al establecer el modelo legal de seguridad privada, lo perfilan como la forma en la que los agentes privados contribuyen a la minoración de posibles riesgos asociados a su actividad industrial o mercantil, obtienen seguridad adicional más allá de la que provee la seguridad pública o satisfacen sus necesidades de información profesional con la investigación de asuntos de su legítimo interés. En esta óptica, la existencia de la seguridad privada se configura como *una medida de anticipación y prevención frente a posibles riesgos*, peligros o delitos. La consideración de la seguridad privada como una actividad con entidad propia, pero a la vez como parte integrante de la seguridad pública, es hoy un hecho innegable.” La pregunta estaría en función de la consideración de la Seguridad como una actividad cuya competencia exclusiva es del Estado, según la CE, artículo 104.1, con importante reserva de ley orgánica para regular estos aspectos de Fuerzas y Cuerpos de Seguridad; artículo 149.1.29 y las STC⁴³¹. En la CE no se mencionó expresamente la seguridad privada como materia constitucional. Pero su implicación en cuanto a los DDFF se puede intuir sin dificultad. El artículo 104 CE otorgó como misión a las Fuerzas y Cuerpos de Seguridad del Estado la protección del ejercicio libre de los derechos y libertades y la garantía de la seguridad ciudadana. El Título VIII, de la Organización Territorial del Estado, estableció la materia competencial de Seguridad y Defensa de los ciudadanos al Estado. Se denominará la seguridad mencionada en la CE como *seguridad pública*, frente a la denominación seguridad privada de la videovigilancia privada. Avanzando por el texto constitucional, se reiteraría así la idea de *competencia exclusiva del Estado* en asuntos de seguridad⁴³². Sería

⁴³¹ Entre otras, véase STC 36/1982, de 16 de junio y STC 325/1994, de 12 de diciembre.

⁴³² La seguridad y la defensa se deben garantizar desde el Estado, cuestión que los artículos 1.1 CE (Estado social, democrático y de Derecho), artículo 9.2 CE (Estado como responsable de las condiciones de la vida social), o artículo 10.1 (promoción de la paz social y el orden político, que impone un límite a los derechos individuales, conforme al respeto a la Ley y a los Derechos de otros ciudadanos) se ma-

el denominado *imperium* del Estado para posibilitar en la realidad los mandatos de las normas. Ante esta exposición, la pregunta resultante sería si existe un derecho a la actividad privada de seguridad, basándose en el derecho a la autodefensa, a la propiedad privada o a la libertad que la CE garantiza. Y si ese derecho a la seguridad puede basarse en la captación, visualización, o transmisión de imágenes que identifiquen o hacen identificable a la persona. Una vez traspasado el límite de autorización a las actividades de seguridad con usos de visualización de imágenes y videograbación, solamente podría justificarse este hecho en una decisión del legislador y, por tanto, una decisión política, pues no es una exigencia constitucional en el sistema español. Se podría calificar a la seguridad privada de seguridad pública en la que intervienen operadores privados por una licencia del poder público (como es el legislador) que así lo reguló en la LSP. Es llamativo que este aspecto de Seguridad del Estado con sus ciudadanos implicados se regulase por una ley ordinaria y no se atenga a la reserva de Ley Orgánica que sí se desarrolla en la LO 4/1997, de utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, aunque la propia LSP del año 2014 se refiera en múltiples ocasiones a la LO 4/1997, más antigua y más obsoleta en asuntos de regulación de usos tecnológicos, o al menos por razones temporales así debería ser. La incidencia de la captación de imágenes por sistemas de videovigilancia o videograbación en la sociedad actual invadiría el área de los DDFF con la fuerza del uso indiscriminado de tales medios y con la sospecha de la falta de control por parte de los titulares de datos acerca de la finalidad de tales grabaciones. Se puede decir que sería casi imposible controlar las imágenes, su tratamiento y su destino. Todo ello con una consideración apreciable hacia el uso práctico de los sistemas de videovigilancia en cuanto a prevención de situaciones de riesgo, que en la ciudadanía se fomentó. Es este hecho, el sacrificio de la protección de datos personales ante la seguridad, con la asunción de un pago privado para completar la actividad de las legítimas Fuerzas y Cuerpos de Seguridad del Estado, el asunto obvio y la justificación de tales actividades. Pensando, además, que el uso de las grabaciones, por ejemplo, en espa-

nifiestan como ejemplos del fundamento de la paz social, la dignidad de la persona y los derechos inviolables.

cios cerrados, como puede ser un centro comercial al uso, sirven a los fines de análisis de conducta para marketing y otros intereses relacionados con el comercio⁴³³ (prácticamente a nivel mundial) y que esos datos, conectados con las actuales bases de datos y cruzados con otros (*big data*), configuran un historial de incalculable valor, tanto para seguridad como para otros fines, *pasando del almacenamiento y procesamiento de datos al análisis y conocimiento*. Se destaca la incidencia de la videograbación en una actividad necesaria como es la producida en entornos laborales, la cual se encuentra claramente afectada por la videovigilancia y la videograbación.

B. La videovigilancia en el entorno laboral. La Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo de 2016.

La tecnología otorga a la empresa posibilidades casi ilimitadas frente al trabajador para vigilar el cumplimiento de las obligaciones laborales. Existen programas para grabar las teclas y las pantallas que pulsan los trabajadores, para controlar los mensajes que envía y recibe en su móvil de empresa o para grabar su imagen y su conducta en toda la jornada laboral. El TC se encargó en diferentes momentos de asuntos relacionados con videovigilancia en entornos laborales. La STC 29/2013, de 11 de febrero, marcó una línea de interpretación jurisprudencial que posteriormente fue modificada por la STC 39/2016, de 3 de marzo.

La STC 29/2013 analizó la sanción disciplinaria a un trabajador por incumplimiento de jornada laboral; la citada sanción se basó en una serie de grabaciones de imágenes realizadas por las cámaras de videovigilancia en su centro laboral. El trabajador esta-

⁴³³ Para el actual análisis de tendencias, esa información es valiosísima. Los movimientos por las salas, las conductas, incluso las conversaciones, las gesticulaciones, las compañías, entre múltiples factores que esta tesis no puede analizar, pues no tiene formación psicológica o psiquiátrica. Son los expertos en conducta los que dirigen esas investigaciones de imágenes. Véase LUCENA CID, ISABEL VÍCTORIA; "El concepto de la intimidad en los nuevos contextos tecnológicos", *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*, Valencia, 2014, pág. 35 y ss.

ba informado de la existencia de las cámaras y de la grabación de imágenes, pero no estaba informado de su finalidad como supervisión de su actividad laboral. El TC entendió que el trabajador debía ser informado de esta finalidad previamente, de forma clara, precisa, expresa e inequívoca. Como no fue así, el TC consideró que se había vulnerado el derecho del trabajador a la protección de datos personales, declarando la nulidad del despido⁴³⁴.

En la STC 39/2016 se reconoce la legitimidad del uso de cámaras de seguridad en el lugar de trabajo, sin consentimiento del trabajador, cuando la finalidad de este tra-

⁴³⁴ En el FJ5, el TC expone que “Estamos, en definitiva, dentro del núcleo esencial del derecho fundamental del art. 18.4 CE, que se actualiza aún de modo más notorio cuando, como en el caso a examen, nos adentramos en un ámbito —el de la video-vigilancia— que ofrece múltiples medios de tratamiento de los datos; sistemas, por lo demás, en auge y desarrollo exponencial, que se amplían y perfeccionan a un ritmo vertiginoso y que se añaden a otros más conocidos (circuitos cerrados de televisión, grabación por dispositivos webcam, digitalización de imágenes o, en particular, instalación de cámaras, incluidas las que se emplacen en el lugar de trabajo). Debe asegurarse, así, que las acciones dirigidas a la seguridad y vigilancia no contravengan aquel derecho fundamental, que tiene pleno protagonismo, por todo lo expuesto, en estos terrenos de la captación y grabación de imágenes personales que permitan la identificación del sujeto. En relación con el contrato de trabajo este protagonismo cobra, si cabe, mayor relevancia habida cuenta la coincidencia existente entre el locus de trabajo, que es donde pueden movilizarse por los trabajadores las garantías fundamentales, y los espacios físicos sujetos a control mediante sistemas tecnológicos.” Existe un voto particular formulado por D. Andrés Ollero Tassara, el cual considera que no se ha tenido en cuenta el principio de ponderación que sí se tuvo como relevante en la STC 186/2000, la cual reconoce el poder de dirección del empresario como “imprescindible para la buena marcha de la organización productiva”. El empleado recurrente en la STC de 2013 aportaba datos falsos sobre su actividad laboral, por lo que este magistrado expone su discrepancia. Otro ejemplo de esa dirección doctrinal es la STS 2618/2014, de 13 de mayo, la cual consideró que existía una clara vulneración empresarial de los derechos fundamentales del art. 18.4 CE provocada por la utilización de las cámaras de video-vigilancia para sancionar a una trabajadora por el alegado incumplimiento de sus obligaciones laborales. Por tanto consideraba ilegal la utilización no consentida ni previamente informada de las grabaciones de imagen para un fin, desconocido por la trabajadora afectada y distinto del expresamente señalado por la empresa al instalar el sistema con carácter permanente, de control de su actividad laboral, contrariamente a lo que comunicó a la representación de los trabajadores, ya que afirmaba que la finalidad exclusiva era la de evitar robos por parte de clientes y que no se trataba de un sistema de vigilancia laboral.

tamiento de las imágenes sea la comprobación del cumplimiento fidedigno del contrato de trabajo (FJ4). En concreto, se desestima en la reciente STC de 2016 el recurso de amparo presentado por una trabajadora de una conocida tienda de ropa que fue despedida después de comprobar su empresa, por medio de cámaras de videovigilancia, que había sustraído cantidades de dinero de la caja, ejecutando una serie de acciones para ello (se llevaba el dinero de la caja y para disfrazar el fraude, realizaba la devolución de prendas que no habían sido en realidad devueltas) En este caso, se considera que el consentimiento para la videograbación no era necesario, que bastaba la advertencia de zona videovigilada que figuraba en la entrada pública al establecimiento⁴³⁵ y el consentimiento se considera implícito (se puede afirmar que tácito) en la propia relación contractual con la aceptación del contrato de trabajo. El TC entendió que se deben ponderar los DDFF del trabajador, en especial a la protección de datos y los DDFF del empresario, con sus facultades de control y vigilancia reconocidas en el artículo 20 de la LET (ley del Estatuto de los Trabajadores) en directa conexión con los artículos 33 y 38 CE. Considera la STC que el poder de dirección del empresario es imprescindible, exactamente lo que opinaba el voto particular de la STC del año 2013. El TC no olvida que las medidas a aplicar en este sentido deben ser⁴³⁶:

⁴³⁵ En este caso, el TC coincide con el Magistrado D. Ollero Tassara, que en el año 2013 presentó su discrepancia, pues afirma que “el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana” ... “El consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario.” FJ4º STC 39/2016.

⁴³⁶ “Del razonamiento contenido en las Sentencias recurridas se desprende que, en el caso que nos ocupa, la medida de instalación de cámaras de seguridad que controlaban la zona de caja donde la demandante de amparo desempeñaba su actividad laboral era una medida justificada (ya que existían razonables sospechas de que alguno de los trabajadores que prestaban servicios en dicha caja se estaba apropiando de dinero); idónea para la finalidad pretendida por la empresa (verificar si algunos de los trabajadores cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona de la caja), por lo que debe

- Adecuadas: proporcionalidad de la medida de vigilancia.
- Justificadas: que existan sospechas razonables de incumplimiento de contrato.
- Idóneas: para verificar las irregularidades sospechadas.
- Necesarias: para probar tales irregularidades.
- Equilibradas: limitación de la grabación a la zona de sospecha.

Para la STC 39/2016 se plantearon tres votos particulares. En ellos se pone de manifiesto que se modifica la jurisprudencia precedente, sin el debido estudio de la situación. Estiman que no resulta justificado el criterio atendiendo al principio de proporcionalidad. No consideran tampoco que existan conflictos constitucionales entre el artículo 20 LET y el artículo 18.4 CE, pues la LET no es una norma con rango constitucional, por tanto, no puede colisionar con el derecho fundamental a la protección de datos. Contrariamente se opina desde el voto particular que “los poderes y facultades del empleador quedan delimitados por el contenido esencial de los DDFF de los trabajadores, resultando obligado tener presente que dichos derechos delinean la regularidad del ejercicio de tales poderes y facultades. Unos y otras solo pueden ejercitarse en términos acordes con el ámbito en el que la plenitud del contenido esencial de aquellos derechos (art. 53.1 CE) quede garantizada”⁴³⁷

Hasta este momento, no había existido una argumentación legal para omitir el derecho a la información sobre el tratamiento de datos personales en el ámbito laboral. Acogiéndose a la lógica empresarial (por otro lado, digna de respeto, pues la trabajadora realizaba una apropiación de dinero indebidamente) la STC de 2016 lleva a confusión, pues tergiversa “la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos (art. 20.3 LET en relación con el art. 6.2 LOPD), con la constitucionalidad del acto (que exige

descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE.” (FJ5, STC 39/2016)

⁴³⁷ Punto 2 del primer voto particular, Magistrado D. Fernando Valdés Dal-Ré, al que se adhiere la Magistrada Dña. Adela Asua Batarrita, como segundo voto particular.

ofrecer previamente la información necesaria, art. 5 LOPD). Y lo cierto es, sin embargo, que cabe proclamar la legitimidad de aquel objetivo (incluso sin consentimiento del trabajador, art. 6.2 LOPD, como señala la Sentencia aprobada) y, al mismo tiempo, hacer constar que lesiona el art. 18.4 CE la utilización, para ejecutar el acto, “de medios encubiertos que niegan al trabajador la información exigible.” (texto del mismo voto particular mencionado)⁴³⁸ Se puede destacar que la STC 39/2016 parece pretender realmente el rango de constitucionalidad para la obtención de pruebas a través de la vulneración de los DDFF constitucionalmente protegidos, como es el derecho a la protección de datos personales⁴³⁹. Estas cuestiones también afectan a la Instrucción 1/2006 AEPD, pues una Instrucción de la AEPD se convierte, según los magistrados y su voto particular, en “canon de constitucionalidad”, lo cual es sinceramente imposible⁴⁴⁰.

En el voto particular formulado por el magistrado Xiol Ríos se realiza una interpretación completamente diferente de los DDFF de los trabajadores y del propio derecho a la protección de datos. Menciona las importantísimas SSTEDH del año 2003, de 28 de enero, *Peck c. Reino Unido*, y 17 de julio de 2003, *Perry c. Reino Unido*; el artículo 5 LOPD, recuerda que resulta necesario que la información sobre la existencia de cámaras de videovigilancia se dirija explícitamente a los interesados (trabajadores en este

⁴³⁸ De forma sincera, el Magistrado mantiene que “En última instancia, la lectura de la resolución de mi disenso me suscita dudas sobre la verdadera finalidad a la que atiende la doctrina sentada, que enuncio en términos interrogativos: ¿se pretende asegurar un control legítimo por el empresario de la actividad laboral, con respeto a las garantías legales y a los derechos fundamentales o, por el contrario y más bien, se busca habilitar controles sorpresivos, que permitan identificar *in fraganti* a un trabajador que no cumpla debidamente su contrato? Si fuera esto último, como lamentablemente así me lo parece, no alcanzo a entender la conexión entre esa intención, no ya de controlar sino de “atrapar” al trabajador, con la libertad de empresa o el derecho a la propiedad que consagra la Constitución”

⁴³⁹ FJ 5 STC 39/2016 en el que se habla de *pruebas de irregularidades*. Ejercer un despido con fundamento no puede violar los DDFF, es una máxima que hasta ahora defendió el TC en multitud de sentencias. Los magistrados hablan de “el exceso del exceso: no sólo la colisión ficticia de derechos sino, adicionalmente, la colisión en la antijuridicidad.” Punto 3 de su exposición.

⁴⁴⁰ Punto 5 del voto particular mencionado.

caso de confirmación de actividades en cumplimiento de la prestación laboral), siendo insuficiente la información de videovigilancia para seguridad y orientada al público en general que circula por el establecimiento.

La situación actual se manifiesta difícil de consensuar. Existiría en este caso un conflicto entre los derechos de la trabajadora a la intimidad y a la protección de datos personales frente a los derechos del empresario a la propiedad y a la libertad de empresa. La solución se produciría a través de la ponderación de los DDFF en controversia. Si bien es cierto que los actos de la trabajadora eran ilícitos, también lo puede ser conseguir pruebas para demostrarlos a través de la violación de los DDFF. Es obvio que la empresa de este caso, a pesar de su buen volumen económico, carecía de atención profesional en cuestiones de seguridad y protección de datos. Lo más lógico y correcto, hubiera sido solicitar el consentimiento informado expreso y por escrito del trabajador/a para las cuestiones relacionadas con videograbación de los espacios de trabajo, incluyendo el tiempo que se deben conservar dichas imágenes y los derechos ARCO desde un primer momento, en la aceptación del contrato laboral, al margen de constantes advertencias sobre la existencia de sistemas de videograbación en lugares estratégicos de la empresa, como son entradas al local, zonas de paso, zonas de almacenaje y zonas de caja o salvaguarda de bienes dinerarios. La empresa, por su parte, debe obligarse a las únicas finalidades para la que esas imágenes de los trabajadores son videovisionadas y grabadas: la seguridad del entorno, entre las que se incluye la seguridad de los propios trabajadores, el seguimiento de la actividad laboral y cumplimiento del contrato de trabajo. El trabajador debe otorgar su consentimiento, se recuerda otra vez, por ser importante en esta exposición. Por otro lado, dar rango constitucional al derecho de la empresa para controlar el cumplimiento fidedigno del contrato laboral (lo que se produce con la STC 39/2016), sería arriesgar un uso indebido del poder del empresario, en especial de grandes corporaciones, cuyo poder no se puede comparar a ese pequeño empresario dueño del bar cuyos trabajadores sirven una bebida sin incluir ese importe en la caja, la pequeña panadería con idéntico problema, el taller al que le sustraen herramientas, y un largo listado de pequeños casos en los que no se reconoció la grabación de imágenes por artulugios case-

ros (no era una videograbación de vigilancia por personal de seguridad, era una simple cámara instalada de forma casera en la mayoría de los casos) como prueba para el despido procedente y esos pequeños empresarios se vieron afectados por los actos ilícitos de personas desleales. No se analizaran los muchos usos indebidos de instalaciones empresariales para fines privados (visionado y grabación de películas por *internet* en horarios laborales, incluso a través de grandes servidores de empresa por trabajadores; robo de bases de datos y de información empresarial para venderla a otros; daños y destrucciones causados a instalaciones empresariales de todo tipo, no sólo tecnológicas, entre otros ejemplos) que no admitieron la prueba de videograbaciones para la sustanciación ante los Tribunales. Todo ello requiere una delimitación más acorde con los tiempos actuales, pero la protección de un bien legítimo no puede producirse con medios o actos que violen los DDFF. Sin lugar a dudas, los trabajadores tienen un derecho fundamental e innegable a la protección de datos, extendido a los datos que se recopilan y tratan por medios tecnológicos para evaluar el trabajo y la conducta de una persona, en especial la videograbación, transmitir a terceros estos perfiles y generar una situación encubierta de tratamiento de datos personales que no se pone en conocimiento del trabajador. Esta situación, que éticamente es muy reprochable y legalmente es ilícita, probablemente se produce en muchas grandes empresas y no podría ser denunciada hasta ahora, aunque las sospechas, sin denuncia puesto que faltan pruebas de sustanciación ante los Tribunales, existen y estarían fundadas.

Otros medios invasivos de la protección de datos de los trabajadores, como puede ser el uso del GPS para saber la localización del trabajador, aún en horarios fuera de su jornada laboral, a través del teléfono móvil o del coche de empresa, por ejemplo, se transforman rápidamente en violaciones de DDFF y convierten el control de los propios datos en algo ilusorio⁴⁴¹. Como se reconoce en la doctrina, existiría un doble

⁴⁴¹ El cambio de doctrina se puede apreciar en el año 2016 con las STS siguientes: STS 4020/2016, de 21 de julio; STS 4070/2016 de 7 de julio; STS 4077/2016 de 12 de julio. A este cambio doctrinal se puede añadir la STEDH 61496/08, de 12 de enero de 2016, que reconoció el derecho de la empresa a controlar a los empleados que comuniquen a través del sistema empresarial. Es el caso *Barbulescu vs. Rumanía*,

plano en los pronunciamientos del TC, que se determina entre las declaraciones formales y las actuaciones sustanciales. Si se sitúa el análisis en las declaraciones formales, el TC se mantendría en una línea de eficacia directa de los DDFF para los trabajadores en su ámbito laboral. En otra línea de discurso sustancial, el TC se pronunció en el sentido limitativo de los DDFF, propiciando que estos sean definidos por el legislador y otras instituciones del sistema laboral, como son los sindicatos y empresarios, principalmente.

C. El uso de dispositivos de videgrabación volantes o drones.

por el que el TEDH avala que el empresario pueda revisar el contenido de las comunicaciones de sus trabajadores a través de un sistema de mensajería instantánea, incluso cuando se realicen desde una cuenta privada, y aunque no exista un perjuicio a la empresa que justifique el control. La Sentencia presenta la controversia sin respuesta a la limitación de la empresa frente a la injerencia en la vida privada de los trabajadores, especial en sus comunicaciones on-line. La empresa puede controlar el uso de esos servicios que pone a disposición del trabajador para evitar un uso indebido, sin necesidad de entrar en el conocimiento de la vida privada de los trabajadores. Un interesante estudio sobre las facultades de vigilancia y control de la empresa sobre los trabajadores en relación a la intimidad se encuentra en la referencia HOLGADO GONZÁLEZ, MARÍA, "La protección constitucional de la intimidad de los trabajadores frente al uso de las nuevas tecnologías de la comunicación", *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*, Valencia, 2014. En la misma línea, el análisis realizado por CIANCIARDO, J., *El conflictivismo en los Derechos Fundamentales*, Barañáin, 2000. expone en el punto 2 su visión razonando sobre las potestades de control empresarial del uso de los equipos informáticos en relación a los trabajadores y su intimidad. Véase también los comentarios de CARRILLO, M., "El uso de internet en la empresa", *Iuslabor*, nº 1, 2016. También CARRIZOSA PRIETO, ESTHER, "Las facultades de vigilancia y control en el centro de trabajo y su incidencia sobre el derecho a la intimidad de los trabajadores", *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*, Valencia, 2014, pág. 94 y ss.. Anteriores a estas referencias, como muestra del interés de la doctrina sobre los aspectos de la protección de datos en el entorno laboral, véase las ideas expuestas en la obra colectiva FARRIOLS I SOLÁ, A., *La protección de datos de carácter personal en los centros de trabajo*, Madrid, 2006.

Estos dispositivos consisten en incorporar una cámara a un pequeño dispositivo aéreo, que se ha calificado de aeronave y que se pilota por control remoto. Aparte de su regulación, todavía temporal, la Agencia Española de Seguridad Aérea se encarga de la regulación de operaciones con drones de hasta 150 kg, y a partir de ese peso se ha establecido una normativa a nivel europeo por EASA (*European Aviation Safety Agency*) En materia de protección de datos y DDFF, la videograbación y visualización de imágenes con datos personales por medio de drones es sumamente intrusiva y no exenta, como en los otros casos, de polémica. El uso de un dron para diversas finalidades muy lícitas todas ellas (Seguridad Nacional, prevención de delitos, ayuda a personas en riesgos diversos, localización de bienes y personas en entornos difíciles, por ejemplo; actividades comerciales, grabaciones de publicidad, junto con otras más frívolas: reportajes de bodas, reportajes de vacaciones) no impide que otros usos no sean lesivos para los DDFF, en especial el derecho a la protección de datos personales. En el año 2015 las Autoridades Europeas de protección de datos (GT29) aprobaron un Dictamen sobre drones que enumera las obligaciones que debe cumplir el operario de un dron antes de usarlo⁴⁴². Se debe cumplir la legislación sobre aviación civil pertinente, el tratamiento debe ser legítimo, proporcional y limitado a la finalidad para la cual se obtienen y procesan los datos. El dron capta datos de personas (imagen y en ocasiones, sonido), geolocaliza y transmite los datos a un sistema informático para su tratamiento. El problema reside en que un titular puede no ser consciente de la captación de su imagen por un dron, al ser muy difíciles de visualizar desde el suelo si el operario no lo desea, por lo que se pueden captar, procesar y almacenar imágenes sin conocimiento y sin consentimiento del titular de los datos. Por supuesto, como no se conoce quién recaba estos datos, ejercer los derechos ARCO resulta imposible por el titular. Se añade el riesgo de interconexión de drones por largo espacio de tiempo, que amplían y dificultan mucho más la posibilidad de violación de los DDFF. Si los drones están a cargo de las Fuerzas y Cuerpos de Seguridad del Estado, por lo menos se conoce quién los maneja, quién es el responsable del fichero o tratamiento; en

⁴⁴² Es el 01673/15/EN del 16 de junio de 2015. Véase en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf

estos casos el GT29 recuerda que los drones no pueden ser utilizados para la vigilancia indiscriminada, el tratamiento masivo de datos personales o la cesión, cruce o finalidades de obtención de perfiles de conducta personal. Se recuerda la obligación del cumplimiento de los DDFF para los fabricantes y para los gobiernos también. Se aconseja la creación de mapas en donde está permitido su uso, exceptuando por lógica las áreas pobladas, privadas o edificadas. Las Autoridades de protección de datos, sin embargo, excluyen el uso doméstico del dron en cuanto a DDFF, siempre que no afecte a éstos, en el que incluyen por lógica la protección de datos personales.

D. La biometría.

Según la AEPD y el GT29, se entiende por datos biométricos *aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos en un sujeto y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos*, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris ocular o la voz. El tratamiento de dichos datos ha evolucionado desde la referencia esencial a aquéllos datos que pueden ser considerados como *estáticos* o invariables a lo largo de la vida de la persona, como su huella genética, su huella dactilar o el iris, a otros que podrían denotar determinadas características de su comportamiento, tales como la forma de andar o el olor desprendido por el sujeto. La finalidad de la captación de este tipo de información personal es el acceso y control de un espacio físico, como puede ser el acceso a un puesto de trabajo. No siempre se debe mostrar, según las Autoridades de control de protección de datos personales, oposición a este tipo de tecnologías, pues son necesarias y muy prácticas en algunos aspectos de seguridad. Por ejemplo, en el DNI y en pasaportes, se emplean criterios biométricos homologados por el Ministerio del Interior. Otros casos a tener en cuenta como posibles y como proporcionados son el control de accesos a instalaciones de seguridad o de interés estratégico; recintos de uso laboral con riesgos y reservados a sólo un grupo de personas; accesos a lugares especiales, como laboratorios. El uso de la captación de datos biométricos para el acceso a un examen, a una piscina o a un simple

recinto de ocio, es claramente desproporcionado, según la AEPD, por el carácter invasivo de la tecnología biométrica. Su precio más asequible produjo una expansión de estos métodos de control, y pueden encontrarse controles de llegada y salida del centro laboral por huella dactilar, por ejemplo, en un simple taller de automóviles donde trabajan una decena trabajadores.

El nuevo RGPD analiza el asunto de datos biométricos en su texto. En el Considerando 51 RGPD se expone que *serán datos biométricos los que permitan la identificación o la autenticación unívocas de una persona física*. El artículo 4.14 del citado RGPD define los datos biométricos como *los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*. El tratamiento de estos datos biométricos se considera *tratamiento de categorías especiales de datos personales* en el artículo 9.1 RGPD y su tratamiento está prohibido, salvo en una larga serie de excepciones que se han comentado.

La obtención de datos personales biométricos debería quedar reservada al Ministerio del Interior para cuestiones de Seguridad y alguna instalación estratégica. Extender la recopilación de datos tan intensos como son los biométricos, es claramente invasiva de la libertad personal. Es cierto que, debido a la situación de terrorismo internacional, la sensación de inseguridad en la civilización europea se extiende. Eso no puede fundamentar, como multitud de doctrina y jurisprudencia han manifestado, la limitación de los DDFF. Debe ponderarse el caso concreto, como la AEPD y el GT29 han manifestado, no se pueden extender los usos legítimos de técnicas invasivas de la protección de datos sólo por miedo. El ATC 57/2007, de 26 de febrero, inadmitió el recurso de amparo de un trabajador de la Administración Autonómica de Cantabria por considerar vulnerados su derecho a la intimidad, pero el TC sí confirmó que los datos de la palma de la mano (datos biométricos) son datos personales y como tales, son objeto de protección⁴⁴³. La recabación de datos y el tratamiento de los mismos debe

⁴⁴³ ATC 57/2007 FJ 5: “Son sin duda, datos personales, con arreglo al art. 3 a) de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), que es la norma que

ser siempre de acuerdo con una finalidad legítima y pertinente, sólo según una necesidad para cumplir un fin determinado que el titular autoriza o que es imprescindible para proteger otro bien mayor. En esa misma línea doctrinal se expresó la STEDH en los asuntos 30562/04 Y 30566/04 (caso S. Marper vs. Reino Unido de Gran Bretaña) de 8 de diciembre de 2008, incluyendo los datos biométricos de huella dactilar en la categoría de datos personales, según el Convenio 108 y el artículo 8.1 del Convenio Europeo de Derecho Humanos. El Tribunal consideró que este tipo de datos y su tratamiento son susceptibles de ser tratados abusivamente, en especial por los poderes públicos, por lo cual se debería establecer por ley la protección debida para lo que denominó *calidad de ley*, para que ésta fuera lo suficientemente accesible y previsible, aportando una protección adecuada ante los posibles riesgos derivados de la arbitrariedad política o de interpretación de las Autoridades públicas. El Tribunal comparó la situación respecto a las huellas dactilares (y en cuanto a las pruebas genéticas, se verá) en su línea doctrinal y jurisprudencial sobre las escuchas telefónicas y la vigilancia secreta, donde se hizo imprescindible fijar los límites respecto al tratamiento de este tipo de datos invasivos. El TJUE dictó Sentencia de 17 de octubre de 2013 en el asunto C-291/12 (caso Schwarz) sobre las medidas de seguridad y datos biométricos en los pasaportes y documentos de viaje que fueran necesarios y expedidos por los Estados miembros de la UE. El Tribunal consideró en este caso como pertinente la toma de huellas dactilares o de la imagen del iris ocular con la finalidad de impedir el flujo ilegal de personas en el territorio de la UE, pero con la salvedad de verificar si se pueden concebir otras técnicas que no vulneren (o que lo hagan en menor medida) los derechos de las personas.

Las técnicas invasivas corporales deben, por tanto, proteger bienes importantes, como puede ser la seguridad de las personas o de las instalaciones ante posibles y reales

cumplimentó el mandato constitucional al legislador, establecido en el art. 18.4 CE, que dispone que la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. Los datos respecto de los que se ha previsto la garantía contenida en el art. 18.4 CE no son sólo los datos íntimos de la persona, protegidos éstos por el art. 18.1 CE, sino cualquier tipo de dato personal cuyo conocimiento o empleo por terceros pueda afectar a sus derechos (STC 292/2000, de 30 de noviembre, FJ 6)”

amenazas. Como ya se ha comentado, se plantea la duda para otras finalidades no tan importantes pero muy extendidas, como puede ser la toma de huella dactilar para la entrada en un centro deportivo. Quizá la mayoría de usuarios del centro se sientan cómodos con esa exhibición de seguridad, pero puede considerarse invasivo el almacenamiento y tratamiento de datos biométricos, que siempre debe tener suficientes garantías y finalidades legítimas, por lo cual, muy posiblemente sólo el Estado democrático, con la limitación y controles del legislador, puede autorizar este tipo de prácticas en empresas o instituciones⁴⁴⁴.

8.3.3 La información personal que se publica en los medios de comunicación.

La comunicación se puede definir como la acción y efecto de comunicar o comunicarse, el trato, la correspondencia entre dos o más personas, y nuestro Diccionario aplica también esta voz a la petición del parecer por parte de la persona que habla a aquella o aquellas a quienes se dirige, amigas o contrarias, manifestándose convencida de que no puede ser distinto del suyo propio. Los denominados medios de comunicación son actualmente instrumentos de transmisión pública de información, como emisoras de radio o televisión, periódicos o internet, entre otros ejemplos. Pueden ser utilizados para comunicar de forma masiva, para millones de personas, sin límites. Ese límite lo podrá establecer el emisor de la información o incluso su receptor, si no quiere verlo. Pero la información puede estar disponible con carácter ilimitado. Los ciudadanos acceden a material informativo audiovisual, de lectura o de imágenes a través de canales de comunicación. Para la sociedad actual estos canales son esenciales pues establecen el desarrollo de interacciones humanas muy importantes, que aumentan cada día. La necesidad de comunicación es una expresión de la necesidad intrínseca al ser humano de no estar solo, de relacionarse con otros, de enriquecerse como indivi-

⁴⁴⁴ GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 105. También TOMÁS MALLEN, BEATRIZ, "Privacidad vs. seguridad en el ámbito europeo", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Madrid, 2014, pág. 237.

duo y como sociedad. Los medios de comunicación lo hacen posible, desde el conocimiento y el debate social. Algunos de estos medios de comunicación son gigantescas plataformas tecnológicas supranacionales, que informan de cualquier asunto que acontezca en el planeta y con una función también de entretenimiento y de conocimiento nunca antes conocida por la humanidad. Por estas razones, no existe actualmente una definición única para los medios de comunicación, pues se pueden crear mañana mismo más formas que hasta hoy no se conocían, con objetivos, beneficios y usos diferentes⁴⁴⁵. La situación actual no está exenta de fuerte polémica. Para algunas sociedades contemporáneas o sectores sociales, los medios de comunicación son una herramienta eficaz y rápida de propagar contenidos de todo tipo. Sin embargo, para otros sectores de la sociedad, estas mismas herramientas son consideradas un vehículo de manipulación social y violación de DDFF. Los diferentes sectores sociales son conscientes del valor que poseen las comunicaciones y utilizan los medios de comunicación para exponer sus ideas o para intentar extender su visión de la realidad, con fines diversos. Lo realmente cierto actualmente es el poder innegable a nivel mundial de los medios de comunicación, más allá de la calificación tradicional del siglo XX como *cuarto poder*. Las comunicaciones son tanto sociales, de muchos o en abierto, como interpersonales, en reducidos grupos de intereses que se encuentran en la red, generando un pluralismo enriquecido. Ante todas estas ventajas existen inconvenientes debidos especialmente a la sobreexposición pública de ciertas actividades y/o conductas que anteriormente formaban parte de lo privado o de lo íntimo a través de datos personales. Las redes sociales y los medios de prensa amplifican sin límites previos todo tipo conductas y de informaciones, entre las que se incluye los datos de carácter personal. Establecer los límites a estas situaciones, generando una nor-

⁴⁴⁵ En estos momentos destaca el denominado *internet de las cosas*, la interconexión digital de diferentes objetos (cotidianos o no tan cotidianos, como un marcapasos cardíaco a una base de datos que informa a médicos y responsables del tratamiento de un paciente) y personas a través de internet. El concepto de internet de las cosas lo propuso Kevin Ashton en 1999. Un ejemplo actual: se están desarrollando actualmente nanopartículas para incluir en la medicación (tableta o cápsula) de un paciente, para que, una vez ingerida, informen al médico de tratamiento de la ingesta, a través de su teléfono móvil.

mativa que sea efectiva en un nuevo entorno no territorial en el que se cuestiona seriamente si la persona tiene realmente el control sobre sus datos personales o simplemente es un espejismo de la regulación, consistente más en un acto de fe en nuestro sistema jurídico y social que en una realidad⁴⁴⁶.

A. El derecho a la protección de datos y su relación con el derecho a la libertad de expresión e información.

La temática genera actualmente una discusión social intensa⁴⁴⁷. Cuando el artículo 20 CE fue redactado, los medios técnicos por los cuales los derechos expresados en sus

⁴⁴⁶ Véase las interesantes propuestas de BOIX PALOP, A., "La construcción de los límites a la libertad de expresión en las redes sociales.", *Revista de Estudios Políticos*, nº 173, 2016. También otras obras colectivas como RALLO LOMBARTE, A., *Derecho y Redes Sociales*, Navarra, 2010. GALÁN MÚÑOZ, A., *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación*, Valencia, 2014. GALÁN MÚÑOZ se expresa con las siguientes palabras ante el nuevo reto: "Así sucede, por ejemplo, con muchas de las informaciones de nuestra vida privada y profesional o de la de nuestros amigos y familiares que difundimos voluntariamente publicándolos en Internet sin ser realmente conscientes de que, una vez que lo hacemos, perdemos el control sobre unos datos que, por mucho que puedan parecer inocuos, pueden y de hecho son recopilados en grandes ficheros que, si son adecuadamente procesados, pueden servir para elaborar detallados perfiles de las personas a las que están referidos, reveladores aspectos esenciales de su intimidad, como su tendencia sexual, sus creencias religiosas o su ideología política"; cita de página 205. No se debería obviar que, como ya se ha expuesto, la privacidad se consagró como un derecho en EEUU por la polémica suscitada entre el juez Samuel Warren y la prensa norteamericana. El derecho fundamental a la protección de datos personales y su conflicto con los medios de comunicación se mantendría en este momento aún sin regular en España. Más recientemente DOMÍNGUEZ MEJÍAS, I., "Hacia la memoria selectiva en Internet. Honor, intimidad y propia imagen en la era digital a partir de la jurisprudencia española.", *Revista Iberoamericana de Ciencia, Tecnología y Sociedad - CTS*, nº 11, 2016, pág. 4 y ss.. El autor denomina la situación actual en internet como de "hiperdesarrollo fáctico de las libertades de información y expresión"

⁴⁴⁷ Ya existía con anterioridad a estas fechas de 2017. Véase COTINO HUESO, L., "Datos Personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público. Comentario al artículo 3.", *Comentario a la Ley de Protección de Datos de Carácter Personal*, Madrid, 2010, pág.

cinco puntos eran muy distintos a los que se tiene acceso en el presente. Los constituyentes no pudieron prever la aparición de redes sociales como *Facebook* o *Twitter*. La libertad de expresión se limitaba a una serie de medios de comunicación (periódicos, revistas, radio y televisión) y a unos pocos literarios que bien podían estar en manos de personas con formación amplia en letras y ciencias para ofrecer un contenido que no se va a tildar de controlado, pero sí era lento en su difusión y muy predecible. Las redacciones eran lugares llenos de máquinas de escribir, teléfonos fijos que se colapsaban, y después de pocos años, los más avanzados tenían lo que se llamaba un teletipo y posteriormente un fax, que llegó en la década de los años ochenta. Por tanto, su límite, también reflejado en el propio artículo 20.4, como respeto a los derechos reconocidos en el Título I CE, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la

295-321. Del mismo autor, en relación con obras colectivas muy interesantes, véase también COTINO HUESO, L., *Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías.*, Valencia, 2010. Véase la tesis doctoral de Jürgen Habermas en 1982, “La Estructura cambiante de la Publicidad” en su traducción del alemán original, “*Strukturwandel der Öffentlichkeit*”, publicidad entendido como hacer pública una información, como externo, no como espacios de anuncios sobre productos. La publicación de aspectos personales de otros, sean personajes conocidos por el arte, la ciencia, la política, el conocimiento o la chabacanería, o sean ciudadanos anónimos, los que conforman una civilización silenciosamente, se han convertido en una fascinación de masas. Se entraría de lleno en la filosofía y la sociología del Derecho para analizar qué estímulos conforman este tipo de conductas, en un dilema constante entre información e intimidad. Véase el epígrafe que se dedica a este asunto en PÉREZ LUÑO, A., *Derechos Humanos, Estado de Derecho y Constitución*, Madrid, 2010, pág. 351 y ss.. Se toma la cita cervantina del Quijote que utilizó PÉREZ LUÑO como anécdota, por un sentir de afinidad, expresada por el personaje de D. Diego de Miranda: “*ni gusto de murmurar, ni consiento que delante de mí se murmure; no escudriño las vidas ajenas, ni soy lince de los hechos de otros*”. Una referencia a tener en cuenta sería DE DOMINGO, T., *¿Conflictos entre derechos fundamentales?*, Madrid, 2001, pág. 285 y ss. El autor analizó en el año 2001 el conflicto entre el derecho a la libre información y el derecho a la intimidad, resaltando la conducta que el TC y el TS resolvieron. Para el autor el conflicto entre el derecho a la libre información y los datos íntimos (sólo analiza este asunto en función al derecho a la intimidad, no frente al derecho a la protección de datos) tendría su origen en la posibilidad de que alguna información basada en hechos veraces y de interés público sean datos íntimos. Se referenció con textos de SOLOZABAL ECHEBARRÍA y GARCÍA SAN MIGUEL.

protección de la juventud y de la infancia, no era fácil pero no resultaba prácticamente imposible de concebir. Además de los códigos deontológicos de los profesionales, hace 40 años que una noticia, un comentario, una opinión, una imagen, un video, un audio, estuviera en la calle en segundos se consideraba prácticamente imposible, como era aún más imposible que esa información fuera realizada en su contenido y en su envío por un simple ciudadano que estaba allí con un pequeño dispositivo de grabación, edición, eventual almacenamiento y envío por medios de telecomunicación. La Jurisprudencia del TC y del TS han desarrollado una buena parte de la doctrina para los casos de colisión de derechos, entre el artículo 20 y el artículo 18, pero sólo para su punto 1, no tan extensa para su punto 4, la protección de datos personales. La libertad de expresión e información suelen entrar en conflicto con el derecho a la protección de datos personales, pues informar, difundir noticias y opiniones, imágenes, comentarios, a través de un medio de comunicación, tiene serias implicaciones en el tratamiento de datos personales que afectan a la intimidad de las personas, entre otros derechos que entran en colisión. Como se ha dicho, ningún derecho fundamental es absoluto, por lo cual se deben establecer límites que favorezcan la protección de los derechos y libertades de todos los ciudadanos⁴⁴⁸.

Existen, además, normas que específicamente regulan la actividad informativa profesional, como la cláusula de conciencia por la Ley Orgánica 2/1997 de 19 de junio. Los que se consideren afectados por el ejercicio de la libertad de expresión pueden contar con el llamado derecho de rectificación, desarrollado por la Ley Orgánica 2/1984 de 26 de mayo, que se agota con la rectificación de los hechos que le aluden y se con-

⁴⁴⁸ PAUNER CHULVI, C., "Implicaciones del futuro Reglamento europeo sobre protección de datos en la libertad de información", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Madrid, 2014. Muy anteriormente se expresaron las ideas de BUSTOS GISBERT, R., "El concepto de libertad de información a partir de su distinción de la libertad de expresión. ", *Revista de Estudios Políticos*, nº , 1994, pág. 261-290. El autor realizó una distinción entre el derecho a la libertad de expresión y el derecho a la libertad de información, en un contexto de crítica doctrinal. Dirigió también una tesis doctoral de GONZÁLEZ CIFUENTES, C., *El derecho a la intimidad de los altos cargos*, Salamanca, 2011. que se cita como referente especializado en la intimidad de altos cargos, con alguna mención a la protección de sus datos.

sideren por el afectado inexactos, cuya divulgación pueda perjudicarle. Una difusión de información de relevancia mundial, con acceso libre por cientos de miles de personas en cuestión de segundos no era predecible cuando se realizaron estas leyes. Por tanto, la libertad de expresión e información frente al derecho a la protección de datos personales está aún por definir. En *internet* puede apreciarse el creciente número de informaciones sobre cuestiones públicas, pero también sobre datos privados que se entienden bajo la ley de protección de datos. Surgen innumerables preguntas, como puede ser si se considera libertad de información o libertad de expresión que se exponga en *internet* (*YouTube*, plataforma de videos) información relativa a Fuerzas de Seguridad del Estado y sus actuaciones (de indudable interés público amparado por la libertad de expresión e información), cargos públicos y sus coches oficiales o sus movimientos en la esfera propiamente privada (recogida de sus hijos en su colegio, ir a un restaurante, visitar una tienda). Los implicados y sus reacciones son diversas, desde hacerse voluntariamente fotos (*selfis*) con las personas que están allí, a no querer la difusión de esas informaciones por considerarlas privadas o incluso íntimas. Esto en cuanto a la esfera pública informativa, es decir, personas o cuestiones que tiene el calificativo de público, por su cargo, su profesión o su popularidad en los medios informativos. Otro caso es que las personas no conocidas se vean introducidas en una red de información y divulgación a través de la publicación no deseada de datos personales, de situaciones que, en su mayoría, no pueden ser controladas. No es la misma situación informar sobre cuestiones públicas desde medios informativos que las situaciones de divulgación de datos personales a través de redes sociales, que no son de interés público⁴⁴⁹.

⁴⁴⁹ Véase los ejemplos de FERNÁNDEZ BARRERO, MARÍA ÁNGELES ; GUIRADO BORREGO, VÍCTOR, *Comunicación y desarrollo en la era digital. Congreso AE-IC 3, 4 y 5 de febrero de 2010*, Madrid, 2010, . Se destacan los usos del ámbito profesional periodístico en las redes sociales; en este momento se continua con esos usos sin limitación.

La AEPD suplió, de nuevo, en el informe 0132/2010, la ausencia de regulación de este aspecto, que sí fue previsto en el artículo 9 de la Directiva 95/46/CE⁴⁵⁰.

El Informe 0132/2010, se redirige a la Jurisprudencia del TC en cuanto a los conflictos entre el artículo 18 y el 20 de la CE en general. En un resumen de estas Sentencias, se estableció una regla general: *el derecho del artículo 20 prevalecerá en los supuestos que tengan como contenido información veraz y de relevancia pública, sobre materias y personas a su vez relevantes públicamente*, lo que se ha denominado por la doctrina *excepción periodística*⁴⁵¹. En cuanto al derecho a la protección de datos personales, el aludido Informe se basó en la SAN 3658/2009, de 09 de Julio, la cual analizó la publicación de imágenes por un medio de comunicación de una víctima de los atentados de Madrid el 11 de marzo de 2004 durante su estancia en el hospital. La AN consideró que la imagen era un dato personal y su tratamiento había sido excesivo, teniendo en cuenta que no se contaba con el consentimiento de los afectados, ni se encontraba dicho tratamiento amparado por la libertad de información y, en todo caso, se había producido un uso desmedido de la imagen de las personas afectadas como

⁴⁵⁰ Cuyo enunciado es el siguiente: "En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados Miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión."

⁴⁵¹ La denominada excepción periodística en la Directiva 95/46/CE no fue interpretada con el mismo criterio por los Estados miembros. El GT29 así lo reflejó en diferentes informes, resaltándose por su presencia en el tiempo el Informe "sobre Protección de Datos y Medios" del año 1997. Este informe concluyó, sin embargo, que, pese a las diferencias, el ejercicio del derecho a la protección de datos en los medios de comunicación era muy similar, debido a la excepción periodística y al particular tratamiento de los diferentes Tribunales Constitucionales de la misma, dando preferencia al derecho a la libertad de expresión e información cuando se encontraba en colisión con el derecho a la protección de datos personales. A ello se añadía el respeto de las reglas deontológicas de la profesión en cuanto al respeto de la vida privada y de la intimidad de las personas, junto con sus normas autorreguladoras en diferentes Estados miembros. Véase la exposición de PAUNER CHULVI, C., "La actividad periodística en los ordenamientos nacionales y europeos sobre protección de datos", *Hacia un nuevo derecho europeo de protección de datos*, Valencia, 2015, pág. 582-586.

dato personal puesto que la finalidad y el carácter noticiable de la información se cumplía suficientemente sin ser necesario incluir imágenes directas de los pacientes. La sentencia fue matizada por la AEPD con el sentido de la Directiva 95/46/CE. El Informe entendió que la excepción periodística a la aplicación de la normativa sobre protección de datos “debe entenderse como *manifestaciones del principio de proporcionalidad* consagrado en el artículo 4.1 de la LOPD, a cuyo tenor, los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido” (...) “De este modo, la información a divulgar debería ser la que resulte necesaria para que informaciones que revistan la relevancia pública a la que se ha venido haciendo referencia puedan ser conocidas por los ciudadanos. Del mismo modo, cualquier información adicional que, conteniendo datos de carácter personal, resulte irrelevante para que la información facilitada tenga el carácter noticiable constitucionalmente requerido debería ser objeto de un *previo procedimiento de disociación*.”

En una línea doctrina similar, la STS 1105/1999, de 18 de febrero, condenó a un periodista por un delito de revelación de secretos, al acceder y divulgar la noticia de la existencia en una cárcel de dos reclusos, con *imágenes, nombres y apellidos*, los cuales eran enfermos de SIDA y trabajaban en la cocina del centro penitenciario. El TS consideró que *la noticia era la presencia de enfermos de SIDA en la cocina y no la identidad de los mismos*, por lo que existía delito. La misma doctrina se repitió en el ATC 298/2000, de 13 de diciembre, que inadmitió el recurso de amparo interpuesto contra la STS de 18 de febrero de 1999. Otra resolución mencionable en este sentido sería el ATC 155/2009, de 18 de mayo, que conoció el caso de una revista que publicó el listado de médicos y farmacéuticos para documentar un reportaje sobre el exceso de recetas y usos de antibióticos. Se consideró en este ATC que no existía prevalencia del derecho a la información al producirse una intromisión en el derecho a la protección de datos (o de autodeterminación informativa) El ATC confirmó la Resolución de la AEPD de 5 de septiembre de 2005 y la SAN de 12 de enero de 2007, admitiendo que

se produjo un tratamiento no consentido y una publicación indebida de datos personales de médicos y farmacéuticos. Todas estas resoluciones son aplicaciones del principio de proporcionalidad⁴⁵².

En el entramado informativo y de expresiones vertidas en la red, se pueden diferenciar dos aspectos que se interrelacionan continuamente, como son, en primer lugar el ámbito de los que se van a denominar usuarios anónimos, ciudadanos que a su vez son titulares de datos personales pero que usan los medios de comunicación para ejercer su libertad de expresión e información, al mismo tiempo que comunican con otros usuarios y consiguen lo que ahora mismo tanto se promueve: el reconocimiento social, a través de seguidores en internet; y un segundo ámbito, el de los profesionales de la información y la comunicación, los que a través de múltiples plataformas de medios generan información (cuya etimología es la acción de dar forma a algo), dan forma a un hecho para su transmisión a través de un medio de difusión, en este caso, los *mass media* o medios de comunicación de masas, recibidos simultáneamente por una gran cantidad de individuos. Los medios de comunicación, de los que lógicamente forma parte *internet* y sus redes sociales en la actualidad, tienen como finalidad clásica formar, informar y entretener a sus usuarios, siendo en este momento también un *medio de intercomunicación*, pues el usuario no recibe solamente la información, también puede interactuar con el medio y con los profesionales que se muestran *ejerciendo su derecho a la libertad de expresión e informando al mismo tiempo que se es informado*. Se diferencian estos medios profesionales de los usuarios individuales (solos o en grupos de interés) en que los objetivos de los medios de comunicación profesionales se basan en el beneficio económico del empresario o grupo empresarial que los dirige, habitualmente concentrado en grandes grupos de comunicación multiplataformas (internet, radio, televisión, como algo residual, prensa o libros), e influir en su

⁴⁵² En este sentido el ATC alega que “Tal intromisión responde a un objetivo legítimo, provocar un mayor impacto de la publicación en los lectores de un artículo encaminado a informar sobre el abuso en la prescripción de antibióticos y los perjuicios para la salud derivados del mismo, que sin embargo podía haberse alcanzado por otros medios, sin la referida invasión en la esfera personal de médicos y farmacéuticos.”

público, financiándose mediante la publicidad, un aspecto muy importante, pues los empresarios que publicitan sus productos y servicios en los medios son empresas, nada es gratis en los medios, el precio es la influencia en la decisión de compra del usuario-consumidor ante un mercado. Se analizan a continuación estos dos ámbitos o situaciones de estudio, teniendo en cuenta que en la realidad se encuentran interconectados.

A.1 La libertad de expresión e información de los usuarios anónimos en las redes sociales y otros medios de comunicación.

Como un posible punto de partida para establecer límites a la confrontación del derecho a la protección de datos y el derecho a la libertad de expresión e información en las redes sociales a través de internet, un amplio sector de la doctrina entiende que los límites no tienen por qué ser diferentes en su núcleo a los límites que se aplican al derecho a la libertad de expresión e información en otros canales o medios de comunicación. Aunque existe un potencial de maximización de los efectos negativos en la sociedad de la información vertida en redes sociales, también es cierto que fomentan exponencialmente el pluralismo democrático y ese mismo riesgo de ofensa se transforma en potencial de respuesta ante las expresiones negativas, confrontando ideas que permitan una clarificación, salvo que determinados contenidos contrarios no se difundan adecuadamente; en este supuesto, se estaría ante un impedimento a la pluralización aumentando los riesgos sociales de radicalización de grupos o personas, que los responsables sociales deben compensar. No se debe olvidar que las redes sociales son también en la actualidad una manifestación de las patologías sociales e individuales, dignas más del estudio de la psiquiatría social que del Derecho. Con todo, las expresiones en *internet* y en las redes sociales son una forma de expresión dentro del marco constitucionalmente protegido, lo que aporta la diferencia es el canal o medio de comunicación que se emplea y la dimensión del daño, tanto en materia penal co-

mo civil⁴⁵³. La dimensión del daño no se ha podido definir todavía y está en manos de los legisladores. BOIX PALOP considera que las expresiones en redes sociales, por muy abyectas que sean, no pueden trascenderse de tal modo que las consecuencias sobrepasen los límites de la proporcionalidad. Son, para el autor citado, sólo expresiones, no son hechos de violencia física efectivos. Lo que sí es completamente cierto es que la efectividad de los mensajes de odio se suprime con la ignorancia de los mismos, con no verlos, no contestarlos y no seguirlos en las redes sociales⁴⁵⁴. Sería más sensato y un síntoma de madurez en una sociedad democrática, en la que el pluralismo y la libertad de expresión e información sean vehículos para convencer, que las redes sociales no sean un cauce para insultar ni una excusa para reprimir conductas, pero que, en cualquier caso, la utilización de datos personales sea restrictiva, en especial imágenes⁴⁵⁵. La sencilla trazabilidad de las conductas en las redes sociales facilita que las verdaderas conductas lesivas puedan ser perseguidas e identificados sus

⁴⁵³ LLANEZA, PALOMA, "Aspectos legales: periodismo, ciudadanos y la ley", *Periodismo ciudadano. Evolución positiva de la comunicación.*, , 2011.

⁴⁵⁴ Véase BOIX PALOP, A., "La construcción de los límites a la libertad de expresión en las redes sociales.", *Revista de Estudios Políticos.*, nº 173, 2016. El autor adopta una posición a favor de la libertad de expresión, fuera la que fuese, minimizando las consecuencias del mal uso de las redes sociales. Presenta casos muy mediáticos, en los que realmente aplicando el principio de proporcionalidad los Tribunales no han apreciado unas conductas antijurídicas graves. Pero no analiza las consecuencias en los ciudadanos que no tienen defensa ante las conductas irrespetuosas de otros, mucho menos divulgadas pero lesivas en los individuos y en sus entornos.

⁴⁵⁵ El asunto del derecho a la propia imagen se configura también como derecho fundamental autónomo e independiente: "se configura como un derecho de la personalidad, derivado de la dignidad humana y dirigido a proteger la dimensión moral de las personas, que atribuye a su titular un derecho a determinar la información gráfica generada por sus rasgos físicos personales que pueden tener difusión pública. La facultad otorgada por este derecho, en tanto que derecho fundamental, consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad informativa, comercial, científica, cultural, etc. perseguida por quien la capta o difunde" STC 81/2001, de 26 de marzo (FJ 1). En el mismo sentido STC 156/2001, de 2 de julio (FJ 2) en la cual se afirma que la imagen es "el primer elemento configurador de la esfera personal de todo individuo, en cuanto instrumento básico de identificación y proyección exterior y facto imprescindible para su propio reconocimiento como sujeto individual"

autores. Y no se debe olvidar, como se ha expuesto, que las empresas de redes sociales (*Facebook o Twitter*) que ofrecen este tipo de servicios deben obtener beneficios, no son organizaciones sin ánimo de lucro, por lo que harán todo lo que esté a su alcance para atraer y fidelizar al mayor número de ciudadanos como usuarios, persiguiendo siempre el objetivo empresarial y no estando tanto interesadas en el fomento de la pluralidad de opiniones ni en la merma de los DDFF como en sus resultados económicos, por lo que no se fomenta la pluralidad, la calidad del debate, o el libre contraste de las ideas⁴⁵⁶. Por todo ello, noticia puede ser un hecho a nivel internacional o nacional pero muchos hechos publicados en *internet*, dentro de sus plataformas de redes, que ahora son prácticamente todos, tienen un interés para un reducido número de personas, pero no por ello menos trascendente en sus consecuencias. Para una pequeña población puede ser importante las fotos sobre un hecho local transmitidas a través de los dispositivos móviles a todos sus grupos de redes sociales. Eso no es anti-jurídico, muy al contrario, puede ser una forma de comunicar asuntos de interés general. El mismo sistema sirve para otros fines antijurídicos, como puede ser conductas de injurias y vejaciones, tan comunes en este momento, parece ser, entre escolares y estudiantes, pero también en el ámbito laboral o asociativo. A las personas sensibles se les afrenta en situaciones poco recomendables y muchas de ellas no se saben defender. En el mundo actual, para micro sociedades, el uso de las tecnologías se ha convertido en una forma de comunicar violando los DDFF, convirtiendo el derecho a la información y expresión junto con el uso de las comunicaciones en el medio apropiado para realizar conductas lesivas. Lo que puede parecer una broma, en la mente y sensibilidad de otros puede no serlo. Son hechos que no pueden ser considerados jurídicamente punibles, pero son realmente maliciosos, dañinos y éticamente reprochables⁴⁵⁷. Se marca la diferencia entre la información y la difamación o burla, entre la

⁴⁵⁶ Véase la posición de LÓPEZ RICHART, J., "Difamación en la web 2.0 y responsabilidad civil de los prestadores de servicios de alojamiento", *Derecho privado y Constitución*, nº 26, 2012, pág. 143-201. Las empresas de contenidos no tuvieron el menor interés en su momento, con la LSSI (ley de Servicios de la Sociedad de la Información) de regular estos aspectos.

⁴⁵⁷ La conocida frase es muy aplicable: jurídicamente no punible pero moralmente o éticamente reprochable. No se va a entrar en la teoría del delito, que permite resolver cuándo un hecho humano es

sátira crítica y el insulto. Las definiciones son claras. Informar significa dar forma o describir, enterar o dar noticia de algo; fundamentar, inspirar (por ejemplo, la expresión *valores que informan el sistema democrático*); difamar significa desacreditar a alguien, de palabra o por escrito, publicando algo contra su buena opinión y fama, en curiosa conexión con el verbo divulgar, según nuestra RAE, que tiene el significado de publicar, extender, poner al alcance del público algo. La sátira es un arte, es una composición en verso o prosa cuyo objeto es censurar o ridiculizar a alguien o algo. Un discurso o dicho agudo, picante y mordaz, dirigido a censurar o también puede poner algo en bajo concepto y estima, pero, sin lugar a dudas, con humor. El insulto es una ofensa hacia alguien provocándolo e irritándolo con palabras o acciones, ofensa, del verbo ofender que la RAE, sorprendentemente, define como humillar o herir el amor propio o la dignidad de alguien, o ponerlo en evidencia con palabras o con hechos. Ofender significa también ir en contra de lo que se tiene comúnmente por

calificable de delito, sólo se aportan unos ejemplos: los videos sobre caídas y golpes. No se entiende qué se encuentra de divertido en ese tipo de circunstancias, que muy bien pueden ser dolorosas y lesivas para sus protagonistas. También la publicación de situaciones desagradables, embarazosas. Una cantidad de información dentro de las redes que está indexada con nombres y apellidos a imágenes de todo tipo, fotografía, video y audio acompañando su contenido. Información personal que muchos comparten voluntariamente, pero otros no comparten, les hacen estar dentro de un conocimiento general de sus datos personales sin su voluntad y sin su conocimiento. Lo que es un derecho para unos, es una violación de sus derechos en otro. Un caso llamativo: páginas *web* que almacenan videos en los que se puede ver a ciudadanos/as desnudos o en *topless*, con la parte del torso descubierta, en playas o piscinas. Si bien es cierto que se puede solicitar su retirada, cuando esto sucede ya ha sido publicado todo el contenido; en ese momento la conducta lesiva se ha producido. Otro ejemplo llamativo: las redes de acoso a menores en colegios u otros espacios. Llegado el momento, las situaciones pueden ser tan preocupantes como la noticia de la muerte por suicidio de un pequeño de 11 años por acoso escolar. Lo que antes no pasaba de ser una situación de *pandilla* y, por tanto, controlable, había trascendido de tal manera a otros alumnos y a otras personas por las redes sociales, que el implicado se sentía expuesto. Presumiblemente sufría de tal modo, que, para no ir al colegio, se quitó la vida. ¿Cómo se puede abordar y evitar este tipo de sucesos? La misma rigidez que se pide a las empresas para la seguridad y tratamiento de datos personales no se aplica en absoluto a los particulares que realizan todo este tipo de acciones, aunque la AEPD haya confirmado que estas personas (víctimas de otras y su conducta) están protegidas por la LOPD.

bueno, correcto o agradable, pero también como hacer daño a alguien físicamente, hiriéndolo o maltratándolo como persona, sentirse humillado o herido en el amor propio o la dignidad. Con estas definiciones como base, el presente estudio se orienta desde la libertad de expresión e información, respetando las opiniones diversas, por muy opuestas y críticas que parezcan (e incluso atendiendo a la sátira como expresión del genio literario), pero teniendo como límite el respeto debido a los DDFF para no humillar, no herir y no ofender. A ello contribuye el derecho a la protección de datos personales, límite de la libertad de expresión e información.

La ponderación se aplica a los medios de comunicación, obligados por la Constitución y la Jurisprudencia de nuestros Tribunales. Esa misma ponderación no se aplica, ni tan siquiera la medida, en las conductas de ciudadanos anónimos que se ven dentro de las redes. Por supuesto que la comunicación de todos esos datos no es necesaria, ni pertinente. Por supuesto que es excesiva. Y puede llegar a ser delictiva. Pero no se puede, hasta hoy, realizar acción alguna contra este tipo de prácticas generalizadas para que no se produzcan. Los *paparazzi* eran para los famosos en general. Parece ser que ahora, en la nueva generación, todos son *paparazzi* de todos, para subir a la red la foto o el video que más afinidad consiga en cualquier red social. La información no es sólo ejercida por una profesión, las noticias no tienen ese ámbito y relevancia pública que promulga el TC y el TS. Simplemente basta con que un grupo social quiera imponer una forma de extorsión y poder fuera del sistema jurídico para que la información, dentro del grupo relevante, tenga consecuencias personales, a veces nefastas, y por supuesto no tenga ninguna consecuencia jurídica, pues no se puede probar, en la mayoría de los casos, la directa acción del mal uso de las redes sociales sobre determinadas consecuencias o incidentes en la vida de un ciudadano⁴⁵⁸.

⁴⁵⁸ Como en este caso real: un muchacho hace siete años participa en las fiestas de su pueblo, con las peñas y la diversión, consume grandes dosis de alcohol y participa en grupos de fotos en las que se le pudo ver seriamente ebrio, en condiciones poco adecuadas. Pasan los años, y el joven se convierte en jefe del departamento comercial de una empresa internacional, cambia su imagen a una más acorde con su nuevo trabajo y vida social. En el pueblo, al enterarse de su ascenso laboral, se acuerdan de esas fotos de peña y de fiesta local y las publican, con nombres y apellidos, en una red social. El asunto

Cualquier información personal en los medios puede estar bajo la tutela del derecho a la protección de datos personales en cuanto que un dato de carácter personal es cualquier información que permita la identificación de la persona titular o la haga identificable. El derecho fundamental a la protección de datos otorga a la persona la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos. Este derecho, en muchos casos de divulgación informativa, no pasa de ser enunciativo, estando más en las circunstancias y en la previsión del titular que de los medios para hacerlo efectivo. Cuando la situación derive en un claro delito, nos encontraremos con el fenómeno y posible delito de *ciberbullying* o *ciberacoso*, aunque muchas de las conductas van más allá en sus consecuencias que el simple acoso.

Ya que la regulación de protección de datos no otorga efectiva protección a esos casos, ¿se puede tratar esta temática desde el derecho a la intimidad, al honor y a la imagen? Es algo a tener en cuenta, pues el TC reconoció en varias Sentencias que estos tres derechos, presentes también en el artículo 18 CE, están íntimamente relacionados⁴⁵⁹, aunque es muy difícil compaginar ambos con los hechos. El legislador no dio una definición del derecho al honor en la CE ni en otras leyes. El ámbito de los derechos del artículo 18 CE son de difícil determinación, especialmente frente al derecho a la información, artículo 20 CE. Existe, en todo caso, un *núcleo duro* del contenido de los DDFF recogidos en el artículo 18 CE: al ser derechos inherentes a la persona, no se puede considerar que aumentan o decrecen totalmente, existe un mínimo de res-

trasciende a la empresa empleadora, que le despiden fulminantemente, alegando simple inadecuación para el puesto. El detonante fueron las fotos, que además se enviaron estratégicamente a los responsables de personal de la empresa empleadora por individuos debidamente cubiertos por el anonimato. En las palabras de BOIX PALOP, los mensajes (y se añade, las imágenes) se almacenan no solo en la memoria colectiva, sino también en la memoria digital de servidores y redes. Obra citada, página 60.

⁴⁵⁹ Como pueden ser las SSTC 170/ 1994, de 7 de junio, FJ 4; también 176/1995, de 11 de diciembre, FJ 5. Sobre esta cuestión las reflexiones de MAGDALENO ALEGRÍA, A., *Los límites de las libertades de expresión e información en el Estado social y democrático de Derecho.*, Madrid, 2006, pág. 292-297. Citando a VIDAL MARIN, aporta en estas páginas una definición del derecho al honor extrapolable a este epígrafe: “el derecho al honor es aquel derecho derivado de la dignidad de la persona, consistente en el derecho a ser respetado por los demás”.

peto social, como es la negación de amparo constitucional a la información injuriosa, lesiva y ofensiva⁴⁶⁰. Al igual que se debe tener en cuenta la participación del individuo en el sistema social, por lo cual el honor y la dignidad tendrán mayor o menor extensión en función del nivel de participación en la sociedad y su comportamiento dentro del mismo, el respeto se debe ganar por el individuo dentro de la sociedad en la que participa, y la sociedad debe respetar al individuo dentro de las normas.

Surge el principio de ponderación de derechos como posible vía de solución en caso de conflicto entre la protección de datos personales y la libertad de expresión e información. Llamativo es para una parte de la doctrina, que una institución de la Administración del Estado –aun independiente- como es la AEPD, sea el órgano que efectúa la ponderación de libertades públicas y otros derechos fundamentales⁴⁶¹. Esto ha cambiado en parte después de la Sentencia del TJUE en el caso *Google*, pero no deja de ser muy llamativa la actuación de la AEDP en cuanto a órgano que evalúa la relevancia o no de la defensa de los derechos de la persona, derechos de rango constitucional. Porque en este punto ha quedado ya claro que de lo que tratamos no es tanto de datos aislados a los que se les asigna más o menos protección y por lo que se tienen más o menos derechos, defendidos por una respuesta de nuestro sistema legal por multas administrativas y acciones judiciales de diferente clase y calado. Tratamos de la defensa y protección efectiva de los Derechos Fundamentales en toda su amplitud, dentro de un escenario no territorial, por medio de recursos siempre obsoletos que no alcanzan a los avances tecnológicos, vehículos inocentes o no tan inocentes de la continua violación de derechos fundamentales, lo cual hace que la llamada protección sea tan inefectiva como sólo recurrente a nivel nominal, como una declaración bien intencionada de buenas obras que difícilmente se pueden realizar (lo que la doctrina denominó *fumus bonis iuris*).

⁴⁶⁰ STC 99/2002, de 6 de mayo, FJ 7.

⁴⁶¹ COTINO HUESO, L., "Datos Personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público. Comentario al artículo 3.", *Comentario a la Ley de Protección de Datos de Carácter Personal*, Madrid, 2010, pág. 295-321. Véase también en este sentido BOIX PALOP, A., "La construcción de los límites a la libertad de expresión en las redes sociales.", *Revista de Estudios Políticos.*, nº 173, 2016.

Desde una perspectiva civil de protección y defensa de los derechos de la personalidad, la doctrina planteó que la intimidad y los derechos de la personalidad no solamente son obligaciones y derechos de un solo individuo, pero es la persona titular de los derechos (como puede ser la intimidad) quien aporta el mayor grado de responsabilidad en la gestión de los mismos, exigiendo al sistema jurídico una tutela efectiva ante las vulneraciones e intromisiones de terceros. En la sociedad de la información y las telecomunicaciones el titular de derechos no ejercería adecuadamente un filtrado de sus expresiones y, por tanto, no es consciente de la relevancia jurídica de sus actos pues su conducta está inducida por las emociones⁴⁶².

A.2 La libertad de expresión e información a través de los medios profesionales de comunicación.

Entrando en el tratamiento de los datos personales por los profesionales del periodismo, el profesional se encontraría confrontado con miles de datos en todo tipo de me-

⁴⁶² Véase en este sentido las reflexiones de DE LA TORRE OLID, FRANCISCO; CONDE COLMENAREJO, PILAR; "Consideraciones críticas en torno a la autogestión y preservación de la intimidad en un escenario de riesgo", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, , 2014, pág. 42 y ss. Los autores confrontan los artículos 18 CE y 68 CC, entre otros, considerando el artículo 10 de la CE como referente iusnaturalista de la dignidad de la persona. Se extiende la intimidad desde el mismo momento del *nasciturus* (con la publicación de ecografías de no nacidos) hasta cualquier tipo de dato íntimo, que incluye todo lo que la mente (que no el pensamiento) puede imaginar. Es lo que los autores denominan *sociedad del riesgo*, en la que se incluye todo tipo de grabaciones de vídeo, no tan sólo las que los Cuerpos y Fuerzas del Estado realizan, también las privadas, las comerciales y las invasivas empresariales. Es lo que se pudo considerar como "una provocación generalizado para facilitar que las personas divulguen mediante nuevas tecnologías datos íntimos, arrastrando a la población con modas que centran en la imagen, en la opinión y en el pensamiento la posibilidad de divulgar lo propio (a través de prácticas tentadoras, como el *selfie* o la posibilidad de encontrar seguidores de nuestras opiniones)". Los autores aportan como solución a esta situación una educación en valores, más que una sobreproducción normativa, para conseguir lo que denominaron *opinio iuris*, sin obviar la tutela de los DDFF, los cuales fueron considerados por los autores como poco protegidos por el Estado y las AAPP.

dios y soportes que debe gestionar. Sin una regulación apropiada para la gestión de la información, al ciudadano se le ofertan cuestionables formatos informativos. Los legisladores y la doctrina, hasta la fecha, no han abordado la situación en función de los nuevos medios de comunicación. Un video en *YouTube* puede convertirse en un fenómeno viral si se expone en los medios de comunicación masivos, como puede ser una emisora de televisión, por lo que afecta, no sólo a la vida de una persona, sino a todo un colectivo político, sindical, societario, entre otros ejemplos, con influencia positiva en algún caso y con gran riesgo para otros casos. La prevalencia del derecho a la información sobre el derecho a la protección de datos personales se otorgó hasta ahora por los Tribunales a favor de los medios profesionales del periodismo, (como se comenta en distintos epígrafes) evitando, muy posiblemente, delimitar adecuadamente ambos derechos. La AEPD no delimitó (hasta la fecha presente) al periodismo ni al derecho a la libertad de expresión, sólo resolvió sobre casos concretos que le fueron planteados. Los periodistas, generalmente, ignorarían la LOPD y el derecho fundamental a la protección de datos: todos los datos personales que tienen en sus Pc, agendas de todo tipo (en papel o electrónicas), en teléfonos móviles, entre otros soportes, son datos de sus titulares, por tanto, sin consentimiento de los titulares no pueden ser tratados. Simplemente al encontrarse en sus archivos se convierten en ficheros con datos personales y estos profesionales se convierten en responsables de los mismos y de su tratamiento. Por supuesto, como los titulares no saben qué información consta en qué soportes por quién no podrían ejercer sus derechos ARCO. La actividad del periodismo está sujeta a la normativa sobre protección de datos personales (LOPD y su Reglamento, además del nuevo RGPD). En toda la actividad periodística se tratan datos personales, antes y después de cualquier publicación. En muchos casos, los datos tratados son de especial consideración, son datos sensibles, con especial protección por las normas constitucionales. Se recuerda también especialmente que los datos de carácter personal sólo pueden recogerse cuando sean *adecuados, pertinentes y no excesivos* en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, tal y como se regula en el artículo 4.1 de la LOPD y los artículos 8.2 y 8.4 del Reglamento. Se podrían añadir los

artículos 4.2 de la LOPD y el artículo 8.3 del Reglamento por los que los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles (o distintas en algunos casos que ha tratado la AEPD) con aquellas para las que los datos hubieran sido recogidos. El artículo 4.3 LOPD mantiene que los datos deben ser exactos y puestos al día, lo que sería prácticamente imposible en el mundo periodístico, que se basa, en muchos casos, sobre especulaciones e inexactitudes que suelen llevar a la investigación de hechos diversos. La cancelación de datos no se puede pensar para esta profesión, pues para la agenda y para la información que tratase un periodista algo así sería impensable, su patrimonio profesional se basa en la historia de las personas. Para dar más argumentos a esta exposición, el artículo 6.1 LOPD impone que el consentimiento del titular sea inequívoco e informado, salvo que la ley disponga otra cosa. La LOPD entre las excepciones que regula, la única que se puede aplicar a la práctica del periodismo es la de *datos en fuentes accesibles al público* del artículo 3.j) LOPD, con un listado muy restrictivo, y cuyo tratamiento sea necesario para satisfacer un interés legítimo perseguido por el responsable del fichero (periodista, por ejemplo) o por el tercero al que se comuniquen los datos, con una importantísima salvedad: *siempre que no se vulneren los derechos y libertades fundamentales del interesado*. Las sanciones de la AEPD por vulneración de los mandatos de la protección de datos fueron muchas y variadas, en especial por publicar informaciones procedentes de páginas *web* o de otras fuentes accesibles en *internet*, pero que la AEPD y la AN consideraron que su publicación viola DDFF⁴⁶³ En este asunto, el artículo 7 LOPD convertiría en ilegales todos los millones de datos que se encuentran en cualquier soporte de los profesionales de la información, los cuales identifican sin problemas a políticos, líderes religiosos, líderes sindicales, personas en sus creencias, en su tendencia sexual, en su estado de salud, por citar algunos ejemplos. Los medios y

⁴⁶³ Entre otras, SAN 4399/2008, de 5 de noviembre. La AEPD y la AN consideraron que una web e Internet no son medios de comunicación, sino canales de comunicación, por lo que no se consideran fuentes accesibles al público y, por tanto, los datos personales que se tratan necesitan el consentimiento del afectado o titular. Esta doctrina de la AN no siempre es uniforme y está sujeta a variación. En otro caso, SAN 2148/2007, admite que lo publicado en una web es una publicación en un medio de comunicación.

los periodistas no solicitan ningún tipo de consentimiento en ningún tipo de soporte (sea escrito, de voz, entre otros posibles) para el tratamiento de informaciones basadas en datos sensibles o de especial protección. El artículo 7.4 de la LOPD prohibió expresamente este tipo de tratamientos⁴⁶⁴. Los periodistas y los medios tratan, almacenan, ceden y transmiten datos sensibles, e incluso se especializan en su investigación. Similar tratamiento se produce para los datos de origen racial, de colectivos afectados por una enfermedad, de colectivos activistas de homosexuales y lesbianas. El artículo 7.5 genera todavía más controversia en estos momentos. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las AAPP competentes. Se recuerda que las Sentencias de los Juzgados y Tribunales junto con los Registros Públicos no se consideran fuentes accesibles al público por el artículo 3.j) LOPD. Toda la información que tuviera similar temática está sujeta a los principios y leyes de protección de datos personales. La LOPD no excepcionó el tratamiento de datos personales que tenga su fundamento en la libertad de expresión e información⁴⁶⁵, aunque la Directiva 95/46/CE permitió a los Estados miembros establecer regulaciones sobre la materia. La falta de regulación, sólo justificable por la ausencia de voluntad por parte del legislador, hace que la actividad periodística se encuentre seriamente judicializada, llegando a ser

⁴⁶⁴ STS 482/2006, de 25 de enero de 2006, FJ 2 y 3. La multa fue de 300.000 Euros, una de las más cuantiosas que este estudio ha observado. El TS argumenta que “el principio de culpabilidad consiste en la falta de diligencia observada por la entidad recurrente al tratar de forma automatizada un dato relativo a la ideología del denunciante, resultado irrelevantes las invocaciones (...) acerca de la ausencia de intencionalidad o a la existencia del error, y ello por cuanto el elemento culpabilístico del tipo sancionador aplicado concurre cuando se incluye el expresado dato sobre ideología, no siendo precisa la concurrencia de una intencionalidad específica tendente a revelar datos privados del afectado.”

⁴⁶⁵ SAN 5744/2008, de 1 de octubre FJ 7: Al no tener regulación específica, la AN afirma que “Serán las circunstancias concretas de cada caso las determinantes de la prevalencia de uno u otro derecho. Para ello debemos atender a la naturaleza de la información que se facilita, la finalidad perseguida, el medio utilizado, el número de destinatarios posibles, la existencia de intereses generales en la obtención de ese tipo de información y su afectación al derecho a la propia imagen en su manifestación de autodeterminación informativa.” Estamos de nuevo ante el ejercicio de la ponderación.

absurda y costosa para todos los implicados⁴⁶⁶. La libertad de expresión e información debe ser considerada como máxima para un Estado de Derecho, tan fundamental como el respeto a la protección de datos personales. El nuevo RGPD en su Considerando 153, dedica una especial atención a las libertades de expresión e información⁴⁶⁷, exigiendo un respeto máximo a la normativa sobre protección de datos, pero sin merma de las importantísimas libertades de expresión e información. Tal conciliación es po-

⁴⁶⁶ En este sentido, el breve análisis de RODRÍGUEZ, J., "La autodeterminación informativa como barrera a la libertad de información y al ejercicio profesional del periodismo", *Anàlis. Quaderns de comunicació i cultura.*, nº 42, 2011, pág. 79-94. Se apunta en esta referencia que no se publica información personal en medios mucho más importantes que las redes sociales y medios de comunicación en general, como es la anonimización obligada en Sentencias y Boletines Oficiales, los cuales son mucho más relevantes que la posible información de casos y situaciones en las redes sociales o en los informativos televisados en cualquier formato, incluido el más seguido en la actualidad, donde diferentes periodistas de opinión dicen analizar situaciones informativas generando una especie de *show* en sus discusiones. Otro análisis más pormenorizado en MARTÍNEZ MARTÍNEZ, S., "El derecho a la intimidad en el periodismo participativo: consideraciones desde el ámbito de la ética y la regulación deontológica de la información", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Madrid, 2014.

⁴⁶⁷ Considerando 153 RGPD: "El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales con arreglo al presente Reglamento. El tratamiento de datos personales con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio."

sible, sin merma en el periodismo y con una protección de datos adecuada. Los medios de comunicación deberán adaptarse para cumplir con las obligaciones que promueve este nuevo texto europeo, entre ellas el denominado *derecho al olvido*, por el cual los medios de comunicación deben eliminar datos personales no relevantes o con información obsoleta de internet y que se tratará a continuación con la denominación que le ha otorgado el RGPD, *derecho de supresión*.

Y la regulación se muestra necesaria. Es una realidad creciente la publicación de fotografías, datos personales, información de todo tipo, acompañada de imágenes, vídeos, comentarios críticos llegando a lo lesivo en sus opiniones, continuamente por todos los medios audiovisuales especialmente, en televisión, *Facebook*, *Twitter*, *Instagram*, diarios de prensa. En los últimos tiempos se afianzó la costumbre de los medios de resaltar conductas, calificándolas de delictivas, ilícitas, no éticas, no morales, pidiendo responsabilidades y atribuyéndose unas competencias que superan los límites que admite el Estado de Derecho para las actividades informativas. Se denomina *pena de prensa* a la publicación de información, que basada en documentación teóricamente en manos de los Poderes del Estado y en sus Fuerzas de Seguridad (Policía o Guardia Civil) o en investigaciones de los Tribunales (algunas bajo secreto de sumario) o incluso sin esa referencia, sólo *por fuentes informadas*, inculpan a una persona ante la sociedad con el uso de palabras que sólo un Tribunal competente puede usar en las Sentencias. Esas conductas de la prensa van mucho más allá que el derecho a la información constitucionalmente admitido y violan, flagrantemente, los DDFF de la persona, que siendo culpable o inocente de los delitos que se le imputasen por la prensa o por simples usuarios de redes sociales (ahora parece que todos pueden ser periodistas, jueces instructores y Tribunales), no tiene ningún control sobre la información personal que se vierte sobre ella y sobre sus allegados (familia, amigos, compañeros de trabajo) en los medios. A través de los medios informáticos y las redes sociales se llega a la información de lo absurdo. No se permite que los Tribunales sustancien los hechos con pruebas fehacientes y en Derecho. No se admite en los medios el respeto debido a la persona por el sistema de DDFF y de los DDHH. Se están generando situaciones en las que se increpa y se promociona el *odio social*, la rebelión a las normas

democráticas, el linchamiento público⁴⁶⁸. Es muy preocupante que se promuevan este tipo de conductas; en vez de promover desde los medios el diálogo y confrontación de

⁴⁶⁸ Véase la SAN 1241/2015, de 31 de marzo. Imágenes de personas detenidas en la operación policial denominada *Pretoria*. Las imágenes del demandante ante la AN se obtuvieron entrando en el Juzgado esposado y con una bolsa azul en las manos que portaba sus pertenencias. Estas imágenes fueron accesibles para los medios de comunicación pues no se respetó el protocolo policial. Un error que no se produce habitualmente, pues los Cuerpos de Seguridad del Estado siempre cuidan de estos asuntos. No es fácil saber en todo momento quién porta una cámara. Otros casos son los recientes tratamientos a expresidentes de la Junta de Andalucía, los insultos a investigados de tramas de corrupción vertidos en todos los medios, las vejaciones fotográficas que se les realiza sólo por ser de un determinado partido político a ellos y a sus allegados, van mucho más allá que la simple libertad de expresión. Se llega a la *cultura del odio*. Ser cuestionado ante un Tribunal no implica ser objeto de todo tipo de burlas e insultos. Otras conductas que sufren ataques en las redes sociales, como los toreros por parte de los animalistas, van más allá del propio torero, que es la figura pública, atacando a sus familiares. El ataque físico a dos miembros de la Guardia Civil y a sus parejas se convocó y se extendió en las redes sociales, llamando al insulto y al odio. Ante la situación, redes como *Twitter* ha decidido dotar de verificación a las cuentas en las que los usuarios usen su identidad real

<http://www.eleconomista.es/negocio-digital/social-media/noticias/7742333/08/16/Twitter-condecera-la-verificacion-a-los-usuarios-que-usen-su-nombre-real.html>

y también generar un código de conducta para frenar el lenguaje del odio en las redes sociales, junto con Facebook y YouTube. En este sentido las reflexiones de NIETO MARÍN, ADÁN; MAROTO CALATAYUD, MANUEL; "Redes Sociales en internet y data mining en la prospección de comportamientos delictivos", *Derecho y redes sociales*, Madrid, 2010, pág. 237. , en la obra colectiva coordinada por RALLO LOMBARTE, A., *Derecho y Redes Sociales*, Navarra, 2010. El autor se manifestó claramente en contra de la autorregulación por las propias empresas de las conductas ilícitas, *cuasi* punitivas, extendidas en las redes sociales. Lo calificó en el epígrafe 4, como "Una falsa solución: la autorregulación como pastor del rebaño". No aceptó las denominadas *políticas de privacidad* ni la *declaración de derechos y responsabilidades* con especial acento en Facebook. Para este autor, la empresa tiene un papel predominante en estas relaciones y el usuario es simplemente sujeto de normativa de adhesión, sin posibilidad ninguna de control. O acepta lo que existe bajo su normativa o que no use sus servicios, es una empresa privada. El consentimiento, como se analiza en este texto dentro de otro epígrafe, es la base de toda la relación, como base de legitimación para el tratamiento de datos personales. En esos documentos que casi ningún usuario lee, las empresas reconocen que existen riesgos para el usuario de las redes sociales, pero también derivan toda la responsabilidad y las consecuencias negativas a los usuarios. Las empresas de redes sociales no garantizan la protección de datos en ningún caso, sólo alertan y solicitan

ideas razonadas y argumentadas se esgrimen insultos, descalificaciones y absurdos, que después no son hechos antijurídicos en un Tribunal por falta de prueba fehaciente o tipología penal. Se recuerda que la consideración de hechos probados es sólo para aquellos que el Tribunal, en la sentencia, aprecia como ciertos y que sirven de base para la determinación del derecho al supuesto admitido. La sociedad decide qué tipo de sistema prefiere, en este momento nuestra sociedad ha decidido que este debe ser el principio orientador de su convivencia, aunque en la realidad se vertió en una forma de juicios paralelos por una sistemática orientación de la opinión social a través de determinados medios que extienden las informaciones a la violación de los DDFF. El escarnio de conductas no es la vía para la paz social, que se basa más en el pacto y en los acuerdos. El respeto, incluso con el que violase la norma, la convivencia, en sus aspectos más dolorosos, son necesarios, para generar un Estado de Derecho, que no es otro que el Estado de la Razón, no es un estado de argumentos sin sentido jurídico y descalificaciones de vulgar lenguaje. Sólo aquellas expresiones e informaciones que sean valiosas para la formación de la opinión pública en un Estado democrático deben prevalecer en casos de conflictos con otros derechos, en especial ante los derechos a la protección de datos personales y a los que se consideran DDFF en el artículo 18 CE, los derechos a la intimidad, al honor y a la propia imagen. El derecho a la protección de datos personales en un ambiente como el que vivimos actualmente sería una ilusión porque el respeto debido a la persona y a su identidad no se produce ni se promueve, aludiendo a una justificación que no es admisible: el derecho a la información y a la libertad de expresión que resulta preferente en estas situaciones, según los medios de comunicación. No se puede infravalorar de ese modo el Derecho constitu-

del usuario que sea cuidadoso con los contenidos que exhibe, cosa imposible en muchos casos, por ese afán de relevancia pública que invade la sociedad actual. Hasta los individuos u organizaciones completamente irrespetuosos con los DDFF quieren su relevancia en las redes sociales, como se puede apreciar en los recientes conflictos por actos yihadistas o en la guerra de Siria.

Otra opinión en

<http://www.eleconomista.es/negocio-digital/social-media/noticias/7602524/05/16/Twitter-YouTube-y-Facebook-firman-un-codigo-de-conducta-para-frenar-el-lenguaje-del-odio.html>

cionalmente admitido a la información y a la libertad de expresión en el artículo 20 CE. Más en línea con la doctrina del TC, la STC 171/1990, de 12 de noviembre, FJ 5, afirma respecto al valor de los derechos y libertades del artículo 20 CE que “no puede configurarse como absoluto, puesto que si viene reconocido como garantía de la opinión pública, solamente puede legitimar las intromisiones en otros derechos fundamentales que guarden congruencia con esa finalidad, es decir, que resulten relevantes para la formación de la opinión pública sobre asuntos de interés general, careciendo a tal efecto legitimador, cuando las libertades de expresión e información se ejerciten de manera desmesurada y exorbitante”. Y de manera desmesurada y desorbitante se realizan horas de televisión en este momento, con temas relevantes en el fondo de los asuntos y sobre todo implican la utilización de datos personales de forma, en muchos casos, abyecta, mal intencionada, insultante y degradante. En ocasiones, al visionar algunos de esos programas que en teoría tratan temas controvertidos de corrupción, de conductas antijurídicas, se tiene la impresión de estar ante uno de los *shows* de sensacionalismo periodístico. Precisamente por su visionado desde la perspectiva del Estado de Derecho es más ofensivo el formato, que no respetaría en lo más mínimo, ya no sólo el derecho fundamental a la protección de datos personales, sino el más importante por sus implicaciones, el derecho a la presunción de inocencia del artículo 24 CE, pues transgreden de tal forma los límites a la información y a la libre expresión de ideas que sus formatos son difamatorios y denigrantes de la persona, con la intención más de un *hiperrealismo* televisivo que de informar seriamente sobre hechos relevantes y generando una presunción de culpabilidad y de inoperancia del sistema jurídico que no es tal. En el núcleo estaría un tratamiento de datos personales que sólo podría considerarse en contra de todo DDFF. Los DDFF no son sólo derechos subjetivos protegidos frente a las injerencias del ejercicio del poder, son también elementos funcionales de la democracia, por lo que comportan una doble dimensión. Los dos aspectos se complementan y son de igual rango e importancia. Siguiendo la interpretación institucional de los DDFF, se puede concluir que ambos derechos, el derecho fundamental a la libertad de expresión e información, y el derecho fundamental a la protección de datos, no son contrarios sino complementarios dentro de la

actividad democrática, bajo una regulación adecuada y consideración de la profesión periodística a la persona como sujeto de DDFF, sin excepciones⁴⁶⁹.

Se piensa que se puede informar y expresar libremente sin la utilización de tales imágenes y sonidos, que no por ser de representantes públicos (sean políticos, empresarios, sindicalistas, miembros de una confesión religiosa, de una raza determinada) o de personas famosas (actores, artistas) dejan de ser sujetos de protección⁴⁷⁰. Los me-

⁴⁶⁹ Se toma como referencia el texto de MAGDALENO ALEGRÍA, A., *Los límites de las libertades de expresión e información en el Estado social y democrático de Derecho.*, Madrid, 2006, pág. 62 y ss. Se cita en el texto a los autores VILLAYERDE MENÉNDEZ, SOLOZABAN ECHEBARRÍA, HÄBERLE Y BÖCKENFÖRDE, este último realizó un interesante análisis en el año 2008 sobre lo que en alemán se expresa como "*Online-Durchsuchung*" o búsqueda en la red BÖCKENFÖRDE, T., "Auf dem Weg zur elektronischen Privatsphäre", *JZ Juristen Zeitung*, nº 19, 2008, pág. 925-939. Los beneficios también se deben tener en cuenta, como apunta la doctrina. Véase MARTÍNEZ MARTÍNEZ, S., "El derecho a la intimidad en el periodismo participativo: consideraciones desde el ámbito de la ética y la regulación deontológica de la información", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Madrid, 2014, pág. 160. La *red de testigos* ofrece una impagable información instantánea para determinados hechos, redimensionando el ejercicio del derecho a la libertad de expresión e información, que (para exponer hechos *sólo hechos*) se convierte en un medio muy ventajoso, pero que injiere de forma lesiva en los ciudadanos si se entra en la captación y distribución de datos personales. Que un Gobierno trate datos personales de forma masiva e indiscriminada se considera ilegítimo, e igualmente lo es que se traten datos por particulares y empresas para exponer *la vida de los otros*. La autora menciona los estudios de la UNESCO sobre esta cuestión y aboga por la regulación internacional a través de códigos deontológicos como, por ejemplo, el Código Internacional de Ética Periodística de la UNESCO, en cuyo artículo 6 se expone el respeto de la vida privada y de la dignidad del hombre, como principio esencial para regir la labor profesional.

⁴⁷⁰ Como doctrina proveniente de EEUU, un país no exento de libertad de expresión y donde la prensa representa una base indispensable de su sistema político, la Sentencia de la Corte Suprema de EEUU en el caso *The New York Times Vs. Sullivan (1964)*. El Tribunal señaló que la publicación de noticias sobre figuras públicas es legítima, aun existiendo riesgo de difamación, con la excepción de que la noticia sea falsa o difamatoria de forma dolosa, con la intención de difamar. Es una cuestión claramente establecida por la realidad que el tratamiento a las personas por los integrantes de las redes sociales no puede ser debidamente contrastado y es en muchos casos, difamatorio dolosamente, por el solo hecho de emplear imágenes manipuladas y palabras que sólo la jurisprudencia puede emplear después de un procedimiento. Otro ejemplo puede ser el artículo 6.2 del Código Italiano sobre Deontología del trata-

dios y los particulares, con una cámara en mano (recordemos que ahora cualquier dispositivo móvil tiene una), se dedican a grabar y emitir grabaciones de cualquiera en situaciones socialmente irrelevantes desde el punto de vista del Derecho y que, en ocasiones, sólo alimentan odios o bajos instintos, antidemocráticos en cualquier caso⁴⁷¹. Sin embargo, el derecho a la libertad de expresión e información tiene una importantísima función social. En palabras de VILLAVERDE MENÉNDEZ, *el ámbito vital protegido que corresponde a la libertad de expresión e información es la libre formación de la opinión pública para el funcionamiento del pluralismo político, base del Estado democrático*⁴⁷².

No toda la información que puede ser relevante desde un punto de vista divulgativo y espectacular es necesaria en su tratamiento desde la información veraz y la protección de datos. Simplemente se pueden establecer límites sobre datos personales invasivos, no sobre informaciones trascendentes. La limitación y la regulación no es cesura. Un ejemplo comentado, el ocultamiento del rostro de la persona juzgada por ase-

miento de datos personales en el ejercicio de la actividad periodista, el cual dispone que la esfera privada de las personas conocidas o que ejercen cargos públicos debe ser respetada si las noticias o los datos no tienen relevancia en relación con su actuación o vida pública. Véase a este respecto RODOTÁ, S., "Las lecciones de wikileaks: nueva transparencia y nueva distribución del poder", *Transparencia, acceso a la información y protección de datos.*, Barcelona, 2015, pág. 14 y ss.

⁴⁷¹ Es el muy rentable discurso del odio o *hate speech* que actualmente triunfa en los medios de comunicación en los países occidentales. El sentimiento de odio no constituye un delito en el Estado de derecho, sólo son delitos los actos que realizan las personas que tienen sentimientos de odio y afrentan los derechos de otros. En Europa, Alemania se propuso limitarlo constitucionalmente, y en España tiene siempre su cobertura penal a través del delito tipificado de apología de la violencia o del odio a personas, grupos, o situaciones. Se instiga por determinado tipo de organizaciones con diversos intereses, entre los que se encuentran también los económicos-empresariales, o, por otro lado, la movilización de personas que sufren de algún modo consecuencias negativas o injusticias sociales. Un ejemplo: culpar a los inmigrantes del paro que sufre un trabajador o de la delincuencia común. Se oculta bajo el pelaje del supuesto derecho al trabajo de un nacional, la conducta discriminatoria de todo tipo.

⁴⁷² MAGDALENO ALEGRÍA, obra citada. Se menciona brevemente el estudio del autor sobre jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) MAGDALENO ALEGRÍA, ANTONIO; "Libertad de expresión y partidos políticos en la jurisprudencia del Tribunal Europeo de los Derechos Humanos.", *Anuario de la Facultad de Derecho de la Universidad de La Coruña.*, nº 11, 2007, pág. 431-450.

sinato. Limitación que no se aplica a otros sujetos de derechos fundamentales, alegando trascendencia de la noticia. El interés público se centra en la *materia* sobre la que trate la noticia y su incidencia en la opinión pública, no sobre los datos personales, no sobre la imagen de cualquier persona en situaciones determinadas, retransmitidas con escarnio⁴⁷³. Para determinados tipos de medios, no tiene sentido la protección de datos, el respeto a la persona, pues se basan en el sensacionalismo que ejerce parte de los medios. Un medio de comunicación serio y dentro del Estado de Derecho no emitirá datos personales que sean maliciosos e injuriosos o lesivos de DDFF. La jurisprudencia del TC así lo manifestó en Sentencias donde aplicó el principio de ponderación para dar prioridad o preponderancia al derecho fundamental a la libre expresión e información. Es lo que la doctrina califica de *adecuación de las expresiones*⁴⁷⁴,

⁴⁷³ En este sentido véase CORDERO CUTILLAS, I., "Redefiniendo los derechos de la personalidad en el siglo XXI", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, 2014, pág. 26 y ss. . Por ser los implicados personajes públicos, no por ello dejan de tener derechos. Los autores mencionan la STEDH de 24 de junio de 2004, asunto *Von Hannover vs. Alemania* (caso *Carolina de Mónaco*). El Tribunal afirmó que, "aunque el público tiene derecho a estar informado sobre las actividades de las figuras públicas (y especialmente los políticos), en este supuesto no había que proteger ese derecho" Se referían a unas fotos de la Princesa Carolina de Mónaco, que "no contribuían a ningún debate de interés general para la sociedad y habían sido tomadas sin el consentimiento de la demandante". Es evidente el acoso que algunas figuras públicas y sus allegados soportan. Los autores consideran que el derecho a la libertad de expresión e información (o libertad de prensa) cede en estas ocasiones a favor del derecho a la vida privada y a la propia imagen. Por supuesto, también ceden esos mismos derechos ante la protección de datos personales y es el Estado el garante de la eficacia de los mismos. Véase DE DOMINGO, T., *¿Conflictos entre derechos fundamentales?*, Madrid, 2001, pág. 14-27. Se afirma en el prólogo por MARTÍNEZ PUJALTE que "la alternativa a la tolerancia de las informaciones inveraces no es otra que la ocultación de las noticias". No es la idea que se pretende exponer. No se acepta la censura previa, sólo se promovería la defensa de los DDFF de los implicados, no utilizando datos invasivos para transmitir informaciones. En otra página del prólogo, el autor del mismo decide que "no tiene por qué haber un vencedor y un vencido, un contendiente al que asiste la razón y otro que no la tiene en absoluto. Con frecuencia sucederá que ambos litigantes tendrán parte de razón, y que el juez deberá establecer el adecuado equilibrio entre las posiciones en disputa" Es una posición conciliadora, muy acorde con un derecho más razonado que promueva conductas equilibradas para el respeto de los DDFF.

⁴⁷⁴ A modo de ejemplo véase MAGDALENO ALEGRÍA, obra citada, p. 333 y ss. el autor reseña una serie de STC y del TEDH que establecen el sentido de la adecuación de las expresiones. Entre ellas se men-

de la que se infiere en el presente estudio, *adecuación de las imágenes*, como forma de expresión que informa mucho más que las palabras. Las expresiones no pueden ser injuriosas, de menosprecio, denigrantes, acusatorias, de exposición de otros allegados al sujeto del que se aporta información. Las imágenes tampoco. No sólo se puede hablar de la protección al derecho fundamental del artículo 18.1 CE, derecho al honor, sino también se debe tener muy en consideración el derecho a la protección de datos del artículo 18.4 CE, y su implicación en los DDFF, pues unos datos pueden ser relevantes para la información legítima (en el caso de personas públicas, nombre, cargo público, incluso imagen de archivo institucional, lo cual coincide muy posiblemente con lo que el titular de los datos dio su consentimiento para tratamiento por los medios y por otros responsables de tratamiento, son los datos personales que el titular quiso hacer públicos) junto con los hechos de los que se tiene constancia por los medios (el supuesto hecho antijurídico denunciado) pero otros datos no son ni relevantes para la información, ni tienen ninguna justificación⁴⁷⁵. De especial consideración

cionan STC 178/1993 FJ4 de 31 de mayo; STC 232/1993, de 12 de julio, FJ4; STC 154/1999, de 14 de septiembre, FJ4. STC 121/2002, de 20 de mayo, FJ 4; STC 52/2002, de 25 de febrero, FJ8; STC 83/2002, de 22 de abril, FJ6.

⁴⁷⁵ Existen medios de información que viven de generar escándalo a través del escarnio y la exposición pública de datos personales, como puede ser la imagen del titular de datos en directo siendo llevado en un coche policial detenido con esposas, ya comentada o siendo introducido en un coche policial desde su domicilio; la imagen de su esposo/a o su compañera/o sentimental entrando en los juzgados o en la cárcel con marcada expresión de angustia o de tristeza; la imagen manipulada para chistes de todo tipo, vejatorios en muchos casos, en medios de Internet y llevados a la televisión, la imagen y dirección del domicilio del investigado, que implica a sus vecinos en la información; la imagen de sus hijos, aún pixelada si son menores, en la que se ve cómo visten o qué coche usan, a qué colegio o universidad acuden, a qué trabajo; la imagen de locales (restaurantes, cafés, tiendas) asimilada al investigado, lo que daña gravemente la reputación de los negocios y repercute en los puestos de trabajo de las personas que los gestionan; imágenes de personas y nombres que por una u otra circunstancia tiene relación con el investigado: compañeros de trabajo, trabajadores de una empresa, compañeros de estudios con la imagen de la Universidad, edificio de la parroquia donde se ubican los hechos, hospital de tratamiento de la persona. Las imágenes se repiten una y otra vez, aunque los hechos ya no sean actuales ni trascendentes, e incluso cuando ha existido Sentencia absolutoria o la persona ya ha cumplido su condena. Los casos son ilimitados.

por su expansión en los últimos meses son las imágenes de personas víctimas de ataques terroristas. La publicación en *internet* y en redes sociales de fotos y videos, sin respeto alguno a los implicados, a los heridos y a los fallecidos y sus familiares, amigos, allegados, resulta éticamente y deontológicamente reprochable. Es realmente la imagen el dato personal más invasivo, y esa misma imagen es el alimento de determinados programas de televisión, páginas *web* o redes sociales, que sólo con palabras e información de imágenes respetuosas con las personas y sus DDFF parece ser que no pueden tener actividad económica. Las imágenes mostradas no tienen interés o valor informativo, muestran el dolor y las consecuencias de la violencia para aumentar la audiencia y los ingresos económicos del medio. La justificación basada en la relevancia de la información emitida no puede vulnerar el derecho fundamental a la protección de datos en los casos descritos. Nos encontramos con lo que se puede calificar de *un límite derivado de los derechos de los demás y de la defensa de bienes y valores constitucionales*.⁴⁷⁶ En el Estado social, democrático y de Derecho los Poderes Públicos no sólo están obligados a respetar los DDFF, también lo están los particulares, sean personas jurídicas o físicas, que violan los mandatos de respeto del Estado de Derecho, como *nuevos centros de poder*. Los DDFF, como se viene apuntando en el presente estudio, son principios ordenadores de la vida social del Estado y, por tanto, son eficaces frente a particulares cuando su naturaleza así lo explicita⁴⁷⁷. La STC

⁴⁷⁶ Ambas expresiones son utilizadas por MAGDALENO ALEGRÍA, obra citada, p. 292-381. “Todo derecho tiene sus límites, que, con relación a los derechos fundamentales, establece la Constitución por sí misma en algunas ocasiones, mientras que en otras el límite deriva de una manera mediata o indirecta de tal norma, en cuanto ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionalmente protegidos. Los citados bienes pueden estar expresamente citados en la Constitución (...). O bien pueden derivarse implícitamente de ésta. Los aludidos límites implícitos para poder ser aplicados tienen que ser explícitamente desarrollados por el legislador. Esta labor es de carácter constitutiva, lo que implica que sólo serán de aplicación en el caso de ser concretados por el legislados de acuerdo a lo establecido en el artículo 53 de la Constitución. Esto es, mediante una Ley que deberá ser proporcional y respetar el contenido esencial del derecho fundamental limitado.” Cita de p. 337.

⁴⁷⁷ Por ejemplo, el derecho de huelga y la libertad sindical en las relaciones laborales. Se exceptúan los DDFF que sólo el Estado puede realizar como son las garantías del detenido, por ejemplo, aunque, co-

101/1983, de 18 de noviembre, FJ 4 sintetiza la eficacia del artículo 9 CE, con el argumento de que la sujeción de los Poderes Públicos a los DDFF es de diferente intensidad a la sujeción de los ciudadanos; mientras que los particulares tienen un *deber general negativo* de abstenerse de cualquier actuación que vulnere la Constitución, los poderes públicos tienen además un *deber general positivo* de realizar sus funciones de acuerdo con la Constitución. El TC mantendría una jurisprudencia a favor de la eficacia frente a los particulares de los DDFF en esta línea de la STC del año 1983.

Sólo se puede calificar la situación actual de moda o tendencia (con grandes riesgos) de la sociedad, quizá necesitada de una vía de expresión a sus emociones ante la grave crisis económica, tendencia que los medios de comunicación y de expresión (desde cadenas de televisión hasta redes sociales) han materializado en horas de audiencia o en seguimiento de muchas personas. No se olvide que los mismos medios que dan pábulo a conductas que violan el derecho fundamental a la protección de datos más básica, son mantenidos por la publicidad de empresas con diferentes intereses económicos, y, por ende, políticos. Con respeto total a las líneas editoriales, una conducta más acorde con la consideración debida, no ya sólo al derecho fundamental a la protección de datos, sino también a todo el conjunto de DDFF y al Estado de Derecho, haría a estos medios grandes desde el punto de vista comunicativo, generando ese sentido fundamental de toda sociedad democrática que se denomina opinión pública⁴⁷⁸. Por otro lado, tampoco están exentos de responsabilidades los legisladores, los

mo se ha comentado, los datos personales del detenido no pueden ser objeto de información (tratamiento) que lesione su derecho fundamental a la protección de datos. MAGDALENO ALEGRÍA, obra citada, p. 394 y ss.

⁴⁷⁸ Una opinión contrastada puede ser la que expresa BOIX PALOP, A., "La construcción de los límites a la libertad de expresión en las redes sociales.", *Revista de Estudios Políticos.*, nº 173, 2016. El autor cuestionaría las posibles implicaciones de las libertades de expresión e información como conductas lesivas. Aun estando de acuerdo en los ejemplos que el autor propone como reacciones desmesuradas (que no se realizan en otros casos), lo que sí se considera obvio es la implicación de un tratamiento excesivo de los datos personales, en unos casos, y en otros una desmesurada expresión en el lenguaje y las imágenes, que unido al expansivo alcance de las redes sociales se transforma en un daño expuesto a multitud de personas.

cuales, en vez de cumplir con su misión de limitar y definir el derecho fundamental de libertad de expresión y comunicación junto con el derecho a la protección de datos, dejan el asunto en manos de la AEPD o de los Tribunales. El nuevo RGPD sigue en la línea de la Directiva, dejando en la voluntad legislativa de los Estados miembros la regulación por ley del tratamiento de datos personales en los medios de comunicación e información, para fines periodísticos, de expresión académica, artística o literaria, línea que no mantiene para otro tipo de actividades económicas menos lesivas para la protección de datos personales, las cuales regula en su normativa⁴⁷⁹.

B. La fuerte controversia y las consecuencias negativas de la publicación de información personal en prensa y en Boletines Oficiales.

El repertorio de publicaciones consideradas Diario o Boletín es sumamente amplio. Los datos personales se consideran por el artículo 3 j) de la LOPD y 7.1.d) del Reglamento como fuentes accesibles al público. Este tipo de publicaciones engloba desde el Diario Oficial de la Unión Europea hasta los Boletines de las entidades locales, pasando por el Boletín Oficial del Estado y los de las Comunidades Autónomas. A los efectos del

⁴⁷⁹ Artículo 85 RGPD: Tratamiento y libertad de expresión y de información

1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.
2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.
3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas.

presente estudio se incluyen dentro de esta categoría los Boletines del Registro Mercantil. Son considerados todos ellos de titularidad pública y bajo la regulación de la LOPD para este tipo de ficheros. Para complicar algo más esta normativa, cada Boletín o Diario tienen su regulación específica, obligándose a proteger los datos de carácter personal, además de proteger el honor y la intimidad de los afectados. Estos datos han producido una cantidad enorme de controversias, pues los datos personales eran publicados en otras páginas web o repertorios electrónicos y telemáticos no oficiales. Es un asunto de máxima actualidad, por la Sentencia del TJUE denominado por los medios *Caso Google*. El asunto, resumido, se basa en la reclamación ante la AEPD de un ciudadano español, que solicitó a Google la retirada de sus motores de búsqueda de información sobre un embargo de la Seguridad Social del año 1998. Los anuncios relativos a la subasta de la Seguridad Social se habían publicado a su vez en un diario de ámbito nacional. El interesado también pidió al diario la retirada de esa información, sin resultado positivo. Solicitó entonces a la AEPD que sus datos fueran protegidos, y la Agencia, después de no encontrar solución a través de Google, se dirigió a la AN, quien, a su vez, remitió ese caso al Tribunal de Justicia de la Unión Europea (como hemos reseñado, TJUE) El abogado general del Tribunal, Niilo Jääskinen, elaboró un dictamen en 2013 a favor de la empresa Google frente a España y su AEPD, alegando que el motor de búsqueda (empresa Google) no es responsable de las informaciones que se publiquen en otros medios. Pero el Tribunal en su Sentencia no resolvió en ese sentido, lo que dio lugar a toda una nueva visión de los derechos a la protección de datos personales. Según esta sentencia del TJUE, Google o cualquier otro buscador está obligado a eliminar de la lista de resultados de una búsqueda cualquier dato relativo a una persona, los enlaces a páginas web publicados por terceros que contengan información de carácter personal, si el afectado lo solicita. La AEPD elaboró multitud de informes y resoluciones sobre asuntos similares a la publicación de informaciones personales en Diarios o Boletines por medios electrónicos y telemáticos, que se incluyen rápidamente en motores de búsquedas. Las consecuencias negativas para los afectados pueden trascender más allá del interés legítimo a su publicación.

Similar a lo anteriormente expuesto es el caso de la publicación telemática de las Sentencias y Resoluciones judiciales. Colisionan el principio de publicidad de las Sentencias de la CE, desarrollado en los artículos 205.6; 232 y 266 de la LOPJ y el derecho a la protección de datos personales. También recientemente la AEPD ha publicado Informes e incluso Resoluciones como la del año 2015, R/01374/2015⁴⁸⁰. El delito se calificaba contra la propiedad industrial, y fue cometido en el año 2009. Google recibió ese mismo año una petición de retirada de los datos personales de este ciudadano y denegó la actuación, según lo que se refleja en la Resolución de la AEPD, alegando que *la información es de interés público en relación a su vida profesional*. Posteriormente, la AEPD consideró que se debían atender las peticiones de este ciudadano, basándose en la reciente Sentencia Google de 13 de mayo 2014, la cual sirve para orientar estos asuntos de forma más acorde con la protección de datos y la defensa de los DDFF. También argumenta esta Resolución con la SAN 1378/2015, de 31 de marzo FJ 1, por la que se ordena que “hay que indicar al responsable del fichero que las sentencias judiciales dictadas por los tribunales no son una fuente de acceso público, y que es preciso el consentimiento de los afectados para el tratamiento de los datos que en ellas aparecen. Si quiere publicar alguna sentencia, sólo podrá hacerlo siempre y cuando esté anonimizada, es decir, que no figuren datos personales en la misma”

La AEPD concluyó la Resolución R/01374/2015 con el siguiente texto: “Consecuentemente, procede la exclusión de los datos personales del reclamante al tratarse de

⁴⁸⁰ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, “Resolución R/01374/2015 retira de datos personales publicados en Sentencia penal.”]. http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2015/common/pdfs/TD-00022-2015_Resolucion-de-fecha-01-06-2015_Art-ii-culo-16-LOPD.pdf en la que se reconoce a un ciudadano español condenado a 20 meses de multa por un Juzgado de lo Penal de Cádiz, a que se retiren todos sus datos personales de la sentencia publicada y que es accesible por el buscador Google, lo cual le produce un perjuicio máximo pues manifiesta a la AEPD que “Desde dicha publicación no tengo ni encuentro trabajo y estoy en estado de total exclusión social, ya he pagado y sigo pagando el error que cometí y no estoy dispuesto a consentir más humillaciones sobre mi persona”. Es el derecho fundamental a la reinserción lo que este ciudadano no consigue.

datos obsoletos, excesivos y no concurrir interés preponderante del público en tener acceso a esta información a través de una búsqueda en *internet* que verse sobre el nombre de esta persona”. La identidad de los ciudadanos es irrelevante desde la perspectiva del interés público sobre la información⁴⁸¹. Sobre este punto existe discrepancia; se alegaría que en determinados casos sí existe interés legítimo en conocer la identidad del autor de los hechos.

C. Las repercusiones de la reciente Sentencia Google. El denominado derecho al olvido (Derecho de supresión, artículo 17 RGPD).

El denominado *derecho al olvido*, el derecho de supresión regulado en el artículo 17 RGPD, se ha definido en el Considerando 65 del mismo texto, como el derecho de los interesados a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en *internet*. La AEPD considera a su vez que el denominado *derecho al olvido* es la manifestación de los tradicionales derechos de cancelación y oposición aplicados a los buscadores de *internet*. El *derecho al olvido*,

⁴⁸¹ Anteriormente a la mediática Sentencia Google, el TC se manifestó en la Sentencia STC 114/2006, de 5 de abril, sobre la publicidad de los nombres personales en las diferentes Sentencias del TC. La Opción del Tribunal fue ponderar en cada caso concreto la pertinencia de la publicidad y de los intereses individualizados de los intereses constitucionales concurrentes. El TC mencionó como intereses prevalentes el derecho a la intimidad, las garantías que proporcionara el posible anonimato de las víctimas o el uso de esos datos para fines contrarios a la Ley. Esta opción es muy mesurada, pero dependerá de la interpretación que los magistrados realicen para cada caso concreto, aspecto que se mostró en la STS 545/2015, de 15 de octubre.

mejor denominado *derecho de supresión*, hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa de protección de datos. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia o interés público, aunque la publicación original sea legítima (en el caso de Boletines Oficiales o informaciones amparadas por las libertades de expresión o de información). El resultado de la búsqueda por el nombre es lo que cambia, no las fuentes originales de información, que seguirán intactas, y mostrarán el mismo resultado si la búsqueda se realiza con otro término que no sea el nombre del interesado. Este derecho actualmente reconocido por el nuevo RGPD no estaba previsto en la LOPD y como se ha visto, es consagrado como derecho dentro de la protección de datos personales a consecuencia de la denominada Sentencia *Google*⁴⁸². El

⁴⁸² En el año 2008 el Director de la AEPD, ARTEMI RALLO, presentó en sede Parlamentaria la creciente sensibilización de los ciudadanos para demandar un derecho al olvido en Internet. Años después, se comenzaban a producir las primeras manifestaciones de este derecho. Véase en RALLO LOMBARTE, ARTEMI; , "El derecho al olvido y su protección a partir de la protección de datos", *Telos. Cuadernos de comunicación e innovación. Fundación Telefónica.*, nº 85, 2010, pág. 104-108. Véase también RALLO LOMBARTE, A., *El derecho al olvido en internet. Google versus España*, Madrid, 2014. En un estudio monográfico sobre la Sentencia comentada y ampliada. También a este respecto las ideas de MARTÍNEZ OTERO, J., "El derecho al olvido en Internet", *Revista de Derecho Político*, nº 93, 2015, pág. 103-142. SANCHO VILLA, D., "Developing Search Engine Law: It Is Not Just about the Right to Be Forgotten.", *Legal Issues of Economic Integration*, nº 4, 2015, pág. 357-382. ZÁRATE ROJAS, S., "La problemática entre el derecho al olvido y la libertad de prensa", *Derecom*, nº , 2013. MIERES MIERES, L., "El derecho al olvido digital", *Fundación Alternativas*, nº , 2014. MINERO ALEJANDRE, G., "A vueltas con el "derecho al olvido". Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital.", *Revista jurídica Universidad Autónoma de Madrid*, nº , 2014, pág. 129-155. Otra opinión muy interesante es COTINO HUESO, L., "El conflicto entre las libertades de expresión e información en internet y el derecho a la protección de datos. El derecho al olvido y sus retos: "un falso derecho, a juzgar por un falso tribunal", *Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia*, Madrid, 2014. El autor se manifestó especialmente crítico con el TJUE, siendo el título del epígrafe 4. así: "La ponderación la realizará un "juez" que no quiere serlo, una administración que no es judicial y dará lugar a veintiocho criterios jurisprudenciales en

TJUE aclaró el derecho de supresión frente a los buscadores de *internet*, delimitando los conceptos de responsable del tratamiento y del acceso por otros a determinada información personal, pues consideró que los denominados *motores de búsqueda* y su actividad comercial (se mantienen de la publicidad y de las tarifas que facturan a los que desean ser los primeros en los encuentros que el motor propone en cada búsqueda, no es una actividad sin ánimo de lucro) realizaban un tratamiento de datos personales y que, por tanto, su actividad de empresa está sometida a las normas sobre protección de datos personales de la UE; como responsable del tratamiento, la empresa que gestione el motor de búsqueda eliminará las referencias a datos personales por petición de su titular, aunque esa información no haya sido eliminada por el editor del medio que se indexa. Las excepciones que admite el TJUE son, por una parte, que el interesado tenga relevancia pública o que el acceso a la información estuviera justificado por el interés público. Ambas situaciones se pueden inscribir en la comentada *excepción periodística*⁴⁸³.

la Unión Europea” con una crítica extendida a la AEPD, en línea con BOIX PALOP, en la que cuestiona la independencia de la AEPD y su competencia, ya apuntada, para efectuar la ponderación entre libertades públicas y otros derechos fundamentales.

Otras Sentencias que estiman la aplicación del derecho de supresión en diarios de prensa son: SAN 2487/2015, de 11 de junio; SAN 1072/2015, de 20 de febrero; SAN 621/2015, de 19 de febrero; SAN 2355/2015, de 9 de junio; SAN 616/2015, de 24 de febrero; SAN 782/2015; de 12 de febrero; SAN 483/2015, de 10 de febrero; SAN 636/2015, de 5 de febrero. Véase también las Sentencias que estiman la retirada de información personal de Boletines Oficiales: SAN 411/2015, de 22 de enero; SAN 2980/2015, de 16 de junio; SAN 2338/2015, de 11 de junio; SAN 1609/2015, de 14 de abril, esta última es curiosa pues en el FJ 9 se reconoce la confusa redacción de la Resolución de la AEPD que se recurre por Google en este caso, aunque obligue a la empresa menciona a retirar o eliminar de las listas de resultados los datos del reclamante. Como se puede también apreciar en muchas de estas SAN, Google continuó recurriendo las Resoluciones que obligaban a aplicar el derecho de supresión de los titulares.

⁴⁸³ Véase PAUNER CHULVI, C., "Implicaciones del futuro Reglamento europeo sobre protección de datos en la libertad de información", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Madrid, 2014. También MARTÍNEZ OTERO, J., "El derecho al olvido en Internet", *Revista de Derecho Político*, nº 93, 2015, pág. 103-142. SARRIÓN ESTEVE, J., "Tras la larga sombra de Google Spain. ", *Universidad de Valencia*, nº 1, 2015.

Como consecuencia del pronunciamiento del TJUE en el asunto C-131/12, de 13 de mayo de 2014 (Caso *Google*), las empresas de buscadores mayoritariamente usados por los ciudadanos (*Google, Yahoo o Bing*) realizaron cambios en sus páginas, generando formularios para dar cobertura a las peticiones de los ciudadanos que deseen que sus nombres no figuren en buscadores. En el caso de que la empresa propietaria del buscador no atendiese los derechos de cancelación y oposición de un titular de datos personales, podrá acudir a la AEPD en tutela de sus derechos. El TJUE también estableció en la Sentencia *Google* que el *derecho al olvido* no significa un límite al derecho a la información del artículo 20 CE, para el caso de España. Propone que, bajo el principio de ponderación, se valoren las circunstancias de cada caso. Las informaciones que sean de relevancia pública o que afecten a una figura pública no serán modificadas y la AEPD no aceptará la solicitud de tutela en estos casos⁴⁸⁴. El RGPD no aporta los criterios necesarios para ponderar frente a los diferentes intereses, trasladando al responsable del tratamiento la obligación de ponderar y de transmitir a los terceros que ejercen el tratamiento de los datos personales la exigencia de supresión de su titular. Existe una confirmada dificultad para la supresión de datos en internet, aunque las herramientas técnicas existan, pero sólo para determinadas personalidades protegidas o que tienen una personalidad en la red⁴⁸⁵.

El TS, pocos meses después, rechazó alterar las informaciones del diario *El País* por la aplicación de la Sentencia del TJUE. El Tribunal español alegó en la STS 545/2015, de

⁴⁸⁴ Sirvan como ejemplo las Resoluciones desestimatorias de la AEPD TD/01997/2014; TD/01955/2014; TD/01533/2014; TD/01843/2014. Esta información fue publicada por la AEPD en su web con fecha 27 de septiembre de 2015. http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php Otra

Sentencia en relación con la relevancia pública y la no aplicación del derecho de supresión o *derecho al olvido* son: SAN 2486/2015, de 5 de junio; en la SAN 484/2015, de 10 de febrero, sin embargo, lo estima, al no probar Google la relevancia pública del titular de los datos recurrente.

⁴⁸⁵ GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 241. Se comentaron en otros epígrafes y se volverá sobre este asunto de implicaciones en la igualdad de tratamiento de datos, pues existen diferencias entre determinados perfiles que pagan por su gestión en internet y los demás usuarios.

15 de octubre, que *no se puede crear cada persona una historia a su medida*, eludiendo los hechos del pasado que no se consideren positivos años después, como fue en el caso de los recurrentes. Además, matizaba que las personas expuestas por sí mismas públicamente, no pueden pretender un *curriculum* a su medida⁴⁸⁶. El TS ponderó entre el ejercicio de la libertad de información y los derechos al honor, a la intimidad y a la protección de datos personales y estimó parcialmente el recurso de los afectados, pero sin acceder a la pretensión de eliminar los nombres y apellidos de la hemeroteca digital (lógicamente tampoco de la existente en soporte de papel)⁴⁸⁷. Lo

⁴⁸⁶ Se trataba de la publicación por el diario El País en los años ochenta del pasado siglo XX de la implicación de dos personas en delitos de tráfico y consumo de drogas. Una vez cumplida su condena, rehicieron sus vidas. En la actualidad, los buscadores de internet publicaban las noticias sobre esos hechos delictivos, al introducir como criterio de búsqueda sus nombres y apellidos. Los interesados demandaron al diario El País porque no retiraba las informaciones referentes a los interesados de la hemeroteca digital.

⁴⁸⁷ Según una visión civilista de esta STS la legislación y jurisdicción civil a la que el diario *El País* apela, sobre honor, intimidad y propia imagen sería suficiente para resolver un problema de estas características. Existe la tendencia a considerar que la protección de datos merma parte de las competencias judiciales civiles mermando las libertades de expresión e información en manos de un órgano administrativo, que, según estas tendencias, es juez sin serlo. No entran dentro de esta tesis. Se aporta como crítica y comentario las ideas expuestas por BOIX PALOP, A., "La construcción de los límites a la libertad de expresión en las redes sociales.", *Revista de Estudios Políticos.*, nº 173, 2016, pág. 98 y ss.. Del mismo autor y con una posición crítica frente a lo que denomina *protagonismo administrativo* BOIX PALOP, A., "El equilibrio entre los derechos del artículo 18 de la Constitución, el "derecho al olvido" y las libertades informativas tras la Sentencia Google.", *Revista General de Derecho Administrativo*, nº 38, 2015, pág. 34. El autor expresa que "Personalmente, no tengo dudas de que no es positivo que la Administración arbitre qué contenidos son o no adecuados, incluso a partir de que haya pasado cierto tiempo, e imponga sus decisiones al respecto (siquiera sea en revisión de lo que previamente hayan hecho unos sujetos privados y por mucho que, como no puede ser menos, sus decisiones estén a su vez sometidas al control judicial). No sólo ello, también considero cuestionable que el modelo constitucional reflejado en el artículo 20 de la Constitución de 1978 lo permita. Hay que tener en cuenta, en este sentido, que entre los contenidos de ese precepto hay varias medidas que tratan de desapoderar a la Administración del control sobre los contenidos que publicaban medios privados que tradicionalmente, durante el franquismo, había sido habitual en España. Ése es el sentido, por supuesto, de la prohibición de la censura previa, como plasmación más evidente." Reforzando su interesantísima tesis con la ale-

que también reclamó el TS en su Sentencia fue *la adopción de medidas tecnológicas* por los responsables de las hemerotecas digitales para que las informaciones desfasadas por el tiempo y perjudicial para los afectados no pueda ser indexada por los buscadores⁴⁸⁸. Todo ello no debe suponer una censura previa de contenidos, pues no se evitan o diluyen informaciones, muy al contrario, lo que se desea es que la información tenga un mejor contenido y se eludan las ofensas o las violaciones de otros DDFF, que no tienen por qué ser menoscabados por la libertad de expresión e información. No se silencian informaciones, se protegen datos personales. La Autoridad de control no cierra otras vías de protección judicial, se reitera, como sí se realizaría en el caso no deseado de censura previa. Cuestionando la posibilidad de una mejor organización para la defensa del derecho a la protección de datos personales, no tanto desde el Derecho Administrativo, con un modelo más transparente y participativo de todos los interesados, se tiene por cierta la protección que se ha ejercido en casos flagrantes de violación de DDFF por la AEPD, la AN y otros Tribunales en la defensa de los ciudadanos⁴⁸⁹.

gación de censura previa, pues “considera que para que una publicación quede fuera de la circulación ha de mediar una decisión judicial”. Véase también DOMÍNGUEZ MEJÍAS, I., “Hacia la memoria selectiva en Internet. Honor, intimidad y propia imagen en la era digital a partir de la jurisprudencia española.”, *Revista Iberoamericana de Ciencia, Tecnología y Sociedad - CTS*, nº 11, 2016, pág. 8 y ss. El derecho de supresión no conlleva adscrito un derecho a la desaparición total de los datos. El derecho de supresión sólo afecta a buscadores de internet.

⁴⁸⁸ Se pueden denominar técnicamente códigos robots.txt o instrucciones noindex. Este tipo de programas bloquean la indexación en las búsquedas, aunque la información permanece intacta.

⁴⁸⁹ Véase a título de ampliación con ejemplos aclaratorios la exposición de RALLO LOMBARTE, A., *El derecho al olvido en internet. Google versus España*, Madrid, 2014, pág. 133 y ss. En su exposición el autor afirma que no son adecuados *ni el olvido preventivo ni la censura previa en Internet*. La censura previa se convertiría para el autor en un límite infranqueable para el ejercicio del derecho de supresión (o *derecho al olvido*), al menos en el actual estadio de la técnica de protección de datos. El autor no admitiría tampoco el “olvido ciego” ni el “borrado general de datos” en los buscadores de Internet.

D. El Derecho de supresión de información personal en *internet* y reinserción social.

El tema del derecho de supresión (o *derecho al olvido*) tendría fuertes consecuencias en otro derecho fundamental ya mencionado: el derecho constitucional a que las penas privativas de libertad estén orientadas a la reinserción social (artículo 25.2 CE)⁴⁹⁰. La persona que haya cumplido condena o cuyos supuestos actos delictivos hayan prescrito no debe ser agredida por la información que se vierta en los medios de comunicación y que imposibilite o entorpezca su rehabilitación. Así también se evita la discriminación que produce la desconfianza social en el que fue delincuente, favoreciendo el ejercicio democrático y avanzado de la reinserción social. La difusión de un pasado penal de los ciudadanos no puede ser útil ni para la sociedad ni para la lucha contra el delito⁴⁹¹. Ante las tendencias denominadas *securitarias* del Derecho Penal,

⁴⁹⁰ Texto del artículo 25.2 CE: “Las penas privativas de libertad y las medidas de seguridad estarán orientadas hacia la reeducación y reinserción social.”

⁴⁹¹ Sirva como ejemplo el de EEUU. Se cuestiona la eficacia de la *Wetterling Act* o ley *Wetterling*, la cual sería conocida también como Ley o leyes Megan en su modificación de 1996 junto con la ley Pam Lyncher de Seguimiento e Identificación de Delincuentes Sexuales (*Pam Lyncher Sexual Offender Tracking and Identification Act*). Se promulgó dentro del marco de la Ley Federal de Control de Delitos Violentos y Fuerzas Policiales de 1994 (*Federal Violent Crime Control and Law Enforcement Act of 1994*). Esta ley obligó al FBI a establecer una base de datos nacional de delincuentes sexuales para ayudar a las agencias policiales locales para realizar un seguimiento a los delincuentes sexuales sin los límites de las fronteras estatales. Más de 20 años después, no parece que leyes de este tipo eviten la comisión de delitos y, sobre todo, impiden la reinserción del que fue recluso. Se comenta que ello no exime para controlar por parte de la sociedad conductas lesivas, no tanto como delito sino como seguimiento de posible desequilibrio psiquiátrico, que puede activar a su vez los sistemas policiales de localización del ciudadano que expone a otros a sus conductas lesivas (por ejemplo, la efectividad de las pulseras localizadoras). Pueden ser compatibles los bienes constitucionales a proteger del exdelincuente y de la seguridad de la población, bajo los DDFF de la dignidad humana, el honor, la intimidad y por supuesto una necesaria reinserción en la sociedad. Véase a este respecto ALONSO RIMO, A., “La publicidad de los antecedentes penales como estrategia de prevención del delito.”, *Revista General de Derecho Penal*, nº 17, 2012. Por otro lado, existe la opinión de sectores que promueven la publicación de datos (nombre, apellidos y fotografía) de incluso imputados sin sentencia firme, como se puede

que no forman parte del análisis de este estudio, pero que se comentan como implicadas en el tema de la protección de datos, sería importante recordar los principios y valores democráticos que afectan al Derecho Penal, quizá la visión del derecho donde los DDFF más profundamente deben ser defendidos. En el sistema español predomina la restricción de la publicidad de los antecedentes penales en la línea doctrinal de amplia Jurisprudencia, destacando la del TC. No tiene por qué resultar incompatible el derecho a la libertad de información, el derecho a la justicia y el control del sistema democrático frente a los DDFF del ciudadano que cumplió su condena y que, en justicia también, no debe nada a la sociedad. En sentido contrario se expresó una parte de la doctrina, alegando el derecho a la libertad de información, cuestión muy difícil de aceptar desde un punto del derecho constitucional a la reinserción social⁴⁹².

En los casos de personas conocidas por los medios de comunicación, se podría considerar como patente la reiteración de los hechos pasados que algunos medios realizarían con los datos, en especial, con las imágenes del implicado en conductas antijurídicas. Los asuntos son muy populares y posiblemente contarán con un número de personas que se deleiten en esas exhibiciones. Estas conductas no fomentarían en absoluto una pedagogía social dirigida a los DDFF, sino que además se podrían cuestionar su pertinencia, pues pertenecen al pasado, pero darían la sensación mediática de que la conducta antijurídica no se eliminó de la realidad, no transcurrió, no fue juzgada y resuelta para la sociedad. Se podría tener la sensación de que el ciudadano que fue

apreciar en la posición que mantiene un sector de la abogacía. Alegan que se publican en los medios datos de las víctimas y no de los presuntos autores o sentenciados por los hechos. Lo consideran una advertencia para los posibles delincuentes y una forma de reforzar a las víctimas. Se piensa que tanto los datos de las víctimas como de los delincuentes deberían ser protegidos por igual, salvo que la información personal sea de relevancia para la conclusión de los asuntos (desaparición o búsqueda de una persona, por ejemplo)

http://www.abc.es/espana/abci-publicar-sentencias-foto-agresores-daria-confianza-mujeres-201608142052_noticia.html

⁴⁹² Como ejemplo, las ideas de BUSTOS GISBERT, referencia de la autora GUERRERO PICÓ, M., *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Navarra, 2006, pág. 428.

condenado por un delito, sigue en su ejecución, es siempre *delincuente continuado*, sin que los medios permitieran a la persona una nueva realidad.

Un asunto novedoso estaría protagonizado por la aparición de empresas privadas cuya actividad reside en la eliminación de información publicada a través de *internet*. Ante esta situación, se puede apreciar que el ciudadano cuyo nivel de ingresos permita la contratación de los servicios de eliminación de datos puede hacer efectivo el derecho a la supresión de información. Si son personas que no pueden atender el pago de esos servicios, como se puede deducir, tienen menos facilidades para ejercer su derecho de supresión, por lo que la pregunta estriba en saber qué potencial tendrá la AEPD (o Autoridad de protección de datos) para hacer efectivo el derecho de supresión con la obligatoriedad del nuevo RGPD para todo ciudadano, independientemente de su nivel económico. Todo ello relacionado con el artículo 9.2 CE en cuanto a normas para facilitar su ejercicio efectivo.

8.3.4 La libertad sindical y la protección de datos.

El derecho fundamental a la libertad sindical (artículo 28.1 CE) fue objeto de desarrollo en la Ley Orgánica 11/1985, de 2 de agosto, de libertad sindical (LOLS) El artículo 2.1 LOLS estableció la libertad sindical como actividad de los trabajadores en la empresa. El artículo 8.1 c) LOLS reconoció expresamente el derecho de los trabajadores a recibir información de sus sindicatos en el ámbito de la empresa o centro de trabajo⁴⁹³. El TC, a su vez, ha reconocido en varias de sus Sentencias que el contenido del derecho constitucional a la libertad sindical no se limita a una actividad asociativa u

⁴⁹³ El artículo 28.1 CE se puede considerar como uno de los artículos mejor definidos de la CE en sus definiciones, con un sentido técnico y sin dejar lugar a interpretaciones. Esto es debido a la larga trayectoria del concepto que constitucionaliza, tanto a nivel nacional como internacional. Aun así, el artículo tiene variadas críticas, entre otras, ser obsoleto. Véase VIDAL MARÍN, TOMÁS; "La libertad sindical", *Anuario Parlamento y Constitución*, nº 4, 2000, pág. 201-238, pág. 202. La LOPD reconoce la cesión de datos por autorización en una ley, dentro del artículo 11 LOPD.

organizativa, sino también tiene una *vertiente funcional*, por la que los sindicatos gozan del derecho a ejercer actividades para la defensa, protección y promoción de los intereses de los trabajadores a través de medios de acción, para cumplir las funciones constitucionales⁴⁹⁴. Como todo derecho fundamental, se encuentra limitado, bien por los propios preceptos constitucionales, bien por la necesidad de “*preservar otros derechos o bienes constitucionalmente dignos de tutela*”⁴⁹⁵. El artículo 7.1 LOPD incluyó los datos personales relacionados con la actividad sindical dentro de la categoría de datos especialmente protegidos, en consecuencia, su tratamiento requerirá el consentimiento del titular expreso y por escrito, salvo los relacionados con sus afiliados.

El derecho a la protección de datos protege al trabajador como ciudadano, no tanto como trabajador, en el desarrollo de la relación laboral. Existe un vacío normativo en la materia, que fue suplido, quizá de una forma incompleta, por Resoluciones de la AEPD y los Tribunales. La AEPD realizó una serie de recomendaciones a las empresas a través de la *Guía* a la protección de datos en las relaciones laborales, pues la LOPD no

⁴⁹⁴ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Informe Jurídico 297375/2011 Protección de datos de trabajadores de la Administración Pública"]. Se citan en el Informe reseñado las STC 105/1992, de 1 de julio; STC 145/1999, de 22 de julio; STC 308/2000, de 18 de diciembre; STC 213/2002, de 11 de noviembre. La transmisión de información entre los sindicatos y sus afiliados, entre los delegados sindicales y los trabajadores “es el fundamento de la participación, permite el ejercicio cabal de una acción sindical, propicia el desarrollo de la democracia y el pluralismo sindical y, en definitiva, constituye un elemento esencial del derecho fundamental a la libertad sindical” cita de STC 213/2002 FJ4; en el párrafo que se cita, se exponen a su vez las SSTC 94/1995, de 19 de junio, FJ4; y 168/1996, de 25 de noviembre, FJ6. Véase también la SAN de 14 de abril de 2009, la cual confirmó la sanción a un determinado sindicato por difundir el censo electoral de las elecciones sindicales a través de correos electrónicos y la página web del sindicato, por lo que los datos trascendieron a terceros que no formaban parte de la actividad sindical, vulnerándose, entre otros, el artículo 10 LOPD respecto al deber de secreto que incumben al sindicato.

⁴⁹⁵ El Informe Jurídico cita a su vez las SSTC 11/1981, de 8 de abril; 2/1982, de 29 de enero; 91/1993, de 15 de marzo; 110/1994, de 11 de abril; 52/1995, de 23 de febrero; 37/1998, de 17 de febrero.

mencionaba el asunto de datos de trabajadores⁴⁹⁶. En la práctica, muchas empresas que tienen un número significativo de trabajadores, suelen elaborar códigos tipo de organización y funcionamiento (artículo 32 LOPD), por ejemplo, a través de normas incluidas en convenios colectivos sobre protección de datos y libertad sindical, situación de los representantes de los trabajadores en cuanto a sus datos propios y en cuanto a personas que tratan datos de carácter sensible de otros implicados, bien compañeros de trabajo, bien directivos o personal externo.

Se podría cuestionar el papel que determinan las empresas en el derecho a la protección de datos dentro del espacio laboral. Dentro de unas prácticas positivas, como puede ser la utilización de datos personales de los trabajadores para la optimización de la gestión empresarial y el cumplimiento de las obligaciones empresariales en materia de Seguridad Social e impuestos, se pueden encontrar otras prácticas ilícitas, que rozan, como se ha visto en el caso de la videograbación y vigilancia, el espionaje y el control indebido del trabajador, que por supuesto, nunca pierde su condición de ciudadano protegido por los DDFF. En palabras de DAVARA RODRÍGUEZ, se debe encontrar el *“difícil equilibrio de justicia dentro de la convivencia social”*⁴⁹⁷.

⁴⁹⁶ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Guía La protección de datos en las relaciones laborales"]].

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales2.pdf a 14 de julio de 2016.

⁴⁹⁷ DAVARA RODRÍGUEZ, MIGUEL ÁNGEL; , "El humanismo tecnológico", *Datospersonales.org, Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*. , nº 1, 2003, pág. 1-4. El caso de las PYMES se comenta en esta nota como colectivo que no afronta la necesidad de cumplir con los DDFF de los ciudadanos. Las PYMES han accedido en poco tiempo a medios tecnológicos avanzados, pero no tienen conocimientos de gestión ni recursos para abordar el asunto de la protección de datos. Menor todavía es el interés de los pequeños y medianos empresarios en proteger los DDFF. Cuando se encuentran ante una denuncia por lesión de uno de ellos, su reacción siempre es de incredulidad, rabia, ataque e inoperancia. No saben gestionarlos, lo ven como puro coste empresarial, una sanción es un impuesto más de las AAPP. No existe en la cultura empresarial española el concepto de respeto a los DDFF. Se apunta que la situación de ilegalidad, siendo también de inconstitucionalidad, es sumamente grave.

La actividad sindical sería deficientemente entendida en muchas empresas. Los bajos índices de sindicación fuera de la industria así lo expresan. Esa responsabilidad recae también en los trabajadores y en los propios sindicatos, que no han convencido de su gestión o no existe una cultura sindical en España como para promoverlos. Sin la actividad y ayuda de la Administración, la actividad sindical sería nula. En su vertiente hacia la protección de datos, los sindicatos no han mostrado una actividad acorde con la situación. No se conocen públicamente a través de los medios peticiones o demandas laborales en este sentido. En algunas resoluciones del TC se puede constatar que hubo alguna actividad al respecto, más en relación a la petición de información de trabajadores que en la promoción de una serie de normas sindicales en relación con la protección de datos personales. El ATC 29/2008, de 28 de enero, por ejemplo, rechazó el recurso de amparo interpuesto por un sindicato que exigía un listado de trabajadores/funcionarios a la Administración Pública, argumentando que: “el artículo 9 de la Ley 9/1987 no contempla la hipótesis del suministro de una información generalizada e indiscriminada de todos los aspectos relativos a la lista de puestos de trabajo de un determinado organismo público, ni, mucho menos, de determinados datos que afecten a las situaciones personales e individuales de todos y cada uno de los funcionarios públicos que los ocupan” (ATC 29/2008 FJ3) Aunque se trate de una Resolución en la que una de las partes es la Administración Pública, se puede extrapolar el sentido del texto como límite a la libertad sindical en beneficio del derecho a la protección de datos. En otro sentido, la SAN 371/2013, de 28 de enero, estima que prima el derecho a la libertad sindical frente al derecho a la protección de datos personales, casi con los mismos hechos, la publicación de nombres y apellidos de funcionarios/trabajadores de la Administración Pública por parte de un sindicato. En este caso, la difusión de los datos se limitó al centro de trabajo (Universidad Complutense de Madrid, UCM) por lo cual la AN estimó que, al figurar estos datos personales en la página web de la UCM, y siendo la publicación limitada a este centro de trabajo, primaba el derecho de información del sindicato en su ejercicio de libertad sindical a través de la información frente al derecho a la protección de datos personales. La AN anuló la sanción impuesta por la AEPD al sindicato. La AEPD, en su informe 0101/2008 se

había decantado por una posición más acorde con la protección de datos en cualquier situación ante la cesión, publicación o tratamiento de datos personales de trabajadores. En este Informe se establecen una serie de recomendaciones para la empresa y las AAPP en general donde promueve la cesión y tratamiento de datos de trabajadores de forma restrictiva, en el caso del Informe citado se trataba de correos electrónicos para informar sobre actividades sindicales. El sindicato sería responsable del fichero de datos personales que recibía para poder realizar sus labores informativas, debiendo informar a los titulares de datos, mantener las medidas de seguridad correspondientes y permitir el ejercicio de los derechos ARCO. La AEPD propuso en el año 2008 una sugerencia adoptada por algunas empresas como alternativa a la cesión de datos: implantar listas de distribución para el envío de correos electrónicos por parte de los sindicatos. Con esta propuesta, el sindicato se exime de cumplir con la LOPD y la empresa sigue manteniendo el control sobre los datos que de todos modos por imperativo legal debe mantener para su gestión. En cualquier caso, ante la petición de datos personales de trabajadores por parte de los sindicatos, la empresa debe documentar la cesión, aunque la información se encuentre en formato no automatizado (papel), para eximirse de responsabilidades en caso de que listados y cualquier otra información será tratada de forma no procedente. Igualmente, los sindicatos y los trabajadores pueden optar a multitud de plataformas informativas en la actualidad, desde redes sociales, páginas web, archivos compartidos, como ejemplos, en los que la empresa no tenga ningún tipo de implicación sobre la información que se desee transmitir. Por otro lado, como en los otros casos expuestos, se demanda una regulación por parte del legislador, para definir correctamente la interrelación de ambos derechos, libertad sindical y protección de datos. El artículo 88 RGPD establece que los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad

y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.”

El RGPD establece una fecha para realizar todas estas labores legislativas, en el mes de mayo de 2018. El asunto de la libertad sindical junto con todas las cuestiones que afectan a los derechos de los trabajadores (se supone que se encuentran incluidos los trabajadores/funcionarios de las AAPP) es objeto de regulación específica por parte de los Estados miembros. Estos se obligan a establecer la demandada regulación del tratamiento de datos en el ámbito laboral para toda la UE.

8.3.5 Intimidad, honor y protección de datos.

Una parte de este estudio se realizó a modo de introducción evolutiva y temporal desde el reconocimiento del derecho a la intimidad al reconocimiento del derecho a la protección de datos. La discusión doctrinal quedó zanjada por la STC 292/2000. La doctrina, a partir de entonces, tomó como referente el derecho positivo y la jurisprudencia del TC, manteniendo una actitud crítica, pero sin negar el hecho obvio de la existencia del derecho a la protección de datos personales. La realidad social y tecnológica actual se forma alrededor del derecho a la protección de datos, tanto para el

resto de derechos configurados en el artículo 18 CE, como frente a otros derechos y valores jurídicos relevantes, según se expone en este texto.

También como se ha analizado, la regulación del derecho a la protección de datos (tanto comunitaria como española) estableció dos conceptos de forma muy clara y específica: el concepto de dato personal y el concepto de tratamiento, artículo 3. a) y c) LOPD, respectivamente. De estos textos puede también deducirse que cualquier tipo de actividad, informática, telemática o simplemente manual, de datos personales, es un tratamiento de datos. Este tratamiento de datos, que actualmente puede ser masivo e indiscriminado debido a los nuevos sistemas tecnológicos (*big data*, por ejemplo), barato y accesible a cualquiera, puede constituir un riesgo para el ciudadano. Todo ello conduce, en palabras de MARTÍNEZ MARTÍNEZ, a una *reinterpretación del conjunto del ordenamiento jurídico en calve protección de datos*⁴⁹⁸. Se trata de una idea no exenta de riesgos, pues se podría incurrir en una excesiva producción normativa, o que allí donde el derecho fundamental a la protección de datos debería ceder ante intereses más dignos de protección, la ley no diga absolutamente nada y ello obligue a complejos esfuerzos de interpretación y a los riesgos que una situación así confronta, entre ellos una completa inseguridad jurídica a nivel de DDFF⁴⁹⁹, especialmente en cuanto a los derechos a la intimidad y a la propia imagen (honor), el ámbito de aplicación de la protección de datos frente a esos derechos sería cada vez mayor, con un riesgo evidente de desplazamiento de los derechos al secreto de las comunicaciones, la intimidad o a la propia imagen a favor de considerarlos formas de expresión del derecho a la protección de datos personales, en especial referencia a las imágenes fotográficas o de videograbación, que en la actualidad se tratan por doquier, sin control, tanto por particulares como por empresas⁵⁰⁰.

⁴⁹⁸ MARTÍNEZ MARTÍNEZ, R., "El Derecho Fundamental a la Protección de Datos: Perspectivas", , nº 5, 2007, pág. 52.

⁴⁹⁹ MARTÍNEZ, Obra citada.

⁵⁰⁰ Obra citada, p. 58. MARTÍNEZ considera que la reducción del artículo 18 CE a la protección de datos no significa que sea la técnica más eficaz ni la más adecuada. El autor argumenta en el año 2007 que el derecho a la protección de datos tiene un carácter instrumental desde la STC 254/1993. En la actuali-

Se podrían distinguir varias vías para la protección de la intimidad, la propia imagen y el derecho a la protección de datos personales, una no excluye a la otra. Por una parte, se encontraría la opción civil a través de la ley orgánica 1/1982, de Protección Civil del Derecho al Honor, a la Intimidad Personal y a la Propia Imagen⁵⁰¹. El derecho a la intimidad y a la propia imagen es un derecho irrenunciable e imprescriptible. Por tanto, en el ejemplo de captación de imágenes, se debería contar con la autorización del titular de la misma o concurrir algún supuesto de excepción al consentimiento, considerándose civilmente una intromisión en la vida privada de la persona si no existe tal consentimiento, objeto de demanda de indemnización por daños y perjuicios, cuya cuantía estará en función del daño producido⁵⁰². En segundo lugar, se encuentra la opción penal, la cual está tipificada en el artículo 197 CP, el cual tipifica como delito la conducta por la cual, para descubrir los secretos o vulnerar la intimidad de

dad, dicha instrumentalidad se cuestiona, pues se considera por otra buena parte de la doctrina como derecho autónomo. La STC 14/2003, de 30 de enero, abrió una reflexión a este respecto en relación al caso de la publicación y distribución a medios de comunicación por parte de la Brigada Policial de Valladolid de una fotografía tomada en dependencias policiales a un detenido, sujeto de investigación policial. La demanda de amparo se centraba en los derechos a la intimidad personal y al honor, artículo 18.1 CE, pero el TC resaltó la posible vulneración del artículo 18.4 y, por tanto, del derecho a la protección de datos. El TC consideró en este caso desproporcionada la difusión de este dato personalísimo, pues no aporta nada a la investigación y “pudo dañar la reputación de esa persona, en cuanto conlleva o puede conllevar, teniendo en cuenta actitudes sociales que son hechos notorios, un desmerecimiento en la consideración ajena, quedando de ese modo menoscabada su reputación” (STC 14/2003, de 30 de enero de 2003, FJ 12)

⁵⁰¹ Se comenta que la LO 1/1982, de 5 de mayo, no define los derechos que regula, es decir, no define en qué consiste la intimidad personal y familiar, el honor y la propia imagen. Determina el carácter del derecho como irrenunciable, inalienable e imprescriptible, equivale a la nulidad en caso de renuncia, en otras palabras, es nula ante la ley. Es necesario el consentimiento de la persona desde una perspectiva civil.

⁵⁰² Se podría incluso apuntar la pertinencia de los denominados daños punitivos, por los que el declarado culpable o responsable de violación del derecho a la intimidad, al honor y a la propia imagen estaría obligado a resarcir a los implicados dañados por esa acción por la cuantía equivalente a los beneficios obtenidos por el tratamiento y difusión de los datos. No pertenece a este estudio su análisis exhaustivo, pero se sugiere como posibilidad.

otro, sin su consentimiento, se apodere un tercero de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación. La pena para el delito es de 1 a 4 años de prisión y multa de doce a veinticuatro meses. En este sentido también puede ser condenada la conducta de transmisión y revelación de información íntima descubierta, aunque no se haya participado en la acción de descubrimiento. La tercera opción es la administrativa, ante la AEPD. En el ejemplo de la imagen difundida, lo determinante es que la persona titular pueda ser identificada o identificable a través de ese medio. Sin consentimiento del titular, el tratamiento del dato personal de la imagen se convierte en objeto de sanción por parte del Derecho Administrativo a través de la AEPD, independientemente de las otras vías de protección del derecho a la intimidad y a la propia imagen. El derecho a la protección de datos contribuye, en el caso de los derechos a la intimidad y a la propia imagen, a una mejor defensa de estos derechos constitucionales, sin resultar por ello una colisión entre los mismos. Todos estos derechos se complementan en un momento determinado, pudiéndose activar todas las vías descritas, si fuera concluyente y necesario. También se destaca la interrelación de estos derechos fundamentales del artículo 18.1 CE con otros, también constitucionales, en especial el derecho a la libre expresión e información. Se remite al punto tratado sobre esta cuestión.

8.3.6 Datos relativos a la salud.

El derecho a la salud está íntimamente relacionado con otros DDHH, como son el derecho a la alimentación, la vivienda, el trabajo, la educación, la no discriminación, el acceso a la información y la participación. Este derecho que se analiza junto con el derecho a la protección de datos, necesita de un conjunto de criterios de orden social para generar salud en todos los ciudadanos, como son la disponibilidad de los servicios de salud, la seguridad laboral, alimentos nutritivos y sanos libres de toxicidades, edu-

cación para el cuidado de la salud propia y la de otros. De los derechos tratados hasta ahora, el derecho a la salud se presenta con una implicación social contundente, pues el estado de salud de otros redunda e influye en el individuo. Una sociedad con aguas potables y corrientes, con higiene colectiva, alimentación variada, condiciones laborales seguras, entre otras características, se convierte en una sociedad avanzada. El control de la persona sobre su salud y su cuerpo sin injerencias y el acceso a un sistema de protección de la salud se convierten en objetivos de cualquier política sanitaria en países que alcanzan cierto grado de desarrollo. Para la Organización Mundial de la Salud (OMS) el mundo está interrelacionado en lo que concierne a ciertas enfermedades y dolencias. La violación de los DDHH se traduce en consecuencias sanitarias con mucha facilidad, que implica a todos los países⁵⁰³.

El artículo 43 CE enuncia el derecho a la protección a la salud, no como derecho fundamental, sino como un principio rector de la vida política, social y económica, que se materializará en el reconocimiento de facultades que los ciudadanos pueden ejer-

⁵⁰³ En la página web de la OMS se encuentra gran cantidad de información sobre sus actividades. <http://www.who.int/mediacentre/factsheets/fs323/es/>

Los últimos acontecimientos internacionales, como la Guerra de Siria, se han convertido en alerta sanitaria para los países de acogida, por ejemplo. También se apunta la severa crisis sanitaria producida por el virus ébola, la cual puso también a todo el sistema internacional en alerta. La difusión de los datos personales de los afectados en España por los medios de comunicación, supuso una manifestación de comportamientos colectivos poco recomendables en una sociedad avanzada. Los implicados y sus familias, en algunos casos simples vecinos o compañeros de colegio de los niños que vivían en un edificio que se difundió en los medios, sufrieron las consecuencias de un mal uso de datos personales. La tutela de los datos biosanitarios se encuentran en una encrucijada entre la intimidad y el interés público, como expresó PÉREZ LUÑO, A., "La protección de los datos personales de carácter sanitario", *Derechos Humanos y protección de datos personales en el siglo XXI*, 2013, pág. 122 y ss. La controversia entre el derecho a la intimidad sanitaria del individuo frente a la sociedad surgiría de "la exigencia de los poderes públicos de utilizar la transmisión de esos datos médicos, especialmente de los que hacen referencia a enfermedades contagiosas, o de aquellos que pueden ser utilizados para el desarrollo de avances en la investigación científica y el deseo de los ciudadanos de mantener un control sobre las informaciones que les conciernen". El equilibrio entre los derechos del paciente y la obligación garantista del Estado para mantener la salud de la sociedad es sumamente difícil de desarrollar en la práctica.

cer ante los poderes públicos y ante los otros ciudadanos, con disposiciones que realice el legislador⁵⁰⁴. Sin embargo, los datos relativos a la salud sí se consideran especialmente protegidos por la LOPD⁵⁰⁵, porque se consideran datos íntimos que afectan a la dignidad y libertad del ciudadano titular. Los datos relativos a la salud se encuentran, en palabras de MURILLO DE LA CUEVA, *en un plano en el que confluyen dos derechos fundamentales al menos: el derecho a la intimidad y el derecho a la autodeterminación informativa. E incluso pueden proyectarse sobre otros estrechamente relacionados*, como puede ser la libertad religiosa, ideológica, sexual, entre otros. El

⁵⁰⁴ MURILLO DE LA CUEVA, P., "El derecho fundamental a la protección de los datos relativos a la salud.", *Agencia Catalana de Protecció de Dats. Servicio de publicaciones.*, nº 1, 2005, pág. 18. Véase también la descripción del encuadre constitucional del derecho a la salud que realiza JIMÉNEZ DE PARGA, M., *El Derecho Constitucional a la protección de la salud*, , 2004, pág. 9-27. Más general pero no menos competente es REBOLLO DELGADO, LUCRECIO; SERRANO PÉREZ, M^a MERCEDES, *Introducción a la protección de datos*, Madrid, 2008, pág. 171 y ss..

⁵⁰⁵ La Directiva 95/46/CE estableció la prohibición de su tratamiento en su artículo 8.1. El nuevo RGPD incluye los datos de salud en el artículo 9, como tratamiento de categorías especiales de datos protegidos. Para el RGPD datos personales relativos a la salud son todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (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); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro." Definiciones del Considerando 35 RGPD, resaltando los datos genéticos definidos en el Considerando 34 como "los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente."

artículo 16 CE reconoce el derecho a no manifestar determinadas informaciones personales, como origen racial, tendencia sexual o ideas filosóficas. El artículo 18.1 CE protege la intimidad de las personas. En el caso de la gestión de datos de salud, estos aspectos se quiebran, pues para gestionar la salud de un ciudadano, el personal de atención sanitaria debe conocer aspectos de su intimidad que no se comparten con nadie más o sólo con los más íntimos. Es más, a través de los resultados de determinadas pruebas, el profesional de sanidad conocerá, quizá mejor que el titular de los datos, aspectos de su persona y de su vida.

la Ley 14/1986, de 25 de abril, general de Sanidad, especifica las facultades que tiene el paciente en su artículo 10, desplegando el derecho a la protección de la salud, adjudicando al ciudadano una serie de derechos (se puede describir como *haz de facultades*) y también estableciendo obligaciones para hacerlos efectivos. Reitera esta Ley de Sanidad derechos y deberes constitucionalmente establecidos, como son el derecho a la intimidad, a la dignidad humana, la no discriminación y por supuesto el valor supremo de la vida humana, para la cual la salud es imprescindible. En el año 1986, la Ley 14/1986 reconocía a los ciudadanos el derecho a la información sobre el tratamiento, los servicios sanitarios, los diagnósticos, la existencia de proyectos de investigación; el derecho a la confidencialidad, en especial con un médico asignado o elegido por el paciente; derechos de reclamaciones y propuestas; derecho a la obtención de medicamentos y productos sanitarios. Toda esta actividad generó, como se puede deducir, una ingente cantidad de datos relacionados con la salud. El artículo 23 de la Ley 14/1986 de 25 de abril, general de Sanidad, preveía la creación y utilización de registros en los que se recoge la información relacionada con la gestión sanitaria⁵⁰⁶. Los datos referentes a la salud tienen una amplia regulación específica, pues afecta a multitud de regulaciones, tanto públicas como privadas; su incidencia determinante en la vida de los ciudadanos, como individuos, pero también en la sociedad en general puede ser la causa de que el legislador, en el caso de los datos relacionados con la

⁵⁰⁶ Véase el interesante texto de HEREDERO HIGUERAS, M., "La protección de datos de salud informatizados en la Ley Orgánica 5/1992 de 29 de octubre", *DS Derecho y Salud*, nº 1, 1994, pág. 17-30. El texto es de hace más de 20 años, pero las observaciones son válidas.

salud, sí amplíe su actividad regulatoria, a nivel estatal y de CCAA. En la LOPD todo son expresiones de excepcionalidad para la recabación y tratamiento de datos relativos a la salud. El artículo 7 LOPD, que enumera los supuestos de su tratamiento lícito excluyendo otros posibles tratamientos de datos y marcando directrices estrictas para cuando sea necesario su tratamiento, en sus puntos 2, 3, 4 y 5. Desde el punto de vista de la necesaria atención médica, se debe puntualizar que la LOPD autoriza expresamente en el artículo 7.6 y 8 el tratamiento de datos relacionados con la salud y todos los demás datos especialmente protegidos que sean necesarios para gestionar una situación vital del titular, cuando la finalidad esté relacionada con la protección de la salud y la vida humana⁵⁰⁷. El concepto de dato personal relacionado con la salud se define claramente en el Reglamento LOPD, artículo 5.1.g) como “las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. Se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética”. Como datos relativos a la salud se consideran los relacionados con los fines de la salud, tratados por la Sanidad Pública, la protección social, la investigación científica y las estadísticas públicas, según se reguló en la Directiva 95/46/CE. Se puede extender el concepto de dato de salud a

⁵⁰⁷ Se permite que los datos sobre ideología, afiliación sindical, religión, creencias, origen racial, vida sexual o cualquier otro dato, sean tratados cuando ello resulte necesario para prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamientos médicos o gestión de servicios sanitarios, aunque esta información debe ser tratada por profesionales sanitarios sujetos al secreto profesional o por personas bajo la misma obligación de secreto. Se admite también que se traten los datos especialmente protegidos para el caso de que la persona titular afectada se encuentre física o judicialmente incapacitada para otorgar consentimiento válido. El artículo 8 LOPD autoriza el tratamiento con carácter general a los Centros Sanitarios públicos o privados y a las Instituciones relacionadas con la salud de los ciudadanos, circunstancia que amplía la LBAP, con la obligación de documentar la asistencia sanitaria y al archivo de documentación según unas normas estrictas de seguridad. La LOPD excluye la necesidad de consentimiento del titular para cesiones de datos en casos de urgencia, estudios epidemiológicos o cualquier otra contingencia grave de alerta sanitaria. Para los casos de cesión a entidades aseguradoras es necesario siempre el consentimiento expreso del titular o su representante legal que permite la Disposición adicional sexta LOPD. Véase GARRIGA DOMINGUEZ, A., *Tratamiento de datos personales y derechos fundamentales*, Madrid, 2004, pág. 110 y ss..

todo lo referente con el cuerpo humano, incluyendo los antecedentes familiares, hábitos de vida, hábitos alimentarios, historia personal, trabajo o empleo, enfermedades propias y familiares, pasadas o previsibles, físicas o psíquicas, como se incluyó en el Convenio 108 del Consejo de Europa. Estos datos conforman la *biografía de una persona*⁵⁰⁸.

Aparte de la LOPD y su Reglamento, la Ley 41/2002 de 14 de noviembre, básica reguladora de la autonomía del paciente (LRAP), estableció claramente obligaciones y derechos en cuestiones clínicas y de salud en relación con información y documentación referente a las personas. El artículo 7.1 de la LRAP dispuso que *toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley*. El artículo 3 LRAP trata el concepto de información clínica, como *todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla*. El mismo artículo define la documentación clínica como *el soporte de cualquier tipo o clase que contiene un grupo de datos e informaciones de carácter asistencial*. Los soportes de datos de salud generan la historia clínica, también definida en artículo anteriormente mencionado, como *conjunto de documentos que contiene los datos, valoraciones e informaciones de cualquier índole sobre la situación y evolución clínica de un paciente a lo largo del proceso asistencial*. El artículo 15.1 LRAP establece que todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado (los datos pueden estar en soportes fotográficos, radiografías, gráficos en cualquier formato) de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto

⁵⁰⁸ MURILLO DE LA CUEVA, obra citada, pág. 10. Destaca el autor la STC 202/1999, de 8 de noviembre, anterior a la LOPD, por la cual el TC consideraba vulnerado el derecho a la intimidad de los trabajadores de una entidad bancaria por el almacenamiento en soporte informático de los diagnósticos médicos del trabajador, sin mediar su consentimiento expreso, pues carecía de apoyo legal y suponía una restricción desproporcionada del derecho fundamental. Los datos se habían obtenido a través de los servicios médicos de la empresa durante las revisiones periódicas para vigilar la salud de los trabajadores, junto con los diagnósticos de enfermedad realizados para las bajas temporales de incapacidad laboral.

en el ámbito de atención primaria como de atención especializada. La elaboración de la historia clínica es un derecho del paciente y un deber de los profesionales sanitarios⁵⁰⁹. Se debe procurar la máxima información posible sobre cada paciente para realizar el servicio sanitario de forma correcta y maximizando los recursos, identificando a los profesionales del tratamiento de un paciente, la forma, contenido, fechas y cualquier otro aspecto relevante del tratamiento y de la persona, integrando todos los datos para servir al fin superior, que es la vida humana, el derecho fundamental primordial de toda persona. La información médica es titularidad del paciente, salvo excepciones singulares con el consentimiento del titular o por imperativo legal. Cuando entra en colisión el derecho a la protección de datos o el derecho a la intimidad con el derecho a la salud o a la vida, lógicamente que priman éstos últimos, el derecho a la vida y a la salud. Ello no es óbice para no cumplir con la regulación de protección de datos de forma exhaustiva en cuanto al tratamiento de los datos de salud, tanto por los Servicios de Salud Pública, Centros Sociales, Centros Sanitarios en general o clínicas de cualquier especialidad (odontológica, analítica, fisioterapéutica, entre otras) porque las consecuencias de la inobservancia de la protección de datos, puede tener importantísimas consecuencias en los ciudadanos⁵¹⁰.

⁵⁰⁹ Por ejemplo, la regulación específica en el Real Decreto 1718/2010, de 17 de diciembre, sobre receta y órdenes de dispensación hospitalaria. Se establece las medidas para la protección de la confidencialidad de los datos en los artículos 11 y 19 del RD mencionado. El Real Decreto 183/2004, de 30 de enero, de regulación de la Tarjeta Sanitaria individual, válida para todo el sistema de salud nacional español pero emitida por las CCAA a los residentes en su territorio. La Tarjeta Sanitaria individual permite un acceso a la historia clínica individual de cada paciente. Una visión práctica en GARRIGA DOMINGUEZ, ANA; ÁLVAREZ GONZÁLEZ, SUSANA; "Historia clínica y protección de datos personales: recomendaciones y propuestas en torno al uso de la información.", *El Tiempo de los Derechos*, nº noviembre, 2010, pág. 12 y ss.. "La finalidad principal de la historia clínica es la de recoger y archivar los datos necesarios del paciente para llevar a buen término una adecuada asistencia sanitaria. Consecuentemente, todos los datos que consten en la misma deberán ir encaminados a esta finalidad. Cualquier otro uso de los datos personales contenidos en la historia clínica ha de considerarse secundario, excepcional, restringido y subordinado al primero."

⁵¹⁰ La Ley 11/2007, de 22 de junio, de Acceso Electrónico de los ciudadanos a Servicios Públicos define los documentos electrónicos como "la información de cualquier naturaleza en forma electrónica, archi-

Un dato especialmente protegido relacionado con la persona y que la CE no menciona es el dato genético. La Ley 14/2007, de 3 de julio, de investigación biomédica⁵¹¹, sí define el dato genético: "información sobre las características hereditarias de una persona, identificada o identificable obtenida por análisis de ácidos nucleicos u otros análisis científicos"⁵¹² Es una información personal tan transcendente que afecta a multitud de áreas jurídicas. Permite la identificación del individuo sujeto de derechos y obligaciones vivo o muerto, relacionándole con otros sujetos, que están en ese momento o que han fallecido, pero generando una historia, bien personal, bien genealógica, detectando posibles patologías, capacidades o predisposiciones. Estos datos pueden afectar a la sociedad al ser utilizados con diferentes orientaciones de cultura, raza, medioambiente, educación, trabajo, entre otras⁵¹³. En las manos inadecuadas,

vada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado" La definición se puede extender a otros ámbitos de protección de datos personales. Incidencia en el concepto de dato personal genético tuvo la STEDH sobre los asuntos 30562/04 Y 30566/04 de 4 de diciembre de 2008, por la cual los perfiles de ADN y las muestras celulares son considerados como datos de carácter personal. GONZÁLEZ FUSTER, G., "Comentarios a la Sentencia del Tribunal Europeo de Derechos Humanos 30562/04 Y 30566/04, vida privada y los límites al tratamiento de datos biométricos de personas no condenadas.", *Revista de Derecho Comunitario Europeo.*, nº 33, , pág. 619-633.

⁵¹¹ ABELLÁN GARCÍA SÁNCHEZ, F., "Los análisis genéticos dentro de la Ley de Investigación Biomédica", *Revista de la Escuela de Medicina Legal*, nº junio, 2009. Otros autores también comentan extensamente este aspecto, véase GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 103.

⁵¹² Artículo 3. j), dato genético de carácter personal, Ley 14/2007 de Investigación biomédica.

⁵¹³ GÓMEZ SÁNCHEZ, Y., "La protección de datos genéticos. El derecho a la autodeterminación informativa.", *Revista Derecho y Salud*, nº Extra., 2008, pág. 61. En más detalle, ÁLVAREZ GONZÁLEZ, S., *Derechos Fundamentales y protección de datos genéticos*, Madrid, 2008, pág. 40 y ss. Y más actualmente, ÁLVAREZ GONZÁLEZ, S., "La protección de los datos genéticos de carácter personal", *Derechos Humanos y protección de datos personales en el siglo XXI*, , 2013, pág. 155-184. El impacto en los juristas de la información biomédica es muy considerable. El legislador le ha dedicado a este aspecto de la personalidad mucha más atención que a otros derechos, por lo que doctrinalmente y bajo el punto de vista de la filosofía y teoría del Derecho se comienza a denominar como *Bioderecho* una nueva rama jurídica relacionada con la información y tratamiento del genoma humano, aunque determinados autores, como PECES BARBA o PÉREZ LUÑO analizaban la materia hace muchos años como

se convierte en una información relevante para realizar actos contra los ciudadanos, como discriminaciones ilegales, por razones eugénicas, de raza o de sexo, por ejemplo. Existirían también importantes intereses económicos alrededor de los datos genéticos para la producción de medicamentos novedosos, como, por ejemplo, los medicamentos personalizados que se prometen más eficaces que los medicamentos genéricos.

La LOPD y su Reglamento confirieron a los datos de salud una detallada regulación desde su recabación hasta su eliminación. Deben ser especialmente proporcionales, adecuados, pertinentes y no excesivos, ser tratados para la finalidad específica y legítima, totalmente limitada a la actividad sanitaria, salvo excepciones establecidas en la ley, decisiones de una autoridad judicial o en casos de urgencia sanitaria. Deben ser datos exactos, no pueden contener información irrelevante, salvo excepciones de investigación o de seguimiento profesional, pero con un sistema de disociación adecuado⁵¹⁴. El consentimiento informado para el tratamiento de datos de salud debe ser muy específico acompañando de una obligación de confidencialidad y secreto que deben materializarse en la seguridad del tratamiento, automatizado o no automatizado de los datos de salud. El acceso a la información de la historia clínica por parte del titular se reconoce en el artículo 18 LRAP, con importantes excepciones polémicas: no puede ejercitarse en perjuicio del derecho de terceros a la confidencialidad ni en

posible objeto de regulación. Véase PÉREZ LUÑO, A., *Nuevas Tecnologías y Derechos Humanos*, Valencia, 2014, pág. 38 y ss. . Texto realizado por ÁLVAREZ GONZÁLEZ, S. Véase también PÉREZ LUÑO, A., "La protección de los datos personales de carácter sanitario", *Derechos Humanos y protección de datos personales en el siglo XXI*, , 2013, pág. 113-146.

⁵¹⁴ Los métodos de disociación o anonimización (así lo denomina la Ley 14/2007 de Investigación biomédica, artículo 3.c) se definen como: "proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere. Es aplicable también a la muestra biológica) son amplios y variados. Son la garantía de la confidencialidad y del cumplimiento del derecho fundamental a la protección de datos, junto con el cumplimiento y protección de otros DDFF y derechos en general. Una exposición sobre disociación véase en ABERASTURI GORRIÑO, U., "La cesión de datos de salud fuera del ámbito sanitario", *Revista vasca de Administración Pública*, nº 91, 2011, pág. 17-101. Una pequeña aportación con elementos prácticos en disociación es GÓMEZ PIQUERAS, C., "Disociación/anonimización de los datos de salud", *DS Derecho y Salud*, nº 1, , pág. 43-56.

perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponerse a que se acceda a sus anotaciones de carácter subjetivo. Este punto ha sido muy discutido, pues impide el ejercicio del derecho de acceso a los datos de salud y en general impide el derecho a la protección de datos y a otros DDFF. Solamente se puede justificar esta excepción por la preferencia que otorgó el legislador a los intereses de los profesionales médicos, los cuales participaron en la elaboración de la LRAP⁵¹⁵.

Existe una especial problemática en el tratamiento de los datos de salud por personal no sanitario, pues este tipo de datos son tratados en muchas ocasiones por centros no sanitarios, como puede ser un centro social, en el que los profesionales son trabajadores sociales⁵¹⁶. En estos casos, se debe restringir el acceso a los datos de la historia clínica y permitir el acceso únicamente a los datos de la historia social, la cual contendrá solamente los datos de salud que exclusivamente repercutan en la historia social. Los ficheros serán distintos y los permisos de acceso también deben serlo. La interrelación de ambos ámbitos, el social y el sanitario, a través de sistemas automatizados es cada vez mayor, pues proporciona una gran calidad de atención a los ciudadanos y promueve la salud y la atención integral socio-sanitaria, como puede ser la atención a personas mayores de 80 años, discapacitados, personas en tratamiento de rehabilitación física o mental, entre otros ejemplos, que necesitan servicios sociales y sanitarios coordinados. El tratamiento de datos en grandes servidores con un

⁵¹⁵ MURILLO DE LA CUEVA, obra citada, pág. 15. En otras referencias también se comenta como dudosa su pertinencia: PALOMAR OLMEDA, A., "Confidencialidad y protección de datos en la Ley de Salud Sexual.", *DS Derecho y Salud*, nº 2, 2010, pág. 78. entre otros. El Decreto 29/2009 de 5 de febrero de la Comunidad Autónoma de Galicia sí define qué puede entenderse como anotaciones subjetivas dentro de su artículo 21: "Valoraciones personales sustentadas o no en los datos clínicos de que se disponga en ese momento, que no formando parte de la historia clínica actual del/la paciente o usuario, puedan influir en el diagnóstico y futuro tratamiento médico una vez constatadas." Se añade en el artículo citado que el personal sanitario deberá abstenerse de incluir expresiones, comentarios o datos que no tengan relación o validez con la asistencia sanitaria recibida.

⁵¹⁶ BELTRÁN AGUIRRE, J., "Tratamiento de datos de salud en la prestación de servicios sociales", *DS Derecho y Salud*, nº 1, 2009.

avance importante de la implementación de programas de gestión masiva de datos o *big data*, han puesto de relieve un avance enorme del sector sanitario, asistencial, investigador e incluso farmacológico. Los datos de salud se están transformando con nuevos sistemas de tratamiento en fuentes de prevención de enfermedades, en personalizaciones de los tratamientos, en gestión más eficaz de enfermedades, accidentes y dolencias en general. Todo ello se traduce en una notoria mejora social y en un avance generacional muy importante, gracias al derecho a la salud y su implicación en otros derechos⁵¹⁷.

El otro lado del masivo tratamiento de datos de salud se encuentra en fallos de gestión, bien porque en algunas instalaciones no se ha modernizado el sistema, sigue existiendo archivos incontrolados de papel, por ejemplo; o bien porque el personal que accede a los datos no tiene en cuenta sus obligaciones respecto a la protección de datos. Es cierto que el personal clínico debe dar mayor prioridad a su labor asistencial que a su labor documental. No es menos cierto que muchos de ellos no consideran trascendente la documentación clínica. Otros generan ilícitamente un mercado o trasiego de datos personales clínicos, para diversas finalidades abyectas (en el sentido de despreciable), en el ámbito del Derecho Penal. Los profesionales de la medicina y el personal sanitario están obligados por un estricto código deontológico, que supera la protección de datos personales regulada en la normativa. La confidencialidad y el secreto son la base del derecho a la intimidad del paciente y del derecho a la protección de los datos de salud. Dos derechos fundamentales muy trascendentes y que se consideran de especial protección, en manos de profesionales poco éticos, muchos de ellos ajenos a los DDFF, bien por deficiencias en su formación, bien porque no tienen interés; o bien, en una conducta completamente intencionada, al objeto de

⁵¹⁷ Es interesante ampliar la información sobre temas tecnológicos y sanitarios en la referencia AUTORES, ., "Los Retos de la Seguridad y Privacidad en la atención integral sanitaria y social", *XIII Foro de Seguridad y Protección de Datos en Salud*, nº 116, 2016. No tiene demasiado contenido en relación a los DDFF pero sí es una buena fuente de información sobre el sistema público de gestión de la Sanidad en España.

realizar un acto antijurídico⁵¹⁸. En este sentido, la STS 185/2016, de 3 de febrero, condenó la acción de un médico por delito de descubrimiento de secretos y acceso ilícito a historiales médicos de cinco personas, a pena de prisión por dos años, seis meses y un día.⁵¹⁹ La Sala de lo Penal confirmó la Sentencia de Instancia, que había considerado hechos probados el acceso a los archivos de historiales médicos con su usuario y contraseña de diversas personas, descubriendo datos de especial relevancia. La STS 185/2016, de 3 de febrero se remite a la STS 1084/2010, de 9 de diciembre en cuanto a la interpretación del artículo 197.2 CP⁵²⁰, contra la libertad informática, como “delito que atenta a la intimidad de las personas mediante una conducta típica que va referida a la realización de un uso ilegítimo de los datos personales insertos en programas informáticos, electrónicos o telemáticos. Se trata de datos reservados que pertenecen al titular pero que no se encuentran en su ámbito de protección directo,

⁵¹⁸ Véase el interesante artículo sobre seguridad informática en el sector sanitario. Se conoce la existencia de ataques a los sistemas de datos en EEUU porque en ese país las empresas y las organizaciones están obligadas a comunicar a las Agencias Gubernamentales los ataques de la llamada ciberdelincuencia, con la finalidad de detectar brechas en la seguridad e informar a los ciudadanos. Por esta razón se conoce que el que el año 2015 se produjeron más de 250 fallos en seguridad con el robo de más de 112 millones de registros de datos sanitarios. Esta información se paga con altas sumas en el mercado ilegal de datos personales. Las empresas e instituciones pueden ser también extorsionadas para no hacer público un robo de datos masivo o para devolver su acceso. Otro riesgo es el acceso indebido a sistema de control de maquinaria y tecnología médica, muy peligroso en sus consecuencias. Los delincuentes pueden acceder a marcapasos que lleva un ciudadano implantado en su interior, a máquinas que expenden insulina o medicamentos en general para pacientes críticos, por ejemplo.

http://www.abc.es/tecnologia/redes/abci-millones-datos-pacientes-riesgo-agujeros-seguridad-informatica-201608070100_noticia.html

⁵¹⁹ El asunto comenzó con la ruptura sentimental del condenado con la perjudicada, compañeros de trabajo en un Centro de Salud de Mahón. El condenado penalmente accedió a datos de salud de la perjudicada y sus familiares, descubriendo asuntos íntimos a los que no tenía autorización para acceder. Su conducta es continuada, reiterada, voluntaria y de agresión a la intimidad de todos los implicados.

⁵²⁰ En referencia a la doctrina del TS sobre los datos considerados *sensibles* la STS 185/2016, de 3 de febrero de 2016 se remite a la STS 532/2015, de 23 de septiembre, porque “la ley no distingue a la hora de darles protección y el tipo penal prevé una agravación (art. 197.6 CP) para los supuestos en los que el objeto sea especialmente sensible, afectando a ideología, religión, creencias, origen racial o vida sexual.”

directamente custodiados por el titular, sino inmersos en bases de datos, en archivos cuya custodia aparece especialmente protegida en orden a la autorización de su inclusión, supresión, fijación de plazos, cesión de información, etc., de acuerdo a la legislación de protección de datos, delimitando claramente la titularidad y manejo y cesión de la información contenida en los mismos.” (FJ2) La Sentencia 185/2016, de 3 de febrero, continuó estableciendo una interesante definición de qué supone perjuicio en este tipo de delitos. Perjuicio no supone para el Tribunal que el delito lleve implícita una finalidad económica, sino que perjuicio, en este caso, es también el *“peligro de que los datos albergados en las bases de datos protegidas puedan llegar a ser conocidos por personas no autorizadas*. En el caso ese perjuicio se ha producido, y el autor lo pretendió al tomar conocimiento de un dato personal especialmente sensible en nuestro ámbito cultural, inherente a la intimidad más estricta que no interesa sea conocido fuera de la privacidad y hacerlo con conocimiento de una actuación contraria a la norma que permite su acceso.”⁵²¹ Es relativamente sencillo y frecuente realizar un uso indebido de la información sensible en el ámbito de la salud. Se tiene información sobre tipologías de conductas de diversa índole, desde el médico que contacta con familiares de un paciente en contra de su voluntad y sin consentimiento para informarles de su estado físico, pues lo considera su deber, hasta los accesos por personal no sanitario a datos de salud para finalidades comerciales. Pocos casos llegan a los Tribunales, pues probarlos es muy difícil en la mayoría de ocasiones, al no existir una conciencia de seguridad de datos eficaz. Por todo ello se puede concluir que el derecho fundamental a la protección de datos es constantemente vulnerado en cuanto a los datos especialmente protegidos de salud.

⁵²¹ “El perjuicio se realiza cuando se apodera, utiliza, modifica o accede a un dato protegido con la intención de que su contenido salga del ámbito de privacidad en el que se incluyó en una base de datos, archivo, etc., especialmente protegido, porque no es custodiado por su titular sino por titulares de las bases con especiales exigencias de conductas de protección. (FJ2)” El Tribunal se remite a las SSTs de 11 de julio de 2001 y 532/2015, de 23 de septiembre, al reseñar que el perjuicio se refiere a la invasión de la intimidad y no a la producción de un quebranto económico patrimonial concreto.

9. La Seguridad de los Datos.

La protección de datos se materializa en las medidas de seguridad. La seguridad técnica y real de los datos es su auténtica protección. Tiene muchas vertientes de análisis, técnico y jurídico. El objeto de este estudio, dentro, por lógica, de la normativa jurídica, se centra en el artículo 9 de la LOPD, donde se establece el llamado principio de seguridad, y los artículos del Título VIII del Reglamento de la LOPD, que aporta su lectura técnica, más o menos cuestionable, efectiva y eficaz. La seguridad de datos, su protección, va más allá de la protección de los datos personales y más allá de la LOPD. A nivel técnico, la protección de los sistemas en los que se tratan datos (todos los datos, incluidos los personales) se convierte en una necesidad empresarial de primer nivel. Los datos y su tratamiento serán el núcleo de la actividad empresarial en todos los sentidos, desde los departamentos de innovación (desarrollo de nuevos productos, por ejemplo), los de mercado, marketing y publicidad (estrategias de ventas y expansión), los de finanzas y gestión (importantísima gestión de datos) hasta los de producción o logística. Todos los niveles de gestión empresarial, conectados entre sí por una obvia necesidad de comunicación, se tienen que proteger. No tanto a nivel de los llamados ataques externos, que los hay, sobre todo hacia grandes corporaciones, sino también para pequeñas y medianas empresas, donde los datos son mucho más valiosos de lo que, hasta hace muy poco, se consideraba por sus gestores, más preocupados por ganarse el día a día que por la gestión de sus empresas y actividades económicas, sin diferencias por formación o ingresos.

En cuanto a los datos de carácter personal, las leyes anteriores a la LOPD sirvieron para una tímida concienciación, que se propagó más seriamente ante la llegada de *internet* y sus gestiones de bienes y servicios online; con la llegada de la Administración Electrónica, y con la expansión de la comunicación por terminales móviles denominados *inteligentes*. La LOPD necesitaba del Reglamento para afrontar muchos aspectos en cuanto a la protección de datos personales. El Reglamento pormenorizó las posibles medidas de seguridad, sirviendo de orientación a pequeñas empresas de informática, cuya consultoría, en estos aspectos legales, es más que cuestionable, pero

que la LOPD no prohíbe y, por tanto, existió⁵²². Crea, a su vez, los mínimos de seguridad en función de los datos a proteger, lo que concierne a los empresarios y profesionales sobre la utilización de los datos personales, la obligación de redactar un Documento de Seguridad, el cual debe mantenerse actualizado en cuanto a usuarios y accesos, no sólo a ficheros en formato digital, también a ficheros en formato físico (papel, por ejemplo), tanto para su tratamiento, como por su simple acceso a la zona de almacenamiento de soportes; también se establecen los niveles de seguridad en función de los datos almacenados y su nivel de sensibilidad.

La protección de datos personales y la seguridad de datos pueden ir juntos en su aplicación, pero son dos conceptos diferentes para determinados colectivos, en especial, los técnicos de informática. La seguridad de datos o de la información es un término genérico, como una serie de medidas preventivas o que determinan una reacción ante un supuesto. Pretenden proteger la información, la confidencialidad de la misma, junto con la disponibilidad para los que así lo administren y que sea una información íntegra. La información puede encontrarse no sólo en un ámbito de tecnologías de la información, también puede estar en otros soportes y lugares, que son más físicos, como, por ejemplo, un archivo de documentos en papel, que puede verse en multitud de notarías y Registros. La protección de datos personales tiene una definición jurídica, centrada en las personas y sus datos, pues implica derechos de los ciudadanos. Se pretende evitar efectos negativos hacia las personas físicas y se convierte, por tanto, en una obligación jurídica.

⁵²² Se cuestiona la viabilidad de consultas atendidas por personas que saben un poco de técnicas de informática, pero carecen de cualquier formación en Derecho. Se puede considerar intrusismo profesional, actuar sin la correspondiente acreditación de conocimiento jurídico. Así han sido los frutos: por ejemplo, se destinaban fondos de formación para las adecuaciones a la LOPD, por empresas de formación sin la más mínima idea de Derecho. Eso era un fraude, uno más entre tantos que se cometieron con los fondos de formación. Igualmente, hubo empresas que promocionaban la adecuación a la LOPD bajo formas de distorsión de la realidad, que muchos pequeños empresarios, sin demasiado conocimiento e información, aceptaban, pagando servicios que inducían a suponer que, si no se admitían sus honorarios, la AEPD les impondría una severa multa.

La seguridad, como tal, se puede definir como *la característica que indica que un sistema está libre de todo peligro, daño o riesgo*. Si se habla de la seguridad de la información, puede ser definida como un *conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información*⁵²³. La seguridad se debería entender como “la acción de garantizar que un sistema de información sea eficaz, y un sistema de información es eficaz si obtenemos de él aquello para lo que se ha diseñado”⁵²⁴. La llegada de los sistemas informáticos y la digitalización de la información permiten que toda la problemática de gestión de grandes cantidades de datos en papel, quede solucionada. Se gana espacio físico, de superficie útil, para otras finalidades, se obtiene rapidez en el procesado de la información y mejoras en el acceso, transporte y almacenamiento. También aparecen otros problemas, como se analizó en la evolución del derecho a la protección de datos⁵²⁵. La seguridad en los sistemas informáticos, los soportes de datos automatizados como los denominó la LOPD y su Reglamento, se puede definir como el *conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información*, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. La confidencialidad realiza una protección de los datos ante el conocimiento de terceros no legitimados, sólo deben ser conocidos por las personas autorizadas. La integridad impide que la información sea alterada sin conocimiento de su titular. La disponibilidad de los datos es necesaria para quien está autorizado o legitimado para su tratamiento, sin esa disponibilidad no podrá cumplir con su cometi-

⁵²³ GOBIERNO DE ESPAÑA. MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE. OBSERVATORIO TECNOLÓGICO., "Introducción a la seguridad informática. Seguridad de la información. "]. <http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1>>

⁵²⁴ MIRALLES LÓPEZ, RAMÓN;., "Seguridad de la información y protección de datos personales. ", *Comentario a la Ley de Protección de Datos Personales*, , 2010.

⁵²⁵ Como serían la violación de la integridad de la información (se puede variar con más facilidad), la desaparición de datos (el borrado de datos, bien por error humano, bien por fallo técnico, bien por voluntad de hacer desaparecer la información contenida con fines delictivos o no lícitos) llevan a cuestionar cada vez más la necesidad de seguridad.

do⁵²⁶. La seguridad es un proceso que no termina nunca, pues los riesgos nunca se acaban ni se eliminan totalmente. Eso no quiere decir que no se pueda gestionar. La prevención, el análisis del riesgo y la eficacia de las medidas de seguridad, siempre en pruebas y siempre mejorando, son las mejores herramientas con las que cuenta la seguridad de datos⁵²⁷. La seguridad total no existe en ningún aspecto de la vida, y no existe, por tanto, en la protección de datos de carácter personal. Eso no es óbice, para que no se pongan todos los medios al alcance de una organización para que la seguridad sea efectiva, al menos en mínimos. Se pueden garantizar unas condiciones mínimas de seguridad en su confidencialidad, en su integridad y en su disponibilidad, a través, por ejemplo, de accesos a la información autenticados y controlados, controlando la integridad de los datos, que no se puedan modificar ni se tenga acceso a los mismos si no es con permisos controlados también. Al mismo tiempo, se pueden clasificar los peligros, conocer los que se hayan manifestado, y protegerse contra los daños, al menos, los más probables y conocidos. De esta forma, el riesgo se minimiza.

La AEPD editó en su página web la *Guía de Seguridad de Datos*⁵²⁸. Es un resumen del Título VIII del Reglamento LOPD, contiene un modelo de Documento de Seguridad y una relación de comprobaciones para facilitar la Auditoría de Seguridad⁵²⁹.

⁵²⁶ REBOLLO DELGADO, LUCRECIO; SERRANO PÉREZ, M^a MERCEDES, *Introducción a la protección de datos*, Madrid, 2008, pág. 147 y ss. En este caso, es SERRANO PÉREZ la encargada de presentar los aspectos relevantes de la seguridad en la gestión y tratamiento de datos personales. Aunque no es reciente, sus análisis siguen estando vigentes, pues no se ha prestado la debida atención a la seguridad por parte de las empresas españolas. Se debe reconocer que algo se ha modificado en sus procedimientos, en especial en las grandes corporaciones.

⁵²⁷ Sobre la cuestión, existe una cita de EUGENE SPAFFORD, profesor en la Universidad de Indiana (EEUU) que dice lo siguiente: "El único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes de seguridad bien pagados y muy bien armados. Aun así, yo no apostaría mi vida por él".

⁵²⁸ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Guía de Seguridad de Datos"]. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf

⁵²⁹ El artículo 9 de la LOPD tiene el siguiente enunciado:

Sería más preciso hablar de *seguridad en el tratamiento de datos* que de seguridad de datos. La seguridad se aplica a los tratamientos de datos, no a los datos en sí mismos, independientemente del soporte en que estén los datos. La Directiva 95/46/CE emplea el término de seguridad en el tratamiento, mientras que la LOPD utiliza la expresión seguridad de los datos⁵³⁰.

La gestión de la seguridad en los sistemas informáticos tiene muy poca historia, por lo que no se puede hablar de muchos ejemplos. Los técnicos informáticos van generando diferentes formas de gestionar la seguridad, pero no existe una serie de procedimientos estandarizados y probados, legalmente exigibles, para gestionar la seguridad. Por ello, estas normas del Título VIII del Reglamento de 2007 son muy generales, dejando al responsable del fichero o tratamiento dentro de lo que se denominó *autorregulación de seguridad*. Se van a resumir estas indicaciones, pues son eso, indicaciones más que normativas.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y evite su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Este artículo es una transposición del artículo 17 de la Directiva 95/46/CE del 95. La relación de las medidas de seguridad se encuentra en el Reglamento.

⁵³⁰ Es un apunte del autor MIRALLES LÓPEZ, en el análisis que se referencia, que así lo detecta entre los diferentes textos legales. Existe toda una confusión de términos entre Directiva 95/46/CE, LOPD y Reglamento de protección de datos personales. Se confunde protección de datos, de ficheros, de tratamiento o de información, cuando son cuestiones y conceptos diferentes. El autor lo aclara en las páginas 708-709 de la obra mencionada. En cualquier caso, el sentido de las normas será la protección de los tratamientos, para proteger los datos que nos ocupan, de carácter personal, aunque el concepto sea de gestión de la información, más allá de un imperativo legal.

9.1. La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: el método MAGERIT.

A nivel institucional, existe por parte del Estado el llamado método MAGERIT⁵³¹ (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) que se generó por parte de la Administración española. Este protocolo se elaboró por el Consejo Superior de Administración Electrónica (el anterior Consejo Superior de Informática) Las normas ISO, que la página web de MAGERIT menciona, también realizan varias propuestas en este asunto, como son las normas ISO 31000 y 27000, que pueden ser certificadas como ISO, pero nada más, no existe un estándar obligatorio, no existe un organismo público de verificación de la seguridad en el tratamiento de datos, y por tanto, de la seguridad en los datos personales y su vinculación con los DDFF.

Para MAGERIT existen las siguientes dimensiones de la Seguridad:

- Disponibilidad. Los servicios deben poder usarse con inmediatez.
- Integridad. Los datos deben ser correctos y completos.
- Confidencialidad. Sólo las personas autorizadas deben acceder a una información determinada.
- Autenticidad. Quien trata los datos, debe quedar identificado.
- Trazabilidad. El sistema al completo debe ser auditable, se debe poder seguir su uso y funcionamiento, para “Trazar” un historial sobre su funcionamiento. Este punto es muy importante, pues es la única manera de detectar fallos, errores, acciones lícitas o ilícitas dentro de un sistema de información automatizado.

⁵³¹ GOBIERNO DE ESPAÑA. PAE PORTAL ADMINISTRACIÓN ELECTRÓNICA, "MAGERIT v.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información."]. [http://administracionelectronica.gob.es/pae Home/pae Documentacion/pae Metodolog/pae Magerit.html#.Vk2nUvkveUk](http://administracionelectronica.gob.es/pae/Home/pae Documentacion/pae Metodolog/pae Magerit.html#.Vk2nUvkveUk) Como una anécdota, la actual ciudad y capital de España, Madrid, se llamaba en los tiempos de Alfonso VI de Castilla, Magerit, en el año 1083. Madrid era sólo una pequeña fortaleza. Fue el principio de la toma de Toledo. Es curiosa esta denominación.

Existen otros conceptos muy afines a la actividad técnica de gestión de sistemas informáticos, como son:

- **Análisis de Riesgos.** Es un proceso para estimar la exposición de un sistema a un determinado nivel de riesgo, entendiendo riesgo como amenaza al sistema informático.
- **Seguridad planificada.** Se establecen objetivos de seguridad y se revisa su cumplimiento. De esta forma, se conoce qué medidas funcionan y cuáles no.
- **Implantación de sistemas de seguridad.** Se llevan a la realidad los métodos y técnicas aprobados, un protocolo a seguir por los usuarios y técnicos que acceden al sistema informatizado. En el Reglamento, en el artículo 88.1, se obliga al responsable del fichero o del tratamiento a la elaboración y mantenimiento actualizado de un Documento de Seguridad en el que se describen las medidas de seguridad técnicas y organizativas para cumplir con este mandato legal.
- **Gestión de la seguridad.** El artículo 88.7 del Reglamento establece la figura del Responsable de Seguridad para sistemas que gestionen datos de nivel medio (veremos los diferentes niveles de seguridad de datos que establece el Reglamento) Se está pensando en empresas de determinada envergadura, pero la realidad, como se verá, ofrece resultados muy diversos.

Existe también una vinculación entre seguridad y prevención. La seguridad se define en la prevención, también en sus definiciones lingüísticas. Se trata de *evitar* que se produzcan daños a las personas titulares de datos personales, pues al lesionar un derecho fundamental vinculado con otros derechos de la persona, los efectos de la acción ilícita y dañosa son en muchos casos irreversibles. La prevención será la herramienta para la protección de datos personales más eficaz⁵³².

⁵³² El Considerando 46 de la Directiva 95/46/CE del 95 lo expresaba con el siguiente texto:

“Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado.”

Será en el diseño del tratamiento de datos cuando la seguridad tenga mayor relevancia y más eficacia posterior, tanto por medidas técnicas como de organización (seguridad en el diseño) Es la llamada visión integradora de la seguridad. Si se tienen en cuenta los requerimientos de seguridad una vez diseñado un sistema de gestión, sólo se van a tener incidencias y contratiempos posteriores. La Disposición Adicional Única⁵³³ del Reglamento establece la obligación de que los programas destinados al tratamiento de datos personales tengan en cuenta el nivel de medidas de seguridad aplicables a dichos datos. Existen en este momento varias iniciativas al respecto. Una de ellas es de la Comisión Europea con la Agenda Digital para Europa (*Digital Agenda for Europe, A Europe 2020 Initiative*) con el programa eTEN, en el que se incluye el programa EuroPriSe (*European Privacy Seal*), una iniciativa (desde Alemania, *Land de Schleswig-Holstein*) para promover una certificación a nivel europeo en materia de protección de datos de carácter personal⁵³⁴. Algunas empresas en el ámbito de la protección de datos personales incluyen esta certificación (la información tiene fechas un tanto lejanas, entre 2007 a 2009). En esta línea de gestión de la seguridad en el tratamiento de datos personales se encuentra la normativa del nuevo RGPD la cual establece que los datos personales deben tener un tratamiento para que se garantice la seguridad y la confidencialidad, además de que debe controlar e impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento, reconociendo que la gestión de accesos a los sistemas informáticos, tanto física como a través de programas es lo más importante. El responsable del tratamiento se convierte en la figura más importante para garantizar la seguridad y para evaluar los posibles

⁵³³ El texto es el siguiente: “Disposición adicional única. Productos de software. Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento.”

⁵³⁴ Los links a sus correspondientes páginas web´s son los siguientes:

<https://ec.europa.eu/digital-agenda/en/news/eten-programme>

<https://www.european-privacy-seal.eu/EPS-en/Home>

<https://www.european-privacy-seal.eu/EPS-en/Europrise-sello-europeo-de-privacidad> Este texto explica el proyecto en español.

riesgos, pues es quien administra los accesos y los datos que van a ser tratados, con qué medios y por quién. Para ser legítimo el tratamiento de datos personales debe realizarse en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, no sólo en su uso cotidiano, sino también deben proveerse los medios para garantizar en mínimos la capacidad de una red o de un sistema de información para resistir consecuencias de accidentes o acciones ilícitas, que sean malintencionadas o que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales almacenados o que sean transmitidos. Se mencionan los sistemas de garantías de seguridad que están en funcionamiento actualmente, denominados certificados, en especial para la gestión de información en las AAPP y los ciudadanos, como son el CERT (para EEUU, *Computer Emergency Response Team*) y el CSIRT (más utilizado en Europa, *Computer Security Incident Response Team*). Estos sistemas y certificados funcionan por cifrado de información, una herramienta que se ha determinado muy eficaz para combatir los ataques y accesos indebidos a sistemas informáticos y a las comunicaciones que siempre les acompañan para su gestión y tratamiento. Las consecuencias de una nula o equivocada gestión de la seguridad produce los efectos indeseados de daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de *la anonimización*, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para los ciudadanos. La *anonimización*, técnica que se había mostrado bastante efectiva, es actualmente cuestionable dentro de los avances en gestión de datos masivos o *big data*, que realiza una nueva identificación y singularización (*linkability*) de los titulares de datos personales a través de datos no relacionados en origen, pero que sí se vuelven a relacionar dentro de los sistemas de análisis. Una técnica también muy extendida es la *inferencia*, por la cual se puede deducir, a nivel de probabilidades, datos personales y la identidad de un individuo a través de valores de otros datos. Se utiliza en estadística y tiene una aplicación extendida en los sistemas de *big data*, con capacidad para encontrar una serie de

coincidencias o correlaciones entre datos, infiriendo después el analista las conclusiones que no pueden detectarse a primera vista.⁵³⁵

En el nuevo RGPD se regula un pequeño procedimiento para el caso de que se haya producido una violación en la seguridad de datos personales, por el cual el responsable, sin dilación y en un máximo de 72 horas desde su conocimiento debe notificar la violación de la seguridad de los datos personales a la Autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida. Algo novedoso es la obligación que tiene el responsable de comunicar a los titulares de datos la violación de seguridad producida, cuando pueda entrañar un alto riesgo para sus derechos y libertades. Con esa notificación se pretende que los ciudadanos cuyos datos están en riesgo de afectar a sus DDFF puedan tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales

⁵³⁵ Véase el estudio de GIL GONZÁLEZ, E., *Big Data, privacidad y protección de datos.*, Madrid, 2016, pág. 83 y ss.. Con cita de HARDY, Quentin, “*Rethinking privacy in an era of big data*”, artículo en el *New York Times* de 4 de julio de 2012: “No queremos el nombre. El nombre es ruido. Hay suficiente información en las enormes bases de datos de Google sobre búsquedas en internet, localización y comportamiento online que se puede saber mucho de una persona de forma indirecta”. Cita de página 101.

continuas o similares. La autoridad de control tomará la decisión de la necesidad de su intervención en función de la naturaleza de la violación en la seguridad⁵³⁶.

9.2. El Instituto Nacional de Ciberseguridad, INCIBE

Desde octubre de 2014, en España, se cuenta con el Instituto Nacional de Ciberseguridad, INCIBE, anterior Instituto Nacional de Tecnologías de la Comunicación (INTECO). El INCIBE es un *instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación*⁵³⁷. El CERT es el Centro de Respuesta de Seguridad e Industria a incidentes de ciberseguridad para *aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, aumentar la ciberresistencia de las organizaciones y el diseño de medidas preventivas para atender a las necesidades de la sociedad en general (...) de apoyo en la investigación y lucha frente a ciberdelitos y ciberterrorismo*.

⁵³⁶ Algunos artículos resaltables que tratan la seguridad de los datos en el RGPD son: Artículo 4.12) Definiciones; Violación de seguridad; artículo 5.1.f), Principios relativos al tratamiento de datos de tal manera que se garantice la seguridad; Artículo 30, Registro de las actividades de tratamiento; Toda la Sección 2 del Capítulo IV, Seguridad de los datos personales, artículos 32 y ss; con relación a la seguridad, la normativa de los artículos 40 y ss, Códigos de conducta y certificación, que se analizarán en otro epígrafe; también se relacionan estas normas de seguridad con aspectos importantes de las transferencias internacionales de datos, artículos 45 y ss, con especial énfasis en el punto 2.a) del artículo 45; La novedad del artículo 47, normas corporativas vinculantes, entre otras menciones a la seguridad de los datos. Se exponen los considerandos 39, 49, 83, 85, 86 y 87.

Véanse también como interesantes las páginas web que explican los sistemas de certificados mencionados.

<https://www.ccn-cert.cni.es/>

<https://www.cert.fnmt.es/>

<https://www.csirt.es/>

⁵³⁷ https://www.incibe.es/que_es_incibe/

El INCIBE tiene como misión *reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general*. Como se observa, se trata de actividades de gran interés desde la perspectiva de la protección de datos personales⁵³⁸.

Para empresas, la página web de INCIBE tiene también otra curiosidad: *el Kit de Concienciación*, un *paquete* (la palabra aparece en la página web comentada) de videos interactivos y presentaciones que exponen varias temáticas en relación a la ciberseguridad. Es una buena herramienta para las empresas, sus empleados, colaboradores y usuarios. Tiene ejemplos ilustrativos y prácticos. No es doctrinal ni jurídica, es más bien seguridad básica, ilustrada en la práctica⁵³⁹.

La iniciativa INCIBE se consideraría un avance en cuanto a la involucración de la Administración en la protección de datos personales y un buen sistema para informar a las empresas en cuanto a la seguridad en la gestión de datos, incluidos los de carácter personal. Una serie de *Guías* son también una base para ir concienciando a las PYMES

⁵³⁸ https://www.incibe.es/que_es_incibe/que_hacemos/ Algunos destinatarios de su actividad son: empresas y profesionales que hacen uso de las TIC. Destaca la red IRIS, que conecta empresas e instituciones de la Administración, para la investigación, entre otros fines. También expertos en ciberseguridad y ciudadanos, a través de la Oficina de Seguridad del Internauta, OSI, un servicio gratuito. Tiene como curiosidad una parte de su página web con el epígrafe *Ponte al día*, llena de casos de intentos de captación de datos personales.

⁵³⁹ Si se tiene interés en la ampliación de esta información se encuentra en https://www.incibe.es/empresas/Kit_de_concienciacion/. Un ejemplo: se propone realizar un experimento. Abandonar un pen drive con información de dudosa procedencia en algún lugar visible de la empresa. Sin ser detectada la vigilancia, se debe estudiar el comportamiento de los que acceden físicamente a las instalaciones. Lo que se debe hacer es notificar a la persona responsable de la existencia del pen drive. Lo que realmente ocurre en una mayoría de casos es que las personas intentan ver el contenido del pen drive en los equipos de la empresa. Y lo peor: muchas veces pueden hacerlo porque las empresas no están preparadas para no permitir la lectura de un dispositivo ajeno a su instalación.

y profesionales sobre este importantísimo aspecto⁵⁴⁰. Un apunte crítico sin minusvalorar el esfuerzo y la iniciativa: algunos profesionales y empresarios no van a entender demasiado⁵⁴¹. En estas ideas se ha obviado la acción y conducta del titular de los datos personales, que en gran medida es el más interesado en la protección de sus datos, en cuanto a su conducta poco previsor, pero, como se va exponiendo en este estudio, también es quien más arriesga en cuanto a su gestión. Al ser el responsable del fichero o del tratamiento el obligado a la protección de datos, se analiza por esta tesis la obligación de un tercero, pero sin olvidar al protegido por la LOPD.

9.3. Anexo orientativo: Aplicación de los niveles de seguridad.

Explicar el entramado del articulado relativo a la seguridad de datos y su aplicación en la práctica excede el objetivo del presente estudio. Se tiene como referencia el cuadro-resumen expuesto en la *Guía de Seguridad* elaborada por la AEPD. La expe-

⁵⁴⁰ Se citan sólo a título de ejemplo: “Catálogo de empresas y soluciones de Ciberseguridad”; “Taxonomía de soluciones de ciberseguridad”; “Como Gestionar una fuga de información. Una Guía de aproximación al empresario”; Gestión de riesgos. Una guía de aproximación para empresario”; “Ciberseguridad en comercio electrónico. Una Guía de aproximación para el empresario”. Están en la dirección web: <https://www.incibe.es/empresas/guias/>

⁵⁴¹ Un ejemplo: la Guía de gestión de riesgos. Para un profesional de formación idiomática sencilla, eso del riesgo sólo lo puede conectar su mente con algo negativo y con algo de seguros; emplear este lenguaje puede ser demoledor: “Activo: cualquier recurso de la empresa necesario para desempeñar actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos. La valoración de los activos es importante para la evaluación de la magnitud del riesgo”. Sencillamente un mecánico de taller coge la carpeta sobre este asunto y se va. Más que nada porque no tiene porqué saberlo para facturar, para *hacer caja*, que es en donde tiene puestos sus cinco sentidos. Esto sirva para el caso de que el usuario habitual sea el empresario o profesional. Si es un empleado de una actividad sencilla, se dormirá (fue un caso real en una empresa de limpiezas que entraba en instalaciones comprometidas por su actividad estratégica) La frase en la mayoría de casos es: dígame lo que tengo que hacer para esto y lo hago. La mayoría no van a querer entender mucho más.

riencia en estos casos es que se debe analizar cada caso individualmente de forma específica y desarrollar una estrategia para que los hábitos de gestión se adecuen al ejercicio efectivo de la seguridad de datos. Se aportan algunos apuntes en forma de anexo, por si es de interés y complementa la normativa analizada.

Siguiendo a la AEPD, la Autoridad en la materia de evaluación en el cumplimiento de la LOPD y su Reglamento hasta este momento, los niveles de seguridad se clasifican por el Reglamento en Básico, Medio y Alto.

La *Guía* de Seguridad de la AEPD, ya referenciada, aporta el siguiente texto que se transcribe:

NIVEL ALTO. Ficheros o tratamientos con datos:

- de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual y respecto de los que no se prevea la posibilidad de adoptar el nivel básico;
- recabados con fines policiales sin consentimiento de las personas afectadas;
- y derivados de actos de violencia de género.

NIVEL MEDIO. Ficheros o tratamientos con datos:

- relativos a la comisión de infracciones administrativas o penales;
- que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia patrimonial y crédito); de Administraciones tributarias, y que se relacionen con el ejercicio de sus potestades tributarias;
- de entidades financieras para las finalidades relacionadas con la prestación de servicios
- financieros;
- de Entidades Gestoras y Servicios Comunes de Seguridad Social, que se relacionen con el ejercicio de sus competencias;
- de mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social; que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de las personas; y de

los operadores de comunicaciones electrónicas, respecto de los datos de tráfico y localización.

NIVEL BÁSICO. Cualquier otro fichero que contenga datos de carácter personal. También aquellos ficheros que contengan datos de ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual, cuando:

- los datos se utilicen con la única finalidad de realizar una transferencia dineraria a entidades de las que los afectados sean asociados o miembros;
- se trate de ficheros o tratamientos no automatizados o sean tratamientos manuales de estos tipos de datos de forma incidental o accesorio, que no guarden relación con la finalidad del fichero;
- y en los ficheros o tratamientos que contengan datos de salud, que se refieran exclusivamente al grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.

En el capítulo I del Título VIII del Reglamento se regulan las disposiciones generales. El capítulo comienza con el artículo 79, el cual reitera el mandato legal para los responsables de ficheros y/o tratamientos, con independencia de cuál sea su sistema de tratamiento (automatizado, en un ordenador o en una página web, por ejemplo; o no automatizado, en papel)

El artículo 80 del Reglamento establece los niveles de seguridad: *Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.*

Es el artículo 81, *Aplicación de los niveles de seguridad*, el que desarrolla este mandato muy extensamente y se puede afirmar que difícil de entender, sobre todo para personas no acostumbradas al vocabulario *jurídico-informático*. Por ello se refleja en este epígrafe el texto de la AEPD, mucho más claro.

En el Capítulo III del Título VIII, denominado *Medidas de seguridad aplicables a ficheros y tratamientos automatizados*, se regulan las medidas de seguridad para soportes

de información automatizados, informáticos. Como referencia, de nuevo, la *Guía* de Seguridad de la AEPD, que elabora un cuadro-esquema como ejemplo del Documento de Seguridad, al que dedica el capítulo II del Título VIII la LOPD, con un solo artículo, el 88 y con una extensión poco entendible. Es en el Documento de Seguridad donde se refleja el tipo de datos, el nivel de seguridad del fichero (bajo, medio o alto) y las medidas que se deben aplicar. El Documento de Seguridad es obligatorio para todos los responsables de ficheros o tratamientos de datos personales. Es un documento interno de la organización, especialmente redactado para cada caso concreto, que debe mantenerse siempre actualizado, con independencia del nivel de seguridad que se aplique. Se resumen sus apartados obligatorios en:

Descripción detallada del ámbito de aplicación del documento de seguridad; se realiza una especificación detallada de los recursos protegidos, junto con medidas, normas, procedimientos, reglas y estándares de seguridad que el responsable del fichero o tratamiento debe realizar y comprobar. Las funciones y obligaciones del personal son muy importantes. Deben estar debidamente adjudicadas a cada trabajador o colaborador, incluso empresas externas de servicios (como puede ser una empresa de mantenimiento y limpieza); todos los trabajadores deben tener un nivel de acceso a los lugares donde se produce el tratamiento y almacenamiento de datos (acceso físico) y también un nivel de acceso con claves determinadas, personales e intransferibles, que permitan la identificación indubitable de la persona que accede al tratamiento de datos, con uso del software y sistemas informatizados (acceso lógico). Ambos, acceso físico y acceso lógico, se complementan en determinadas instalaciones, por ejemplo, con la obligatoriedad de claves de acceso a un lugar físico (sin la clave correcta no se abre la puerta), donde se almacenan soportes en papel, por ejemplo, como puede ser una notaría, o lugares donde se almacenan soportes en plásticos o vinilos, como puede ser un almacén de pruebas radiográficas. La tendencia en estos dos ejemplos es a la eliminación de soportes que no sean digitales, a través de la gestión documental electrónica, en el caso de la notaría, y de las radiografías digitales, para el caso de las clínicas. Se impone la gestión informatizada de datos, al probarse mucho más segura, eficaz y económica. El acceso a estos lugares físicos, donde se

encuentran los grandes servidores de datos, es mucho más controlable en accesos físicos y su seguridad lógica implica que las empresas, como responsables de tratamientos, tengan una visión de gestión más avanzada, como quiere promover el nuevo RGPD, por lo que se requiere en el documento de seguridad establecer una estructura y descripción de los ficheros y sistemas de información; los procedimientos de notificación, gestión y respuesta ante incidencias, además de procedimientos de copias de respaldo y recuperación de datos junto con las importantísimas medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos, siendo este un apartado casi imposible de implementar hasta que se ha tenido una incidencia de seguridad. A partir del nivel medio de medidas de seguridad, además de los apartados anteriores, deberán incluirse los siguientes: la identificación del responsable de seguridad y control periódico del cumplimiento del documento de seguridad, lo que se denomina hasta ahora auditoría de seguridad. También, en el caso de haber contratado la prestación de servicios por terceros para determinados ficheros, en el documento de seguridad se debe hacer constar esta circunstancia, indicando una referencia al contrato y su vigencia, así como los ficheros objeto de este tratamiento. Este punto es sumamente importante para los contratos de servicios fuera del establecimiento del responsable. Si se ha contratado la prestación de servicios en relación con la totalidad de los ficheros y tratamientos de datos del responsable, y dichos servicios se prestan en las instalaciones del encargado del tratamiento se podrá delegar en éste la llevanza del documento de seguridad.

Las medidas de seguridad son obligatorias para algo tan sencillo como una relación de clientes con nombres, apellidos, dirección y teléfono, el DNI, y alguna información más. Algo básico para una actividad. Para ello, el empresario/profesional, sus trabajadores y colaboradores, debe entender qué es esta *básica* relación de conceptos:

- Responsable de seguridad.
- Personal de la empresa que accede a sus instalaciones, tanto de forma física como lógica.
- Incidencias. Control de accesos.
- Identificación y autenticación.

- Gestión de soportes.
- Copias de respaldo
- Criterios de archivo.
- Almacenamiento.
- Custodia de soportes.
- Copia o reproducción.
- Auditoría.
- Telecomunicaciones.
- Traslado de documentación.

Todo ello más acentuado cuando se trata de datos de nivel medio y de nivel alto.

Sinceramente, incluso entre colegas de la profesión jurídica se han tenido problemas de comprensión. Entre profesionales tan cualificados como ingenieros o médicos, existe también mucha confusión⁵⁴².

Los ficheros de titularidad privada registrados en la AEPD, según su Memoria de 2014, son algo más de tres millones y medio que se pueden dividir en una media ventajosa de 3 ficheros por entidad. Por lo que sólo un poco más de un millón de organizaciones

⁵⁴² En un ejemplo recurrente, si un asesor fiscal intenta explicar la Ley General Tributaria y los conceptos contables-fiscales en unos días, pero además el Ministerio de Hacienda nos obliga a presentar nuestras obligaciones fiscales en unos modelos creados por cada uno de nosotros, porque debemos identificar nuestras propias obligaciones tributarias por nosotros mismos y si ocurre alguna falta o delito fiscal, es nuestra la responsabilidad como ciudadanos, se tendrían graves problemas para cumplir con tales obligaciones administrativas. Además, la realidad social no se ha concienciado de la importancia de la seguridad de los datos. Por eso, la LOPD, en muchos casos, ni se conoce, ni se quiere conocer, ni se cumple adecuadamente en su núcleo más importante: la seguridad de los datos personales. La prueba son las cifras. El INE, con datos de 2011, expone que en ese año había en España 3,25 millones de empresas. Predominan las de pequeño tamaño o sin asalariados, dedicándose en su mayor parte a actividades de servicios. Más de la mitad son personas físicas (52,5%). Debido al peso de las Pymes, el número de empresas en España es de los más altos de la Unión Europea, donde predominan las empresas entre 1 y 9 ocupados (microempresas). Estas empresas suponían en 2008 el 92,0% del total (excluidos servicios públicos, financieros y agricultura), cifra que en España se situaba en el 93,1%.

privadas tienen ficheros inscritos, lo que indica que muy pocas organizaciones cumplieron la LOPD, pues esta obligación de inscripción de ficheros era, hasta el nuevo RGPD, primordial para su cumplimiento⁵⁴³. Dentro de la denominación *organizaciones* cabe decir que existe una amplia tipología de actividades, no sólo son empresas mercantiles, sino que se podrían ampliar a comunidades de propietarios, asociaciones, o casos de gestión no empresarial.

El artículo 44.3.h) LOPD estableció que es infracción grave mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen. La AEPD y la AN consideraron en su doctrina hasta este momento que el responsable del fichero/tratamiento de datos personales tiene una obligación de resultado con especial diligencia que consiste en el cumplimiento de las medidas de seguridad para que sean eficaces; no basta con que se adopten medidas de seguridad, éstas deben ser eficaces para el objetivo perseguido, el cual consiste en evitar que los datos personales sufran cualquier tipo de alteración, pérdida o incluso acceso por parte de terceros sin legitimidad para su tratamiento o visionado⁵⁴⁴. ”

⁵⁴³

Véase

http://www.agpd.es/portaIwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/Memoria_AEPD_2014.pdf

⁵⁴⁴ La AEPD tiene Resoluciones en las que cita la SAN 4898/2008, de 11 de diciembre de 2008, FJ 4, con la siguiente doctrina: “como ha dicho esta Sala en múltiples sentencias (...) se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros (...) la recurrente es, por disposición legal, una deudora de seguridad en materia de datos y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues también es responsable de que las mismas se cumplan y se ejecutan con rigor”. Similar doctrina se encuentra en la SAN 5138/2008, de 11 de diciembre; el caso se centra en una entidad crediticia que vertió en la basura una cantidad significativa de papel (en su mayoría fotocopias) con datos de carácter personal sin destruir. Como ejemplo de resolución de la AEPD véase en http://www.agpd.es/portaIwebAGPD/resoluciones/procedimiento_apercibimiento/procedimiento_apercibimiento_2014/common/pdfs/A-00223-2013_Resolucion-de-fecha-24-01-2014_Art-ii-culo-9-LOPD.pdf

10. El Deber de Secreto.

El deber de secreto se vincula a la protección de datos personales, concretamente el artículo 10 LOPD establece que *el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo*⁵⁴⁵.

La obligación de secreto respecto a la información que se vaya a tratar o conocer se extiende por multitud de regulaciones y ámbitos jurídicos y profesionales. Para la protección de datos de carácter personal es uno de sus principios fundamentales. Se puede marcar una diferencia respecto a otros principios de la protección de datos personales y este de deber de secreto: las consecuencias jurídicas son diferentes cuando se vulnera. En primer lugar, por sus consecuencias, de casi imposible previsión. En segundo lugar, porque puede llegar a ser un delito al que siguen acciones penales.

Durante muchos años, han ido apareciendo noticias en la prensa sobre vulneraciones de la LOPD, pero en especial, del deber de secreto, como es en casos de abandono en basureros o contenedores públicos de basura de documentación con datos personales unidos a resultados judiciales, analítica médica, filiación sindical, demandas de empleo, currículum vitae, Registros de diversas provincias (Mercantiles, de la Propiedad e incluso Civiles), copias de DNI. Los descuidos, la falta de importancia para este tipo de informaciones que le daba el personal habitual encargado de desalojar estanterías y cajones con cantidad de documentación en papel, llamaron la atención porque el soporte donde estaban estos datos era visible a simple vista, no necesitaba una máquina para su visionado. Se debe pensar cuál no debe ser de alta la cifra de casos en que este tipo de información se vulneró en su seguridad y en su deber de secreto, extrayendo copias de servidores de clínicas privadas con expedientes médicos, por

⁵⁴⁵ Este artículo de la ley española desarrolla el mandato de la Directiva 95/46/CE en su artículo 16.

ejemplo, pero también existió esa misma vulneración en las AAPP, para enviar, como ocurría en muchos casos, información sobre servicios o productos a personas que habían estado en alguna base de datos, que teóricamente, era confidencial. Con una mayor conciencia de la ciudadanía se ha llegado en 2017 a una situación mejorada respecto al deber de secreto, pues las empresas y profesionales se conciencian de la importancia y trascendencia de estos asuntos comentados, aunque se siguen realizando este tipo de actividades ilegítimas, lo único que son mucho más discretas y más cerradas en cuanto a la accesibilidad de los vulneradores. El responsable del fichero o del tratamiento debe también exigir a sus colaboradores de todo tipo el deber de secreto, con el consiguiente apercibimiento en caso de su vulneración. Tanto en el ámbito de la actividad privada como pública. Esto se concreta jurídicamente en las llamadas *cláusulas de deber de secreto* que deben acompañar a cualquier contrato, privado o público, laboral o funcional, e incluso entre empresas o entre empresas y AAPP.

La obligación de secreto no es absoluta. La propia LOPD matiza en su artículo 11 los casos excepcionales en el epígrafe *Comunicación de datos*. El fin legítimo de la comunicación es el resumen de este amplio artículo de la LOPD. Este fin legítimo puede basarse en un imperativo legal o judicial, o en situaciones en las que el afectado debe comunicar sus datos para proteger un bien o una persona en relación con su situación.

El Código Penal dedica el Título X a los Delitos contra la Intimidad, el Derecho a la propia Imagen y la inviolabilidad del domicilio. En el Capítulo I del Título X se encuentran los artículos 197 y ss. CP. que penalizan conductas en relación con la vulneración del deber de secreto⁵⁴⁶.

El artículo 10 LOPD ordena que el deber de secreto sobre los datos personales se mantiene incluso después de terminada la relación con el responsable del fichero o trata-

⁵⁴⁶ Se apunta la dirección web del BOE a fecha de noviembre 2015. Este es el texto que ha servido de referencia. <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444> Se editaba en esta versión la actualización del texto realizada el 31 de marzo de 2015 en vigor desde el 07 de julio de 2015.

miento. El incumplimiento de esta obligación es una infracción grave según el artículo 44.3 de la LOPD.

El nuevo RGPD regula el deber de secreto en el artículo 90, *obligaciones de secreto*-remitiendo a la legislación de cada Estado miembro al respecto, con la condición de informar a la Comisión sobre las normas adoptadas y cualquier modificación sobre las mismas.

11. La Cesión de Datos: Comunicación de Datos personales con consentimiento previo del Interesado.

El artículo 11 LOPD en un texto sumamente extenso (de nuevo); describe cuáles son los casos de comunicación de datos con el consentimiento previo del titular o interesado. Es lo que se denomina también cesión de datos. En las definiciones del artículo 3, punto i), la cesión de datos se conceptúa como *toda revelación de datos realizada a persona distinta del interesado*.

La cesión de datos personales está relacionada con la violación del deber de secreto, pero son conceptos muy diferentes. En la cesión de datos, el responsable del fichero o tratamiento decide con plena voluntad transmitir datos personales a un tercero, que los puede tratar ampliamente por recogida, grabación, conservación interconexión o transferencia. La simple posibilidad de tratamiento es ya una cesión. En la violación de deber de secreto existe una revelación de datos que puede ejecutar cualquier otra persona que no es el responsable del fichero o tratamiento. La cesión puede ser en muchos casos legítima y/u obligada por imperativo legal, en la violación del deber de secreto existe siempre una voluntad ilegítima de tratamiento de datos. La cesión es un tipo de tratamiento de los datos personales, como se define en el artículo 3 c) LOPD al definir el tratamiento de datos personales como *cesiones de datos personales que resulten de comunicaciones, consultas, interconexiones y transferencias*. En la cesión, el tratamiento de datos consiste en la revelación de información personal a un

tercero, pero con autorización del titular de los datos o por mandato legal, en situaciones excepcionales⁵⁴⁷.

En las AAPP las cesiones de datos están organizadas e incluso legitimadas por su propia naturaleza legal⁵⁴⁸. Sin esa interconexión administrativa sería imposible la Administración Pública actual, los servicios, derechos y obligaciones que gestiona, la eficiencia de gestión pública evitando duplicidades, por ejemplo. En el ámbito privado, la cuestión es mucho más complicada en cuanto a aspectos de consentimiento del titular. El texto del artículo 11 LOPD establece que los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado⁵⁴⁹. Esta norma general de consenti-

⁵⁴⁷ TRONCOSO REIGADA, ANTONIO; "Comentario al artículo 11. La comunicación de datos personales. El concepto de cesión.", *Comentario a la Ley de Protección de Datos de Carácter Personal*, Madrid, 2010. El autor se centra especialmente en un análisis sobre la cesión de datos personales, relacionándolos con el derecho fundamental a la protección de datos. Para este autor, "la protección de datos personales no protege los datos personales a toda costa, sino sólo frente a los tratamientos. Si no hay tratamiento, no hay derecho fundamental a la protección de datos, aunque puede haber un derecho a la intimidad." "El derecho fundamental protege las libertades y los derechos fundamentales frente a los tratamientos de datos personales" (...) "el riesgo no es que haya datos, sino que existan tratamientos de datos personales" (...) "es necesario que los datos de carácter personal se hallen registrados en un soporte físico que los haga susceptibles de tratamiento."

⁵⁴⁸ El artículo 21 LOPD regula la comunicación de datos entre AAPP. Se recuerda que esta tesis se centra en la práctica empresarial y ciudadana; por tanto, el tema público no forma parte de su análisis. Se nombra como comentario. Se apunta el tema de interconexión de bases de datos, asunto diferente a la cesión de datos entre AAPP. La interconexión de bases de datos puede dar lugar a múltiples problemas en cuanto a tratamiento de datos personales, pues se injiere directamente sobre información muy amplia que puede dar lugar a información conductual, mucho más amplia que la información personal, con simples datos necesarios para la Administración. Aquí, los criterios de ponderación y necesidad son importantísimos. Se debe buscar siempre la medida más moderada de intromisión para "alcanzar la finalidad con la misma eficacia"- TRONCOSO REIGADA, obra mencionada, página 991-

⁵⁴⁹ La LOPD incorpora el texto de la Directiva 95/46/CE respecto a la cesión de datos, la cual, en su considerando 28 establece que "los objetivos de los tratamientos posteriores no pueden ser incompati-

miento del titular previo a la cesión tiene las siguientes excepciones: cuando la cesión está autorizada en una ley; cuando se trate de datos recogidos de fuentes accesibles al público, cuyo consentimiento del titular se solicita a posteriori, como se ha mostrado en este texto; cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros, teniendo en cuenta que la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique, como puede ser que dicha comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. Tampoco será necesaria la autorización del titular de los datos a la cesión que se produzca entre AAPP para fines históricos, estadísticos y científicos. Otro caso de cesión, ya comentado es el que se realiza por razones de urgencia en la salud del interesado u otra persona legitimada, o en situaciones de alerta sanitaria o estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Al solicitar el consentimiento del titular se debe expresar la finalidad por la que se quiere realizar la cesión y a la que se destinarán los datos, además de señalar la actividad del cesionario (receptor de los datos). Si no es así, el consentimiento y, por tanto, la cesión, se consideran por el artículo 11 LOPD nulos. El consentimiento para la cesión de datos es siempre revocable. Todas estas pautas pueden resumirse en dos aspectos: *la finalidad legítima o directamente relacionada con la actividad y el previo consentimiento del interesado*. Las excepciones se sitúan bajo un estricto mandato legal o en la urgencia para protección o gestión de un bien mayor relacionado con el titular.

bles con los objetivos originariamente especificados". La cesión no puede tener finalidades incompatibles con las que permitieron la recabación y tratamiento de los datos aportados por el titular.

La LOPD recomienda procedimientos de disociación (anonimización) para que no se produzca la obligatoriedad de aplicación de la normativa de protección de datos personales. Este punto es sumamente importante y práctico, pues muchas veces para los fines que necesita una empresa los datos personales son innecesarios en su original fichero⁵⁵⁰.

En la práctica profesional, la cesión de datos suele generar gran confusión para los responsables de ficheros o de tratamiento. Entre otras razones, porque existe para el empresario/profesional una serie de obligaciones legales en las que dicha cesión es un imperativo legal fuera de su gestión mercantil-empresarial. Esto sucede, por ejemplo, en relación a las retenciones fiscales de las nóminas que deben realizar las empresas; las obligaciones de Seguridad Social, por las que la empresa debe recabar una serie de datos personales de su empleado y de toda su unidad familiar, datos clínicos, por ejemplo, muchas veces sin relación con su actividad mercantil. Obligatoriamente el empresario debe recabar y gestionar datos para aseguradoras diversas en función de su actividad. Otro caso de cesión puede ser también la gestión de cuotas sindicales, que se detrae de la nómina del empleado y se ingresa en la cuenta del sindicato a petición del empleado. La empresa, en resumen, adquiere la condición de responsa-

⁵⁵⁰ Un ejemplo: la cesión de datos de venta de vehículos por un concesionario a su marca de referencia, para finalidades relacionadas con estudios de estadística de ventas, marketing, publicidad, procedimientos o cualquier otra relacionada con la mejor gestión de la empresa. Si se desea una publicidad personalizada a cada individuo interesado, sí son necesarios multitud de datos personales. Pero sólo las personas que hayan otorgado su consentimiento para esa finalidad y deseen recibir publicidad de la marca deben recibirla. De todos modos, el concesionario necesita datos personales para cumplir con sus obligaciones ante las AAPP (por ejemplo, matriculación del nuevo vehículo). Una buena parte de datos sí se puede seguir tratando y cediendo sin problemas, al estar suficientemente anonimizados, por ejemplo, edad de los compradores, estado civil, profesión, etc., pero nunca en relación con nombre, apellido, dirección, número de teléfono, matrícula del coche adquirido, o cualquier otro dato que pueda identificar al titular de los datos. La disociación permite una cesión de datos sin que sean datos personales, pues sólo lo serán aquellos datos que permitan la identificación de la persona titular o la haga identificable. En el Reglamento de la LOPD, en su artículo 10, se definen algo más los supuestos de cesión o comunicación de datos para su tratamiento. Es muy extenso también y no aporta novedades, salvo una descripción más pormenorizada.

ble de ficheros y de tratamientos de datos personales que muchas veces nada tienen que ver con la actividad mercantil y sí son obligaciones legales o de actividades colaterales. Estas cesiones, comunicaciones de datos personales a un tercero, son realmente un auténtico quebradero de cabeza para las empresas y generan multitud de conflictos⁵⁵¹.

¿Puede una empresa ceder datos a terceros? No, en principio. Es necesario el consentimiento informado y expreso del titular de los datos para la cesión, en cualquier caso, sobre todo para actividades de marketing y publicidad, que excedan de la relación contractual mercantil que une a un particular con una empresa. Los datos son cada día más valiosos y las empresas proceden a su cesión, por no afirmar que en la mayo-

⁵⁵¹ Un ejemplo reciente: por razones de seguridad, una instalación portuaria exigió a las empresas colaboradoras que los trabajadores fueran identificados para acceder a sus instalaciones por lectura biométrica que se archivaba en sus servidores. Como se dijo en otro epígrafe, la lectura biométrica es la identificación de la persona por el reconocimiento de una característica física única en cada individuo, como puede ser la huella digital, el iris ocular o los rasgos de la cara. La última versión puede también reconocer conductas y comportamientos, olor corporal, ADN, formas de las orejas, de las palmas de las manos, de las venas faciales o de otras zonas corporales. Estos sistemas son automatizados. Los sistemas de acceso a instalaciones que no son biométricos pueden ser olvidados (claves de seguridad, por ejemplo) o perdidos (tarjeta identificativa) cuando no sustraídos o duplicados, en cualquier caso. La biometría es muy segura y muy rápida, por eso se extiende en su aplicación. En el ejemplo que se describe, los trabajadores de una empresa contratada por el titular de las instalaciones se negaron a que sus datos personales, en este caso, biométricos, fueran recabados, cedidos y/o tratados, no ya por la empresa contratante, sino por cualquier otra. ¿Qué hacer en estos casos? El caso fue complicado y se solucionó al margen de la AEPD, con un acuerdo con los trabajadores explicando que era necesario para el mantenimiento de la actividad y los puestos de trabajo. Con garantías adicionales de seguridad, los trabajadores accedieron a que sus datos fueran cedidos.

Otro ejemplo: una empresa cede datos de *curriculums* de sus empleados a empresas subcontratantes, sin que los titulares tengan conocimiento de ello o sin consentimiento expreso. Uno de los trabajadores se negó a ello, ya que no figuraba en su contrato de trabajo la necesidad de dicha cesión. La empresa tuvo que despedir al trabajador con una importante indemnización acordada para compensarle, pues no podía ejercer su actividad mercantil sin la cesión de los datos de los *curriculums* de sus trabajadores.

ría de los casos se *vende* esa información personal para gestión de perfiles de consumo y usuarios⁵⁵².

Existe otro caso también llamativo: el descontrol de cesión de datos de las llamadas redes sociales. En este caso, ya comentado, es por falta de información (voluntaria o involuntaria) del titular de los datos, que promueve con su acción la cesión de datos personales entre toda una inmensa red de usuarios. Es evidente, tanto en la realidad como por reconocimiento de la doctrina, que este tratamiento excede de la esfera familiar y privada, no pudiendo ser calificado como doméstico⁵⁵³. En la mayoría de casos, los usuarios de redes sociales no obtienen el consentimiento informado de otros particulares para publicar datos, en especial, imágenes. Sin embargo, hasta ahora, solamente se han activado canales de denuncia, no de prevención. Es decir, cuando se actúa para proteger datos personales que se exhiben en una red social, es cuando ya se ha producido el daño y la cesión de esos datos es prácticamente intrazable⁵⁵⁴. La denuncia y retirada *a posteriori* no es suficiente para la protección del de-

⁵⁵² Por ejemplo, una empresa de seguros de automóvil solicita el consentimiento de cesión de datos personales para fines casi infinitos: publicidad sin determinar qué empresa es la destinataria, ni tan siquiera qué sector de actividad, estudios de opinión o estadísticos sin especificar su desconexión con el titular de los datos, análisis de perfiles en general para poder ofrecer multitud de productos en función del análisis obtenido, por cualquier medio. Sería legítimo, por ejemplo, el envío de información de esa empresa al titular de datos con el que ha contratado y sólo de su actividad, no de otra. O el uso de los datos del titular para fines estadísticos de la propia empresa contratante, rompiendo entonces la posible cuestión de cesión de datos personales si se desvinculan del titular, haciéndole inidentificable, como en el ejemplo comentado.

⁵⁵³ TRONCOSO REIGADA, Véase obra citada, página 963. El autor cita el Dictamen 5/2009 del Grupo de Trabajo sobre Protección de datos del artículo 29 sobre redes sociales en línea. Cita el caso Lindqvist del TJCU del 2003, y al autor PÉREZ LUÑO. Para este autor se hace necesario el consentimiento informado de los titulares de los datos personales para la cesión pues “esta publicación de datos incluidos en un perfil es una cesión indiscriminada de datos de terceras personas lo que obliga al usuario de la red social a asumir la responsabilidad del tratamiento de los datos y fotografías que aparecen publicadas en el perfil”.

⁵⁵⁴ Se recuerda el caso de las fotos poco edificantes o indiscretas. Si bien es cierto que el titular tiene la opción de denunciar para que se proceda a la retirada de sus datos de la red social, estos ya se han extendido por la red, con las consecuencias ilimitadas descritas.

recho fundamental a la protección de datos, pues como se viene exponiendo, se deben realizar una serie de acciones preventivas y de control. Se entra, en otro caso, en la paradoja ya expuesta: las empresas, profesionales y organizaciones se ven obligadas a mantener unas severas medidas de seguridad y unos protocolos de gestión de datos que después otros (los particulares, ciudadanos expuestos a su vez y a los que se trata de proteger) no contemplan ni están obligados a realizar⁵⁵⁵.

Se plantea otra cuestión importante para este mismo momento y es la posible consideración de la cesión de datos personales como una transferencia internacional de datos (recordemos, TID) en el caso de estar expuestos en diferentes redes sociales de ámbito mundial (por ejemplo, *Facebook* o la red profesional *Linkedin*) o sin usar una base de red social, la propia página web de cualquier empresa en la que sus trabajadores se muestran en internet, para todo el mundo que lo quiera consultar. Lo que promete muchas posibilidades, también puede ser objeto de conductas ilícitas o al menos, desagradables. Se está limitando esta exposición, precisamente por las consecuencias no siempre afortunadas, al menos en cuanto a la exposición de imágenes, que siempre es una fuente de información mayor.

El nuevo RGPD y su futuro desarrollo deberá aportar novedades a la cesión de datos personales y a la prevención sobre las actitudes que violen los DDFF.

12. El control de Acceso a los Datos Personales por cuenta de Terceros.

⁵⁵⁵ Sobre la cuestión, se recuerda que el artículo 44.4. k) LOPD consideró infracción grave la comunicación o cesión de datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave. La consideración como infracción muy grave tendría lugar cuando se llevase a cabo una transferencia internacional de datos a países que no proporcionan un nivel de protección adecuado sin la autorización del Director de la Agencia Española de Protección de Datos (artículo 44.4.d) LOPD)
https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/tratamiento_cesion/cesion/index-ides-idphp.php a 03 de diciembre 2015.

El artículo 12 LOPD reguló otro caso especial de tratamiento de datos personales: el tratamiento que se produce por un tercero que accede a los datos de un responsable de fichero o tratamiento en función de la prestación de un servicio contratado. Es el caso del Encargado de Tratamiento⁵⁵⁶. En este caso, no existe nunca cesión o comunicación de datos. Si no fuera así, se estaría en presencia de una cesión no autorizada y respondería de las infracciones correspondientes, como indica el artículo 12.5 LOPD⁵⁵⁷. El encargado del tratamiento sólo trataría los datos por cuenta de un tercero, pero no sería responsable de los mismos, ni del Fichero correspondiente, ni de las instalaciones, ni de las obligadas medidas de seguridad. Trata los datos bajo las instrucciones del responsable del fichero o tratamiento. El Reglamento de la LOPD define esta figura en el artículo 5. I)⁵⁵⁸. La necesidad de una relación contractual refleja-

⁵⁵⁶ El texto del artículo es el siguiente:

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.
2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con el fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

⁵⁵⁷ Este artículo tuvo su origen en el texto del artículo 17 de la Directiva 95/46/CE.

⁵⁵⁸ Artículo 5.I del Reglamento: Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la presta-

da por escrito entre responsable del fichero o tratamiento y encargado de tratamiento sería una garantía para que no se produzca una comunicación de datos no autorizada por el titular. Otra cuestión a destacar en la práctica sería la confusión entre cesión de datos y encargado de tratamiento, la cual está muy extendida, por no afirmar que muchas veces ambas figuras se *cruzan* o aparecen difusas.

La AEPD no consideró encargado de tratamiento a los trabajadores de una empresa con acceso y tratamiento a datos personales. Como resumen de las condiciones que la AEPD consideró apropiadas en la relación con el encargado del tratamiento se aporta el Informe Jurídico 0457/2008. En él se podría apreciar que lo más importante es el cumplimiento y seguimiento de las medidas de seguridad y la inclusión de la existencia del encargado del tratamiento en el documento de seguridad de la empresa.

El artículo 20 y siguientes del Reglamento vincularon al responsable del fichero o tratamiento con las actividades del encargado del tratamiento, detallando aspectos de su relación. Destaca de nuevo la transferencia internacional de datos personales, que se regirá por los artículos correspondientes, no estando el responsable del fichero exento de responsabilidad sobre este aspecto y necesitando siempre el consentimiento del interesado.

13. Los Derechos de las Personas en la LOPD.

Los principios de la protección de datos personales del Título II LOPD se concretaron en el desarrollo de los denominados derechos de las personas del Título III, que consistió en una relación de *instrumentos jurídicos* para la defensa de los datos personales afectados de un titular. De esta forma, los principios se convierten en hechos, se hacen efectivos, para que no queden solamente en enunciados normativos. Estos derechos serían posibilidades a disposición del titular de los datos personales para ejer-

ción de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

cer un control sobre sus datos⁵⁵⁹. Las facultades o derechos del titular de datos personales configuraron, según parte de la doctrina, el denominado *habeas data*⁵⁶⁰. Aunque los derechos de las personas se ampliaron también a las facultades del titular sobre sus datos que se han expuesto al analizar el Título II de la LOPD, como, por ejemplo, otorgar o no otorgar consentimiento para el tratamiento de datos después de recibir información sobre su recabación, aquí, en el Título III se tuvo una concreción mayor en cuanto a acciones para el caso de que los datos fueran tratados vulnerando el *habeas data*. Son los llamados derechos ARCO, acrónimo de acceso, rectificación, cancelación y oposición. A ellos se debe añadir el derecho a la impugnación de valoraciones, no tan nombrado como los anteriores, pero también recogido en la LOPD. Fue el Reglamento la norma que nombró los cuatro derechos ARCO dentro del Título III. La LOPD tuvo en este sentido lagunas legislativas. El procedimiento para el ejercicio de estos derechos se nombró escuetamente en el artículo 17 LOPD, el cual se remitió al Reglamento, que dedicó los artículos 23 al 26 a este tema procedimental. Toco ello conformó el contenido del derecho a la protección de datos personales. Estos derechos de las personas en cuanto a sus datos personales y su ejercicio, además de su propia denominación o ampliación, se encuentran en este momento pendientes de revisión por la Autoridad de control española, al igual que toda la normativa de protección de datos.

13.1. Derecho a la Impugnación de valoraciones respecto a la personalidad del afectado.

⁵⁵⁹ Son el *haz de facultades* del titular de los datos reconocido por el TC en el año 2000.

⁵⁶⁰ PÉREZ LUÑO, A., "Del Habeas Corpus al Habeas Data", *Informática y Derecho*, nº , 1992. El profesor PÉREZ LUÑO lo trató en varias obras; esta vez se toma como referente la que se puede considerar la primera mención del año 1992, con la siguiente definición de *habeas data*: "La facultad de las personas de conocer y controlar las informaciones que les conciernen procesadas en bancos de datos informatizados" considerando este autor que el *habeas data* es un "cauce procesal para salvaguardar la libertad de la persona en la esfera informática."

Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física se considera por el artículo 4.4 del nuevo RGPD como elaboración de perfiles⁵⁶¹. Anteriormente a esta norma, el artículo 13 LOPD reconoció un aspecto del derecho fundamental a la protección de datos personales que es sumamente importante en sus resultados. Es el derecho de los ciudadanos a no verse sometidos a una decisión con efectos jurídicos, o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad, tanto en una vertiente privada como en actos administrativos. En caso de producirse, el afectado tiene derecho a impugnar dichos actos o decisiones basados en datos personales y también tiene derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. Los perfiles en los que se fundamenta una valoración de comportamiento humano, sólo puede ser prueba en un procedimiento a petición del interesado o titular de los datos personales.

A pesar de que el artículo 13 LOPD no se trató con suficiente amplitud por la AEPD, en la actualidad tiene mucha relevancia. Con el avance tecnológico, cada día es más fácil y probable obtener, utilizar, tratar, comunicar y centralizar datos que generen un perfil personal y de conducta. Que de estos perfiles se forman también decisiones con implicaciones en su vida, su libertad y sus posibilidades, es una cuestión abierta y obvia, en una sociedad prácticamente expuesta en esa *casa de cristal* que mencionaba MURILLO DE LA CUEVA; que, además, esas decisiones pueden ser perjudiciales, se deduce de la realidad. Los ficheros automatizados se crean con esas funciones, entre otras, para sectores tan estratégicos como banca, seguros, consumo, ocio o teleco-

⁵⁶¹ El RGPD mantiene posiciones y regula cuestiones sobre los perfiles personales en los Considerandos 30, 38, 60, 63, 70, 71 (el cual aporta una definición), 72, 73, 75, y 91.

municaciones. En el plano de las AAPP, esa información juega cada vez más un papel determinante. No se quiere decir que no exista este tratamiento de datos personales cuando sea beneficioso para el titular o para la sociedad, por ejemplo, para el tratamiento efectivo de enfermedades o reconocimiento y gestión de servicios sociales. Se trata de poder delimitar los posibles efectos negativos que existen tantas veces en actividades humanas, que no pueden excluirse para poder disfrutar de los efectos positivos.

la naturaleza jurídica del derecho a la impugnación de valoraciones puede ser enmarcada en el hecho de que se trata de un derecho basado en el objeto de impugnación, la decisión basada en un tratamiento de datos, no el tratamiento en sí mismo. Un caso frecuente y real son las evaluaciones de personal por agencias o empresas de recursos humanos, bien para proveer de personal a las empresas clientes, bien para buscar al candidato más apropiado para una posición determinada, desde niveles básicos hasta directivos⁵⁶². Si bien es cierto que cierta subjetividad existe en toda decisión, en especial en el ámbito empresarial, tanto de valoraciones correspondientes al ámbito privado de una persona, como de actividades más públicas y no por ello menos relevantes, como puede ser el desarrollo profesional, llegar a analizar características personales por tratamiento informático de datos, es cada vez más frecuente y sus

⁵⁶² LÓPEZ DEL MORAL ECHEVARRÍA, JOSÉ LUIS; "Comentario al artículo 13 LOPD; Impugnación de valoraciones", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, 2010, pág. 1131. En un asunto tratado por la autoría de esta tesis, una empresa de mediano nivel se vio afectada por la posible denuncia ante la AEPD de un empleado por realizar una valoración de su perfil personal, encargada a una empresa de recursos humanos, que llegó a un análisis psicológico y de personalidad muy íntimo, específico, con resultados por escrito que rozaban lo absurdo. No se sabe para qué quería tratar la empresa este tipo de datos personales y de valoraciones, que muchas veces son deducciones basadas en complejos sistemas psicoanalíticos, más cerca de la suposición que de la realidad. En cualquier caso, hubo problemas entre el titular de los datos y el directivo que había encargado el análisis, que dejó encima de una mesa, sin mucho cuidado, expuesto a cualquier lectura de compañeros o de personal externo a la actividad (limpieza y mantenimiento, por ejemplo) No se llegó a realizar una decisión, al menos en ese espacio de tiempo, sobre el empleado en sí mismo, que le afectara jurídicamente o a sus intereses personales.

consecuencias son impredecibles con los nuevos sistemas denominados *big data*. Todo ello no va a legitimar un uso indebido del tratamiento de informaciones personales.

Este derecho de los titulares a impugnar valoraciones no ofrece excesivas Resoluciones. No es un signo de que no haya sufrido infracciones, sino más bien que este derecho de los titulares no se sustancia en denuncias; puede ser por la dificultad de prueba de su vulneración, también puede ser que se solucione entre las partes, pues generalmente existe mayor interés en continuar la relación que en la denuncia ante la AEPD; si es el caso de personas ajenas, sin relación, muy posiblemente el interesado ni se llega a enterar de que la decisión, por ejemplo, bancaria, se ha basado en un tratamiento de datos personales sobre su solvencia y personalidad. El artículo 13.4 LOPD aportó una garantía adicional al titular de los datos: la prohibición de que las valoraciones personales sean prueba en contra del titular en un procedimiento administrativo o jurisdiccional. Dentro de la LOPD no existía tampoco una tipificación infractora, por lo cual difícilmente se puede impugnar y su eficacia fue limitada. En este caso, se ignoró (por no decir, se incumplió) el mandato de la Directiva 95/46/CE, pues en su artículo 22 ordenó que se provea por los Estados miembros suficientes recursos judiciales para proteger y reconocer los derechos dispuestos en la legislación nacional. El nuevo RGPD considera que las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de *cookies* u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas. Por ello se deberá informar al interesado (titular de los datos o su representante legal de la existencia de elaboración de perfiles y de las consecuencias de dicha elaboración. Se extienden estas consideraciones a lo largo de todo el texto de la norma, incidiendo en el derecho de oposición del titular de los datos a tratamientos que impliquen elaboración de perfiles, que por lógica se tratan para realizar valoraciones. Se regulan especialmente los

programas para la elaboración de perfiles de menores de edad o personas vulnerables y los tratamientos de datos masivos con un gran número de afectados.

Se ha comentado en otro apartado que el nuevo RGPD no exige la obligación de inscripción de ficheros ante las Autoridades de control (Considerando 89) pero sí precisa que es necesario realizar lo que denomina evaluaciones de impacto o de riesgo para los datos personales cuando se realizan grandes tratamientos masivos de datos que implique la generación de perfiles y/o que afecten a las categorías especiales de datos (datos especialmente protegidos, como se ha tratado en este texto), biometría o datos dentro de la normativa penal o penitenciaria, entre otras situaciones. Se requiere por la nueva normativa una evaluación de impacto relativa a la protección de datos para el control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos o para cualquier otro tipo de operación cuando la autoridad de control competente considere que el tratamiento entrañe probablemente un alto riesgo para los derechos y libertades de los interesados, en particular porque impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato, o porque se efectúe sistemáticamente a gran escala ⁵⁶³. Se debe limitar el uso de sistemas automatizados para la generación de perfiles personales en los que se basen decisiones que afecten a titulares de datos personales con la elaboración de normas claras que limiten este tipo de decisiones para el acceso a servicios y derechos, como puede ser un préstamo bancario, un seguro médico o un empleo, no excluyendo la intervención humana y otorgando unos derechos efectivos para impugnar las valoraciones basadas en *algoritmos* que permiten la categorización de las per-

⁵⁶³ Véase considerandos 30, 60, 70, 71, 72, 75, 91; Artículos 14.2. f) y g); 15.1. h); 21.1 y 2; 22.1; 35.3. a); 47.2. e), entre otros del nuevo RGPD. La normativa europea otorga importancia a la elaboración de perfiles personales por sistemas automatizados de tratamiento de datos personales, en respuesta, muy probablemente, a los tratamientos masivos de datos realizados en años anteriores por grandes corporaciones y gobiernos, y por su facilidad de expansión actual a través de los sistemas de análisis masivos o *big data*.

sonas sobre datos observables infiriendo otros datos que no se observan a simple vista, lo que tradicionalmente se ha denominado discriminación.⁵⁶⁴

13.1.1 La conducta penitenciaria.

Se destaca la importancia de la Administración Penitenciaria y el Fichero (de carácter público) de Internos de Especial Seguimiento (FIES), modificado como consecuencia de la STS 2555/2009, de 17 de marzo⁵⁶⁵. Este asunto sí fue objeto de Resoluciones de la AEPD y de Sentencias significativas, pues su ámbito roza el orden público y la Seguridad Nacional, aunque se centre en la información de reclusos que pudieran considerarse problemáticos y en ciudadanos que se relacionan con los reclusos por diferentes motivos, forman parte de su entorno, pero no tienen conductas delictivas⁵⁶⁶. El FIES, objeto de controversia, sigue siendo utilizado por las Instituciones Penitenciarias y por el Ministerio del Interior. No solamente contiene datos de reclusos, como se ha dicho, también de todas las personas que pertenecen a sus círculos de relaciones, tanto familiares como de amistades o de relación de cualquier procedencia (abogado, por ejemplo) que tengan comunicaciones con los internos. No existe constancia ninguna de la inclusión de sus datos en este fichero para los titulares de datos personales que no son el interno penitenciario. Si la información tratada en FIES operara como razón para imponer un régimen más severo a los internos incluidos en sus diferentes

⁵⁶⁴ GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 234. Véase también GIL GONZÁLEZ, E., *Big Data, privacidad y protección de datos.*, Madrid, 2016, pág. 124.

⁵⁶⁵ Fue creado por Antoni Asunción, nombrado director general de Instituciones penitenciarias en 1988 que llegaría a ser ministro del Interior en 1994. En 1991 fue investigado por el juzgado de instrucción número 9 de Sevilla y juzgado años más tarde acusado de diferentes delitos. Por otra parte, las pautas de gestión de Antoni Asunción se siguen, en su mayoría, manteniendo actualmente. Su actuación es controvertida, con el aval de algunos y la confrontación a sus métodos de otros. Existe también el denominado programa SISPE, con información de igual o parecido contenido, que mantiene y trata datos de Instituciones Penitenciarias.

⁵⁶⁶ Como ejemplo, la Resolución R/00433/2014.

categorías, se genera, en este caso, la duda razonable sobre si no es una base de información discriminatoria y sancionadora de conductas de forma automática, lo cual vulneraría el artículo 13 LOPD, y de manera específica el artículo 6.1. del Reglamento penitenciario (limitación del uso de la informática penitenciaria)⁵⁶⁷. Este tipo de información en ficheros públicos y su tratamiento por parte de las AAPP, debe siempre encontrarse bajo control de los correspondientes órganos que emanen de poderes constitucionales, porque, como obviamente se puede deducir, en las Administraciones de Estados no democráticos, los tratamientos de datos se convierten en valoraciones con implicaciones directas en los Derechos y Libertades Fundamentales⁵⁶⁸. La legalidad y la legitimidad de las Instituciones Penitenciarias para tratamiento de datos de internos con la finalidad de la mejor organización de los establecimientos de reclusión no existiría si fuera la base decisoria sobre la que se sustentara una diferencia de régimen penitenciario para los internos incluidos en sus diferentes categorías (existen varias, en función de la peligrosidad o delito) generándose un tratamiento discriminatorio, por grupos o sancionador. Por ello la valoración de la situación penitenciaria del

⁵⁶⁷ El texto del Reglamento penitenciario expresa que “ninguna decisión de la Administración penitenciaria que implique la apreciación del comportamiento humano de los reclusos podrá fundamentarse, exclusivamente, en un tratamiento automatizado de datos o informaciones que ofrezcan una definición del perfil o de la personalidad del interno”.

⁵⁶⁸ Véase a este respecto el comentario de RÍOS MARTÍN, JULIÁN CARLOS, “Los ficheros de internos de especial seguimiento”]. <http://www.derechopenitenciario.com/comun/fichero.asp?id=995>
<http://www.derechopenitenciario.com/comun/fichero.asp?id=995> El profesor de ICADE realiza una serie de reflexiones sobre la existencia y contenido de los FIES. Actualmente el autor realiza una interesante aportación a la mediación en contexto penal y la denominada justicia restaurativa. La fuerte polémica que tuvo la existencia de los FIES denominó a las bases de datos penitenciarias *bases de tratos*, las cuales, desde una perspectiva subjetiva y humana van implícitas a cualquier relación, no sólo a la conducta penitenciaria, con la diferencia de que en una relación directa se puede conocer la existencia o el deseo de *no relación* pero desde una base automatizada de datos, que almacena gran cantidad de información personal, no existe ni tan siquiera posibilidad de conocer el proceso de valoración de la conducta por parte del titular. Otro asunto es la negación de cancelación (o supresión) de información personal en los antecedentes penales, como se refleja en la SAN 3477/2016, de 15 de septiembre, asunto diferente y que la AN rechaza muy razonablemente por motivos de seguridad nacional.

interno de los datos recopilados en ficheros automatizados está terminantemente prohibida por el artículo 13 LOPD y por el artículo 6.1. del Reglamento penitenciario.

13.1.2 Las valoraciones de las entidades de crédito y solvencia patrimonial.

En el ámbito privado, las Resoluciones de la AEPD son mayoritariamente protagonizadas, en cuanto a valoraciones personales, por empresas de crédito y banca. Los ficheros *de prestación de servicios de solvencia patrimonial y crédito*, que la LOPD regula en su artículo 29. Este tipo de ficheros son especiales, pues los datos personales se encuentran en ellos sin consentimiento del titular (muchas veces sin su conocimiento) y la información se cede a entidades sin relación jurídica con el titular de los datos. Se está ante un caso claro de posible discriminación, con las limitaciones de derechos correspondientes, y no hay duda en este estudio de la legitimidad de acciones con alegación de derechos con rango constitucional. Las STS son muy numerosas⁵⁶⁹. Si la

⁵⁶⁹ La jurisprudencia es extensa sobre la vulneración del derecho al honor como consecuencia de la inclusión de los datos personales en un fichero de incumplimiento de obligaciones dinerarias sin respetar las exigencias derivadas de la normativa de protección de datos personales, en sentencias entre las que pueden citarse las 660/2004, de 5 de julio , 284/2009, de 24 de abril , 226/2012, de 9 de abril , 13/2013, de 29 de enero , 176/2013, de 6 de marzo , 12/2014, de 22 de enero , 28/2014, de 29 de enero , 267/2014, de 21 de mayo , 307/2014, de 4 de junio , 312/2014, de 5 de junio , 671/2014, de 19 de noviembre , 672/2014, de 19 de noviembre , 692/2014, de 3 de diciembre , 696/2014, de 4 de diciembre , 65/2015, de 12 de mayo , 81/2015, de 18 de febrero , 452/2015 y 453/2015, ambas de 16 de julio , y 740/2015, de 22 de diciembre , todas ellas mencionadas en la reciente STS 796/2016, de 1 de marzo de 2016 (FJ 5º) Los datos incluidos en los ficheros deben ser exactos y ciertos, pero además, en los ficheros de crédito y solvencia patrimonial deben ser pertinentes, deben servir únicamente para determinar la solvencia económica del titular de los datos, no para otros fines. Por ello, como afirma la STS 796/2016 mencionada, “no cabe inclusión de deudas inciertas, dudosas, no pacíficas o sometidas a litigio, bastando para ello que aparezca un principio de prueba documental que contradiga su existencia o certeza. Si la deuda es objeto de controversia, porque el titular de los datos considera legítimamente que no debe lo que se le reclama y la cuestión está sometida a decisión judicial o arbitral, la falta de pago no es indicativa de la insolvencia del afectado. En caso de que la deuda resulte finalmen-

prueba de vulneración del artículo 13 LOPD tiene dificultad, la prueba de la existencia de un perjuicio tampoco se sustancia fácilmente. Se establece en las Resoluciones judiciales el daño moral, ya que el económico es difícil de probar. En el caso de la inclusión de personas en listas de impagos o de insolvencia, puede pensarse en daños a la actividad profesional de los afectados, cuantificables difícilmente. Si se alega daño moral, se puede decir que los afectados han sufrido la falta de confianza en sus posibles relaciones sociales, mercantiles y jurídicas. Aun así, sustanciar este derecho está lleno de dudas. Se vuelve a utilizar la normativa penal, el artículo 197 del CP, para proteger el derecho del artículo 13 LOPD. Pero en el CP no existe protección preventiva del Derecho a la protección de datos personales. No existe en este momento normativa administrativa para controlar la actividad de tratamiento de información personal por diversas asociaciones o empresas que tienen como actividad la solvencia patrimonial, por ejemplo, en modo de sanciones ante su abuso o control para trazar el intercambio de datos entre los diversos interesados.

13.2. Derecho de Consulta Gratuita al Registro General de Protección de Datos.

Para ejercer los derechos del titular, se consideraba necesario un Registro de Ficheros, denominado en la LOPD Registro General en su corto artículo 14⁵⁷⁰. El nuevo

te reconocida, en todo o en parte, por la sentencia o el laudo arbitral y por tanto pueda considerarse como un dato veraz definitivo. Pero no era un dato pertinente y proporcionado a la finalidad del fichero automatizado, porque este no tiene por finalidad la simple constatación de las deudas, sino la solvencia patrimonial de los afectados. Por ello solo es pertinente la inclusión en estos ficheros de aquellos deudores que no pueden o no quieren, de modo no justificado, pagar sus deudas, pero no aquellos que legítimamente están discutiendo con el acreedor la existencia y cuantía de la deuda.”

⁵⁷⁰ Con el siguiente texto: Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

RGPD cambia esta obligación, todavía por determinar. En principio se establece la eliminación de la obligación de la inscripción de ficheros en las Agencias de Protección de Datos, por lo que la existencia futura del Registro General de protección de datos es dudosa. La obligación de inscripción implicaba cargas administrativas y financieras a las AAPP y a los responsables de ficheros o de tratamiento de datos, pero no mejoró la protección de los datos personales. Se cambia la notificación de ficheros indiscriminada por una serie de procedimientos y mecanismos que se pretenden eficaces, a definir todavía, que permitan determinar los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, puedan entrañar un alto riesgo para los derechos y libertades de las personas físicas. Una de estas nuevas obligaciones de los responsables de ficheros y tratamientos es la documentación de cualquier violación de la seguridad de los datos personales, los hechos relacionados con ella, sus efectos y las medidas de correctivas adecuadas; además deberán rendir cuentas no sólo a la autoridad de control nacional (en el caso español, la actual AEPD u otra con las mismas o similares competencias) sino también al Comité Europeo de Protección de Datos. Otra novedad que resulta de la supresión de la obligación de inscripción de ficheros es que el encargado y, en su caso, el representante del encargado, llevará un registro de todas las actividades y categorías de actividades de tratamiento efectuadas por cuenta de un responsable. Las PYMES resultan exentas de estas obligaciones, pues no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, salvo que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los titulares⁵⁷¹.

Actualmente el acceso al Registro, que está bajo la supervisión de la AEPD, es público y libre, cualquier persona puede acceder a los datos que constan en él, en contraposición a los derechos que sólo el titular ejerce (ARCO) con la identificación oportuna y que son personalísimos. El conocimiento de la información inscrita en el Registro General permite saber el tratamiento previsto con el tipo de datos que se inscriben (fichero) y algo que es sumamente importante: la finalidad del tratamiento, la cesión de datos del fichero inscrito y si existe o no transferencia internacional de datos autori-

⁵⁷¹ Véase Considerando 81 RGPD.

zada por la AEPD. El responsable del Fichero o tratamiento debe incluir esa información en la inscripción de ficheros antes de cualquier tratamiento de datos de carácter personal, cuestión, que como ya se ha analizado, no se cumple en una mayoría de casos. La AEPD permite el acceso a la consulta de ficheros online⁵⁷².

13.3. Derecho de Acceso a los Datos Personales propios del interesado.

El derecho de acceso permite al ciudadano conocer y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento. Así lo define la AEPD en su web, en función del artículo 15 LOPD⁵⁷³. La doctrina mantiene que este es el instrumento más importante de los que otorga la LOPD al titular de los datos. El acceso a la información que consta en los ficheros del Responsable del fichero o tratamiento, es una especial facultad que integra el derecho fundamental a la protección de datos personales. Por su lógica relevancia práctica, el derecho de acceso otorga al titular de los datos lo más importante: información sobre el tratamiento y ubicación de los datos. en otras palabras, quién tiene mis datos, de dónde o de quién los ha obtenido (origen de los datos), dónde los guarda y qué hace con ellos. Así el titular realiza de forma efectiva un control sobre su información vinculada a datos

⁵⁷² http://www.agpd.es/portalwebAGPD/ficheros_inscritos/como_consultar/index-ides-idphp.php

⁵⁷³ El texto del artículo 15 LOPD es el siguiente: 1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. 2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible o inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. 3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes. El artículo de la LOPD es una transposición del artículo 12 de la Directiva 95/46/CE del 95. En los artículos 27 a 30 del Reglamento se desarrolla su ejercicio. http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/index-ides-idphp.php

personales. Forma parte de los llamados por el TC como *deberes de hacer* en la mencionada STC 292/2000.

El responsable del fichero debe permitir el acceso del titular a sus datos, lo cual quiere decir que no podrá barreras a la obtención de información, y será de forma gratuita. El titular, así mismo, no podrá exigir un informe exhaustivo sobre el acceso o tratamiento de sus datos, como resuelve la AEPD en su Informe de 2005 sobre “La Naturaleza y alcance del Derecho de Acceso”⁵⁷⁴.

En las características del ejercicio del derecho de acceso se definen que es *un derecho personalísimo*, como lo es el derecho a la protección de datos personales. Sólo las personas físicas lo pueden ejercer en nombre propio, con la correspondiente acreditación de su identidad. Los menores e incapacitados pueden ejercer este derecho a través de sus tutores legales. Si se designa un representante voluntario, debe ser de forma expresa para ejercer este derecho, pero no es necesario un poder notarial o más bien no se refleja en la ley. En la práctica es conveniente, pues se exige prueba de esa representación. La AEPD pide las mismas condiciones que exige el artículo 1.717 del CC. Es el Reglamento la norma que describe las condiciones específicas del acceso. Además, es *un derecho independiente* del ejercicio de otros derechos ARCO, no es requisito para el ejercicio de los otros derechos reconocidos. *Su ejercicio debe ser gratuito*, al igual que los otros derechos ARCO. No se permiten ni gastos, ni tarificación. No se puede exigir, por ejemplo, la petición de acceso por carta certificada o burofax. El responsable del fichero responde ante la gratuidad del derecho de acceso, estableciendo un procedimiento para ello. En contrapartida, la necesidad de prueba de su ejercicio ante la AEPD supone realizar algunos gastos en medios que acrediten

⁵⁷⁴ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, “Informe Jurídico 0167/2005 Naturaleza y alcance del Derecho de Acceso.”]. https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/derecho_acceso_rectificacion_cancelacion_oposicion/common/pdfs/2005-0167_Naturaleza-y-alcance-del-derecho-de-acceso.pdf Por ejemplo, el titular de los datos no puede exigir el nombre de todas las personas que han tenido acceso a sus datos, como trabajadores que han realizado labores de tratamiento bajo la supervisión del responsable del fichero o tratamiento. Esta misma posición la mantiene en la Resolución 00948/2011.

la petición de acceso, como la carta certificada. Aunque el Reglamento invierte la carga de la prueba al responsable del fichero o tratamiento para el caso de que se discuta haber cumplido o no con la respuesta a la solicitud de acceso, asunto controvertido y plasmado en el artículo 25.5 del Reglamento⁵⁷⁵. *Es un ejercicio limitado en el tiempo*, pues se puede ejercer en periodos no inferiores a 12 meses, como regula el punto 3 del artículo 15 LOPD, salvo que se alegue un interés legítimo del titular. La Directiva 95/46/CE no establecía plazo, es lo que el legislador español ha entendido por tiempo razonable de periodicidad. Así, el responsable del fichero no sufre de acoso o de peticiones reiteradas, injustificadas. *El ejercicio del derecho de acceso se realizará con un procedimiento sencillo*, que no suponga un esfuerzo para el titular. Las empresas de determinada envergadura suelen atender estas peticiones a través de su canal de atención al cliente. La AEPD ofrece en su web formularios o plantillas⁵⁷⁶ para el ejercicio del derecho de acceso, *recordando que antes de dirigirse (el titular) a la AEPD, deberá hacerlo ante la empresa u organismo responsable/titular del fichero donde estén los datos*⁵⁷⁷. *El responsable del fichero o tratamiento debe resolver sobre el derecho de acceso solicitado en el plazo de un mes desde la recepción de la solicitud*, aunque no disponga de datos del afectado. Si después de ese plazo la solicitud no ha sido atendida, el titular puede dirigirse a la AEPD para que haga efectivo su derecho y se dirija al responsable. El límite al derecho de acceso lo suponen derechos de superior consideración, los ya referidos en otros epígrafes como defensa y seguridad nacional, intereses nacionales, como datos de la Hacienda Pública, fines científi-

⁵⁷⁵ Texto que se comenta: Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber. La Jurisprudencia se ha pronunciado a favor del titular en estos casos. STS de 07 noviembre 2007.

⁵⁷⁶

http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/denunciasciudadano/derecho_acceso_den/common/pdfs/derecho_acceso_a1.pdf

⁵⁷⁷

http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/denunciasciudadano/derecho_acceso_den/common/pdfs/derecho_acceso_a1.pdf

cos o estadísticos. La LOPD lo establece en el artículo 23. Esta negación de acceso es sólo para ficheros de titularidad pública. Los ficheros de titularidad privada no tienen ese límite.

13.4. Derecho de Rectificación y Cancelación

El derecho de rectificación consiste en corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento. El derecho de cancelación permite que se supriman los datos que resulten ser inadecuados o excesivos sin perjuicio del deber de bloqueo recogido en la LOPD. Ambos derechos se regulan en el artículo 16 LOPD⁵⁷⁸.

Los derechos de rectificación y cancelación son también determinantes para ejercicio del derecho a la protección de datos personales, pues si solamente se puede acceder a los datos, el derecho se queda sin eficacia completa.

⁵⁷⁸ El texto del artículo 16 LOPD es el siguiente: 1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. 2. Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos. 3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. 4. Si los datos rectificadas o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación. 5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.
http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/index-ides-idphp.php

La LOPD, que como se ve en esta exposición, no tiene una sistemática adecuada a su rango, no definió el derecho de cancelación ni el de oposición, más bien parece un solo derecho con dos manifestaciones, como opina la doctrina. Es el Reglamento, otra vez, el texto que definió ambos derechos como independientes en los artículos 31 a 33.-Se hacen efectivos cuando los datos que se tratan son inexactos, incompletos, no pertinentes y/o excesivos. El artículo 31 del Reglamento LOPD define por primera vez qué es la rectificación de datos en el punto 1: El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

Para el derecho de cancelación, existen múltiples referencias en la norma, tanto en la LOPD como en el Reglamento, pero son muy confusas. El artículo 5.1. b) del Reglamento define la cancelación como un procedimiento en virtud del cual el responsable cesa en el uso de los datos. Este mismo artículo que define conceptos de protección de datos, añade que la cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos. Es decir, la cancelación no significa siempre supresión total, puede ser sólo un bloqueo en el acceso, un cese en el uso y tratamiento de los datos personales de forma transitoria. Con el tiempo, los datos son suprimidos, cuando ya se han cumplido con todas las exigencias para su mantenimiento.

En el caso de la rectificación, el dato personal se mantiene en el fichero correspondiente, pero corregido, manteniendo la fidelidad y veracidad de los mismos. Se sustituye un dato erróneo por un dato correcto. En el caso de la cancelación, el dato se suprimirá o bloqueará, dependiendo de si es necesario mantenerlo por imperativo legal o contractual, pero desaparece del tratamiento de datos.

Si se aplica el artículo 4 LOPD, para mantener la calidad de datos es necesario realizar estas operaciones de rectificación o de cancelación, por parte del responsable del

fichero o tratamiento, sin necesidad de petición del interesado, dentro de las obligaciones del responsable.

Un asunto importante se refiere al consentimiento para el tratamiento de datos en casos de cancelación. Si se revoca el consentimiento, por consecuencia lógica los datos serán cancelados. Al contrario, si se ejerce el derecho de cancelación, revocar el consentimiento no tiene sentido, porque los datos han sido destruidos o bloqueados. Ambas conductas tienen el mismo resultado, el cese del tratamiento de los datos personales.

Las infracciones en la petición de acceso, rectificación, cancelación u oposición se consideran como muy graves según el artículo 44.4 h) de la LOPD.

13.5. La Agencia Española de Protección de Datos, como Control y Garantía para el ejercicio de los Derechos de las Personas.

En la estructura de la LOPD, el Título III, Derechos de las personas, termina con dos artículos en referencia al ejercicio de la tutela efectiva de estos derechos. Son los artículos 18 y 19, LOPD. El artículo 18 tiene como epígrafe *Tutela de Derechos* y el 19 se denomina *Derecho a indemnización*⁵⁷⁹. En el artículo 18.1 se reconoce el derecho de los afectados a reclamar ante la AEPD. Anteriormente, como se ha visto en el ejercicio de los derechos ARCO, lo tendrá que haber hecho ante el responsable del fichero

⁵⁷⁹ El texto del artículo 18 LOPD es el siguiente: 1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine. 2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. 3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses. 4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

o tratamiento que corresponda, para el caso de estos derechos de las personas. Para el reconocimiento de otros aspectos regulados en la LOPD, como puede ser la obligación de petición de consentimiento del titular de los datos, regulada en el artículo 5 de la LOPD, no es necesario que el titular ejerza ninguna acción, sino que el responsable está obligado por la propia ley. Por eso, este artículo 18 LOPD y su desarrollo Reglamentario en los artículos 117 a 119 dentro del capítulo II del Título IX del Reglamento. Si hacemos un análisis sobre el posible procedimiento de tutela de derechos de las personas y el procedimiento sancionador general de infracciones de la LOPD existen obvias similitudes. En ambos es necesaria la denuncia ante la LOPD por una posible vulneración de sus normas. Entre las diferencias existen las siguientes: el procedimiento de la tutela de derechos ARCO tiene como objetivo la garantía de la efectividad de estos derechos, reivindicado por el titular de los datos ante el responsable del fichero o tratamiento antes de acudir a la AEPD. La AEPD requiere al responsable el cumplimiento de los derechos del titular. Si no lo realiza, sí se puede activar un procedimiento sancionador. El procedimiento de Tutela de derechos se inicia siempre a petición del interesado, por lo que tiene un carácter personalísimo. Por otra parte, el procedimiento sancionador general tiene como finalidad corregir una infracción a las normas de la LOPD, teniendo la AEPD, en este caso, una situación de interés especial, al tener como misión el cumplimiento de las normas de protección de datos. El afectado o titular tendría un papel secundario, frente al anterior procedimiento de tutela. El procedimiento sancionador se inicia siempre de oficio por la Autoridad competente, que es la AEPD. Se puede dar el caso frecuente que este procedimiento sancionador tenga como referencia la puesta en conocimiento de hechos vulneradores por parte de un interesado.

La doctrina considera la regulación de tutela de derechos insuficiente, si se tienen en cuenta los derechos protegidos. Para salvar esa debilidad procedimental en la práctica se acude a las normas que rigen el procedimiento sancionador o del procedimiento general administrativo. Lo que sí ha quedado claro, es la importancia de las sanciones, para casos en que el responsable del tratamiento no atienda la petición de la AEPD para hacer efectivos los derechos ARCO.

A pesar de la intención de la norma en hacer efectivos los derechos de acceso, rectificación, cancelación y oposición, la realidad es bien otra. Ya no son solamente los vacíos normativos en la materia, ya es que el uso de datos personales no puede ser controlado, ni por su titular ni por la AEPD. Es una afirmación simple de entender que se deriva de la información expuesta hasta ahora y la que más adelante se expondrá, que ejercer estos derechos ARCO no es fácil por parte del titular ante determinadas empresas y corporaciones, como en el caso obvio de las redes sociales (Facebook, Google, como más recurrente) o en el caso de empresas más cotidianas, como los bancos, suministradoras de energía, telecomunicaciones, por ejemplo. Vamos a suponer que sí tienen en cuenta la petición de acceso, rectificación, cancelación y oposición. Nada en este mundo actual puede garantizar que los datos personales del titular se encuentren en algún servidor de este universo virtual. Sin uso a la vista, pero almacenados. Sin tratamiento general de la empresa, pero sí usados para ciertos fines que pueden ser inimaginables, generalmente son comerciales, pero lo cierto es que su uso puede no ser controlado por el titular de los datos. Sin entrar en las *teorías de conspiración* y sin resultar alarmista, con toda sinceridad, eso es imposible de saber.

13.6. Derecho a Indemnización y Responsabilidad del Titular del Fichero.

El artículo 19 LOPD es la última norma que recoge el Título III, Derechos de las Personas. Es un artículo sin definir y sin desarrollo reglamentario⁵⁸⁰. El citado artículo generó una importante polémica doctrinal. El titular de los datos podría pensar que, al solicitar la tutela de su derecho fundamental a la protección de datos personales, las muy considerables multas por infracción supondrán, de forma automática, un pago

⁵⁸⁰ Su texto es el siguiente: 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. 2. Cuando se trata de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

indemnizatorio a su favor. Sería una suposición fruto del desconocimiento. En primer lugar, porque las normas de la LOPD son de Derecho Administrativo. Las Resoluciones de la AEPD serían medios de prueba, pero no establecen indemnizaciones para los titulares de datos, perjudicados o creyéndose perjudicados por una acción del responsable del Fichero o tratamiento de ficheros de titularidad privada. El artículo 19.3 LOPD atribuyó esta competencia indemnizatoria exclusivamente a los Tribunales de la Jurisdicción Ordinaria. En el caso de ser AAPP los titulares de ficheros, será aplicable el régimen de responsabilidad de las Administraciones Públicas, que se encuentra en las normas de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las AAPP, según el artículo 19.4 LOPD.

La LOPD, por tanto, reconoció un derecho a indemnización para el caso de daño y responsabilidad civil en el artículo 19.1 LOPD, condicionado a que se haya producido una infracción de la norma legal en materia de protección de datos y que, por ello y en consecuencia el titular de los datos sufra un daño en sus derechos o bienes. Se podría dar el caso, frecuente, de que, habiéndose producido una infracción de las normas de protección de datos, no se produzca daño o lesión en el interesado, o que el daño no sea cuantificable. En muchas ocasiones basta con la simple voluntad del responsable del fichero para cumplir con las normas, en especial, para cumplir con los derechos ARCO, y no es necesario ni posible una indemnización al titular de los datos. En otras ocasiones, las pruebas del daño son inexistentes y están más en los sentimientos internos de los afectados; son esos casos sin vinculación pública de los hechos, los afectados son particulares y no hubo ninguna trascendencia más allá del incumplimiento de la LOPD. El responsable del fichero o tratamiento cesa en su conducta antijurídica o hace pública una rectificación, y terminaría cualquier otra cuestión. Los ejemplos son innumerables y fáciles de entender: se envió un correo publicitario de coches sin autorización, se confundió un teléfono por otro desde un servicio de postventa, se felicitó el cumpleaños a un cliente sin su consentimiento expreso, no se realizó el derecho de cancelación de los datos adecuadamente, entre otros posibles casos.

Al contrario, puede interpretarse que, las posibilidades de derecho de indemnización de los afectados por una vulneración de la LOPD, no tiene porqué limitarse a las infracciones previstas en la misma Ley, con ámbito sancionador. El artículo 19 tiene una interpretación doctrinal abierta, se habla de toda la norma de protección de datos (*incumplimiento de lo dispuesto en la presente Ley*, dice el texto). Se entiende que, por lógica, se incluyen los mandatos constitucionales que inspiran la Ley Orgánica de Protección de datos personales y todo tipo de mandato constitucional vulnerado por conductas que incluyan el tratamiento antijurídico de datos personales para violar derechos y libertades fundamentales, junto con la posible indemnización por daños que otras normas protejan⁵⁸¹.

13.6.1 La inclusión de una persona física en un fichero de solvencia.

Un caso frecuente de vulneración con un reconocido derecho de indemnización es la inclusión de una persona física en los denominados *listados de morosos*, por error o por no pertinencia. Las recientes Sentencias del TS condenan a la parte demandada al pago de indemnizaciones entre 5.000 y 9.000 Euros⁵⁸². El art. 29.4 LOPD estableció que sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos. El art. 38 del Reglamento exigía para la inclusión en estos ficheros de datos de carácter personal que fueran determinantes para enjuiciar la solvencia económica del afectado, la existencia previa de una deuda cierta, vencida, exigible, y que haya resultado impagada. Por tanto, los datos que se incluyan en estos registros de morosos deberían ser ciertos y exactos, pero existirían datos contractua-

⁵⁸¹ Por ejemplo, en los casos de difamación en las redes sociales, véase LÓPEZ RICHART, J., "Difamación en la web 2.0 y responsabilidad civil de los prestadores de servicios de alojamiento", *Derecho privado y Constitución*, nº 26, 2012, pág. 143-201.

⁵⁸² Son las siguientes: STS 1715/2013, de 6 de marzo; STS 355/2014, de 22 de enero; STS 672/2014, de 19 de noviembre y STS 2040/2014, de 21 de mayo.

les que pueden ser ciertos y exactos sin ser por ello sean determinantes para enjuiciar la solvencia económica de los interesados, en cuyo caso no son pertinentes.

No sólo se vulnera el derecho fundamental a la protección de datos establecido en las normas de la LOPD y su Reglamento. Existe en estos casos un daño moral y patrimonial del afectado, al vulnerar su derecho al honor, incidiendo negativamente en la reputación y vida profesional de la persona. En la realidad, las grandes corporaciones prefieren pagar las multas de la AEPD y también las indemnizaciones antes que no realizar este tipo de tratamientos, pues los beneficios que obtienen con los *listados de morosos* son considerados como más importantes por las personas que dirigen estas empresas que el coste de errores en la gestión y tratamiento de datos, por no mencionar el respeto a los DDFF⁵⁸³.

El problema para el titular de datos podría ser muy importante y afectar a más esferas que las de la simple gestión bancaria o crediticia, si pensamos en esos cruces de ficheros o datos (*big data*) que se realizaría sin ninguna regulación específica, por ejemplo, para obtener un puesto de trabajo. En ese caso, se considera que la cuantía de las indemnizaciones comentadas es ridícula en comparación con los efectos adversos. A esto se suma el coste económico que genera el acceso a la jurisdicción y eventuales recursos que pueden llegar hasta llegar al TS; por ello es una cuestión dudosa. Si se quiere añadir más incertidumbre, se comenta el asunto de la transferencia internacional de datos o el tratamiento de datos personales fuera del ámbito de aplicación de la LOPD. En ese caso, sustanciar un derecho de indemnización puede tornarse imposible o de unos costes francamente extravagantes. Un daño más adicional, es la discriminación de una persona sólo por estar inscrita en los *ficheros de morosos*. El asunto de estos ficheros se une al derecho a la impugnación de valoraciones basadas en tratamientos automatizados de datos personales.

13.6.2 El daño o lesión sobre la vulneración del derecho a la protección de datos personales.

⁵⁸³ Se comenta que podría este asunto comenzar a considerarse como daño punitivo.

En cuanto al concepto de daño y/o lesión, la LOPD no lo definió para su normativa. La RAE da al concepto de daño el significado de *valor de la pérdida sufrida o de los bienes destruidos o perjudicados* y para lesión vincula la definición al daño corporal, aunque también lo define en función de un contrato. Las vías procedimentales serían las civiles y en su caso, también las penales, con una acción civil indemnizatoria derivada del delito si fuera reconocida su procedencia. El procedimiento civil tendría una naturaleza económica y, por tanto, sería un juicio declarativo ordinario.

En los casos de petición de indemnización de daños y perjuicios, la doctrina⁵⁸⁴ ha optado por una lectura en función de la Ley Orgánica 1/1982, de 5 de mayo, la cual en el artículo 3.3. expresa que *la existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima. La indemnización se extenderá al daño moral que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta en su caso, la difusión o audiencia del medio a través del que se haya producido*⁵⁸⁵. También se valorará el *beneficio que se haya obtenido por el causante de la lesión como consecuencia de la misma*. Son los denominados daños punitivos.

Se discute también si los daños producidos son sólo morales o también son patrimoniales⁵⁸⁶. Eso no ocurre, por lógica, ante daños de naturaleza económica, que se deben

⁵⁸⁴ PUYOL MONTERO, J., "Comentario al artículo 19 LOPD. Derecho de indemnización", *Comentario a la Ley Orgánica de Protección de datos Personales.*, Madrid, 2010. El autor deduce aplicando esta norma que "la gravedad del daño producido (...) no constituye un límite para el reconocimiento de ese derecho a la indemnización o de reparación civil del daño, y ello, sin perjuicio de la procedencia de otras acciones, entre las que se encuentran aquellas de naturaleza penal." Pero, como señala este autor, también se ha producido una interpretación de la normativa en función de la presunción *iuris tantum*

⁵⁸⁵ Obra y autor citados, pág. 1.273. "en el establecimiento de una relación en la presunción del daño siempre que haya una intromisión ilegítima en los derechos fundamentales que tutela"

⁵⁸⁶ En este caso, "la producción de daños de naturaleza moral está amparada generalmente por una presunción *iuris et de iure* sobre la base de la evidente dificultad que conlleva la acreditación de esta clase de daños, y la compleja labor de proceder a una cuantificación objetiva de los mismos."

en cualquier caso probar por el interesado, al ser cuantificables, por las pruebas admisibles en Derecho. Como se señala por la doctrina, la Jurisprudencia no parece calificar los daños morales en grandes cuantías, estando la media sobre 3.000 Euros por cada procedimiento en que se alega daño moral. No es una cuantía apreciable en estos momentos⁵⁸⁷. En el caso del derecho a la protección de datos personales, PUYOL es partidario de que “no debe admitirse una indemnización por daño moral en aquellos casos en que quepa presumir racionalmente que no se ha producido”. La AEPD se limita en su página web a establecer claramente que no tiene competencia para fijar ninguna indemnización de posibles daños y perjuicios ⁵⁸⁸.

14. Los derechos de las personas en el nuevo Reglamento de protección de datos de la Unión Europea (RGPD) desde la perspectiva del consentimiento.

El texto europeo mantiene un conjunto o grupo de principios (que son normas bajo la visión de ALEXY, se recuerda) y derechos del titular (o interesado, según el RGPD) en el que se refuerza el consentimiento del interesado para el tratamiento de sus datos

Se recuerda el concepto de presunción iuris et de iure: presunción absoluta, que no admite prueba en contrario, es una presunción de hecho y de derecho.

⁵⁸⁷ Obra y autor citados, pág. 1.281. Puyol menciona la obra que se tiene en bibliografía de esta tesis: ORTÍ VALLEJO, A., *Derecho a la intimidad e informática*, Madrid, 1994. En otra obra de Ortí Vallejo se analizaban el año 1994 aspectos de lo que se denominaba libertad informática: ORTÍ VALLEJO, A., “El nuevo derecho fundamental (y de la personalidad) a la libertad informática. A propósito de la STC 254/1993, de 20 de julio.”, *Derecho Privado y Constitución*, nº 2, 1994, pág. 305-332. El autor y catedrático Antonio Orti Vallejo dedicaba a este asunto un texto de 1994, mencionado por Puyol Montero. Para el profesor Orti, que el daño moral no pueda probarse y que su valoración tenga que ser discrecional “no obsta a que en el caso concreto se pueda llegar a la conclusión de que no se produjo daño a la intimidad (o) a otros derechos de la personalidad”

⁵⁸⁸ http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/otros_derechos/indemnizaciones-idphp.php a 14 de diciembre de 2015.

personales de forma legítima por quien los recaba. El consentimiento se convierte en centro de toda la protección, como ya se había demostrado en la práctica, aunque también en esa misma práctica de la protección de datos personales se había demostrado que en determinados casos el consentimiento informado no es la base para el control de la información personal, como mantiene la doctrina⁵⁸⁹. El RGPD opta por definir el consentimiento en el artículo 4. 11) con un texto muy similar a la normativa anterior, como *toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*; novedoso es el artículo 7 RGPD, por el que no solamente se obliga al responsable del tratamiento a demostrar que el titular de los datos consintió, añadiendo que si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo, algo que se aplicaba por la AEPD en sus Resoluciones pero que ahora se convierte en norma. También parece que en la nueva regulación no se permite el consentimiento tácito, práctica que hasta ahora sería posible, estableciéndose la forma de consentimiento expreso en todas las situaciones, sin que el silencio del titular de los datos suponga un consentimiento (tácito o presunto). No será vinculante ninguna parte de la declaración del consentimiento que constituya infracción del RGPD. Además, el interesado tendrá derecho a retirar su consentimien-

⁵⁸⁹ Entre otros se recuerdan las críticas al consentimiento informado de BOIX PALOP, A., "La construcción de los límites a la libertad de expresión en las redes sociales.", *Revista de Estudios Políticos.*, nº 173, 2016. También OLIVER-LALANA, A., "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*, Madrid, 2013. En su exposición sobre *big data*, también presenta dificultades a la efectividad del consentimiento GIL GONZÁLEZ, E., *Big Data, privacidad y protección de datos.*, Madrid, 2016. En general, todas las referencias, haciéndose eco de la realidad, dudan de la efectividad del consentimiento en múltiples recabaciones de datos personales, aunque muchos de ellos lo consideran el eje fundamental del contenido esencial del derecho a la protección de datos

to en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo, afirma la norma europea, para evitar imposibles trámites en el ejercicio de los derechos del interesado. Al evaluar si el consentimiento se otorgó libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato, es decir, si el titular o interesado es parte de un contrato en el que son suficientes una serie de datos, pero se solicitan otros no pertinentes, quizá excesivos, que no son necesarios para el cumplimiento del contrato. En ese caso, la posible respuesta puede ser que el consentimiento no se otorgó libremente, y, por tanto, el tratamiento es ilícito. Las excepciones a este principio de consentimiento se basan en los tratamientos necesarios por ley, por urgencia o por riesgo evidente del titular o interesado. Parecería que se tuvo en cuenta el principio de privacidad desde el diseño o por defecto. Estos aspectos se encuentran a la espera de ser definidos por la Autoridad de control competente. Se supone que los derechos ARCO (acceso, rectificación, cancelación y oposición) se mantendrían y se ampliarían en sus definiciones.

14.1. El consentimiento informado

La información que el titular de los datos debería recibir antes de otorgar su consentimiento se regulan ampliamente en los artículos 13 y ss. del RGPD. Destaca la obligación de informar sobre la existencia de decisiones automatizadas incluida la elaboración de perfiles. En este caso se obliga también al responsable de tratamiento a informar sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. Igualmente, relevante es la obligación de informar sobre el tratamiento para un fin que no sea aquel para el que se recogieron los datos personales; en ese caso se proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información

adicional pertinente. Se debe informar igualmente de la intención del responsable de transferir los datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, cuando proceda, la referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado. Con este último punto se tiene en cuenta la transferencia internacional de datos sin consentimiento del titular.

En el resto de derechos del titular, hasta ahora derechos ARCO (se recuerda, acceso, rectificación, cancelación y oposición, artículos 15,16 y 21 RGPD) la información previa se hace imprescindible para dar sentido al consentimiento.

14.2. Los derechos de supresión y limitación del tratamiento,

El derecho de supresión (o *derecho al olvido*, se recuerda) del artículo 17 RGPD ha sido tratado por su importancia en un epígrafe distinto, y se amplía así el derecho de cancelación a las condiciones que la Sentencia *Google* propició. Otro derecho de las personas es el derecho a la limitación del tratamiento, artículo 18 RGPD, por el cual el interesado podrá obtener del responsable la limitación en el tratamiento de los datos cuando el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; o también cuando el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; en el caso de que el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; o en el caso de que el interesado se haya opuesto al tratamiento en virtud del artículo 21.1 RGPD, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado. El artículo 19 RGPD establece una obligación de notificación para el responsable del tratamiento, consistente en comunicar cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija

un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

14.3. El derecho a la portabilidad de los datos

Otra posible novedad en cuanto a los derechos del interesado (o titular de datos) es el denominado *derecho a la portabilidad de los datos*, regulado en el artículo 20 RGPD. El texto establece que el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado anteriormente, para los casos en que el tratamiento esté basado en el consentimiento otorgado para un tratamiento lícito o para la ejecución de un contrato, en ambos casos el tratamiento de los datos se realiza por medios automatizados. En el caso de que se solicite la portabilidad, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. Se debe respetar lo establecido en el artículo 17 RGPD (derecho de supresión), pero esa limitación no se aplicará cuando el tratamiento sea necesario para el cumplimiento de una cuestión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, ni tampoco cuando afecte negativamente a los derechos y libertades de otros. El derecho a la portabilidad complementaría el derecho de acceso a los datos personales frente a la realidad del almacenamiento de datos en internet, como una herramienta más para el control de la información personal, facilitando la promoción de la competencia entre empresas y la elección de proveedor, especialmente en el sector de las telecomunicaciones.

14.4. El derecho de oposición a la elaboración de perfiles personales.

El derecho de oposición (artículo 21) regula las situaciones en las que exista valoraciones de perfiles por sistemas automatizados, como puede ser para finalidades de marketing (el RGPD habla de *mercadotecnia directa*). La excepción de interés público para continuar con el tratamiento al que se opone el titular se mantiene. El artículo

22 RGPD amplía la regulación acerca de las decisiones individuales automatizadas, incluida la elaboración de perfiles. El titular tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la *elaboración de perfiles*, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Las excepciones se basan en el consentimiento otorgado especialmente para el tratamiento y las ya conocidas como excepciones legales o en casos de necesidad obvia. Se exige directamente al responsable del tratamiento la adopción de medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. Tampoco se admiten valoraciones personales por medios automatizados en caso de tratamiento de datos especialmente protegidos, salvo que sean para excepcionales situaciones y con medidas de seguridad adecuadas para proteger los DDFF y los intereses legítimos del interesado.

El RGPD menciona a lo largo del texto las denominadas técnicas de anonimización, que se tratan en el epígrafe siguiente, como obligación del responsable del tratamiento.

No se han regulado avances de forma específica, ya mencionados en este texto, como son el *big data*, *el cloud* o *el internet de las cosas*. Se prevé una mejor definición por la Autoridad de control española, que se supone, seguirá siendo la AEPD. Por el momento, la AEPD ha publicado dos textos, los primeros después del RGPD, uno de ellos sobre procedimientos de anonimización y otro sobre la reutilización de la información personal en el sector público⁵⁹⁰. Ambos estudios se basan en la anonimización de información personal.

⁵⁹⁰ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Orientaciones sobre protección de datos en la reutilización de la información del sector público.]. AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Orientaciones y garantías en los procedimientos de anonimización de datos personales.]. La AEPD utiliza otro término para sus *Guías*, denominadas *orientaciones* en esta ocasión.

15. Las obligaciones del responsable del tratamiento de datos personales en el nuevo RGPD desde la perspectiva tecnológica.

El RGPD parece dirigir la efectividad del derecho a la protección de datos personales hacia las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que estas obligaciones sean uniformes para toda la UE. Se considera que estas obligaciones tienen un componente técnico muy evidente, pues el RGPD establece que la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de su regulación. El responsable debe poder demostrar que sus tratamientos son conformes con el RGPD y que adopta políticas internas para aplicar medidas que cumplan los principios de protección de datos desde el diseño y por defecto. Esto es de suma importancia para las empresas, pues hasta ahora se consideraba que sólo bajo denuncia a la AEPD las conductas de protección de datos eran inspeccionadas, pocas veces la AEPD inició inspecciones de oficio. El RGPD considera que dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, anonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Vincula la protección de los DDFF a los desarrolladores de herramientas técnicas exigiendo su desarrollo desde el diseño, además de que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. La norma europea especifica que los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos⁵⁹¹.

⁵⁹¹ Considerandos 11, 13, 19, 28, 78, 80, 89, 90, 97, 98, 99 y 150, entre otros. Capítulo IV, responsable del tratamiento y encargado del tratamiento, artículos 24 a 43 RGPD.

15.1. El Representante del responsable del tratamiento que no tenga establecimiento en la UE.

Otra obligación muy importante para el responsable o el encargado del tratamiento no establecido en la UE que esté tratando datos personales de interesados que residan en la Unión y cuyas actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la UE, independientemente de si se requiere un pago por parte de estos, o con el control de su comportamiento en la medida en que este tenga lugar en la Unión, es que debe designar a un representante en el territorio de la UE, a menos que el tratamiento sea ocasional, no incluya el tratamiento a gran escala de categorías especiales de datos personales o el tratamiento de datos personales relativos a condenas e infracciones penales, y sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, vista la naturaleza, el contexto, el ámbito y los fines del tratamiento, o si el responsable del tratamiento es una autoridad u organismo público. La norma no matiza si ese representante debe ser una persona física o jurídica pero sí debe actuar por cuenta del responsable o el encargado y puede ser contactado por cualquier autoridad de control, por lo cual se entiende que debe ser una persona física apoderada debidamente, que represente al responsable del tratamiento o a otra empresa. El representante debe ser designado expresamente por mandato escrito del responsable o del encargado para que actúe en su nombre con respecto a las obligaciones que les incumben y la designación del representante no afecta a la responsabilidad del responsable o del encargado, es decir, no lo desvincula de la norma. El representante debe desempeñar sus funciones conforme al mandato recibido del responsable o del encargado, incluida la cooperación con las Autoridades de control competentes en relación con cualquier medida que se tome para garantizar el cumplimiento del RGPD. Y una nota más, el representante designado debe estar sujeto a medidas coercitivas en caso de incumplimiento por parte del responsable o del encargado⁵⁹².

⁵⁹² Considerandos 80 y 139 entre otros; artículo 4.17, definiciones; informaciones que deben facilitarse al titular o interesado artículo 13 y 14; La regulación de esta figura se encuentra en el artículo 27

15.2. Infracciones y sanciones

En el asunto de infracciones y sanciones, el RGPD especifica que éstas seguirán siendo sanciones administrativas impuestas por la Autoridad de control del Estado miembro. En ese aspecto, parece que el cumplimiento del derecho fundamental a la protección de datos seguirá siendo competencia de la Administración del Estado, sin olvidar el derecho a la tutela judicial efectiva y las posibles acciones de indemnización por vía civil o de denuncia por vía penal (artículos 78 y 79 RGPD), más en dirección de compensar daños en otros derechos y bienes que en la compensación por la violación del derecho fundamental a la protección de datos personales, como ya se ha analizado.

15.3. El Delegado de protección de datos (*Data Protection Officer*, DPO)

Se incluye en el nuevo texto europeo un reconocimiento de la dificultad para el cumplimiento la norma, pues se recomienda desde el propio texto que el responsable o el encargado del tratamiento cuente con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial; o también se recomienda la asistencia especializada si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados. En el caso de que las actividades principales del responsable o del encargado del tratamiento consistan en el tratamiento masivo de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales puede que sea conveniente o incluso necesario contar con asesoramiento en la materia (*Data Protection Officer*, DPO en sus siglas en inglés). Se reconoce en el texto que en el sector privado las actividades principales de un responsable están relacionadas con sus actividades primarias, profesionales, y no están relacionadas con el tratamiento de datos perso-

RGPD; sus actividades se regulan en los artículos 30, 31, 35 y 58 entre otras que puedan ser reguladas con posterioridad.

nales como actividades auxiliares, por lo que puede ser muy acertada la recomendación. El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Los delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente. La figura del delegado de protección de datos se regula en los artículos 37 a 39 RGPD. Sería una novedad para España, pero cuenta ya con un largo recorrido en otros países de la Unión Europea, por ejemplo, en Alemania (con la denominación *Bundesbeauftragten für den Datenschutz*, BfD) primer país en incluirla en su normativa federal sobre protección de datos personales (*Bundesdatenschutzgesetz*, BDSG, artículo (*Paragraph*) 22) de 27 de enero de 1977, que opera a través de competencias federales dentro de la Administración; en los diferentes Land (o Estados Federales) existiría la figura del *Landesdatenschutzbeauftragte* y para el sector privado existe la figura de *Datenschutzbeauftragter* (asimilable a esta figura del delegado de protección de datos)⁵⁹³. Por influencia de Alemania se incluyó en la Directiva 95/46/CE, la cual se derogó por el RGPD, en virtud de lo previsto en su artículo 94, una vez que el mismo comience a ser aplicado en el año 2018. La figura jurídica se extiende a toda la UE, pero el RGPD, sin embargo, no lo definió dentro del artículo 4 RGPD⁵⁹⁴. Es obvio que se está ante una importante oportunidad para que las empresas realmente contraten y otorguen su confianza a profesionales capacitados, con per-

⁵⁹³ Algunos títulos en alemán, más como ejemplos que como referencia: HOCHREITER, M., *Die heimliche Überwachung internationale Telekommunikation*, München, 2001. GOLA, PETER; JASPER, ANDREAS, *Das Bundesdatenschutzgesetz im Überblick*, Heidelberg, 2011.

⁵⁹⁴ La Comisión Europea en su propuesta de 2012 para el nuevo RGPD, no incluyó la definición de DPO, pero parece ser que sí lo define uno de los documentos de Trabajo de los servicios de la Comisión relativo a la evaluación de impacto de su propuesta (SEC (2012) 72 final, de 25 de enero). En este documento se define al DPO como una persona responsable dentro del responsable o del encargado del tratamiento para supervisar y monitorear de manera independiente la aplicación interna y el cumplimiento de las normas de protección de datos. El DPO puede ser tanto un empleado como un consultor externo, en una posible traducción.

fil jurídico, o con profesionales multidisciplinares que puedan aportar sus conocimientos en común para la defensa de los DDFF ante posibles tratamientos y riesgos. De los considerandos y de los artículos del RGPD se pueden destacar como funciones del DPO asesorar e informar al responsable del tratamiento de datos personales de las obligaciones que conforma el tratamiento de datos según el RGPD, las cuales deben ser constadas en su cumplimiento, se entiende, por escrito, además de atender las auditorías que correspondan, formar al personal y asignar responsabilidades dentro de la organización en la que se ejerza sus funciones. Importa también el control de la documentación, la respuesta a las solicitudes de los interesados (titulares de datos personales) y de la Autoridad de control correspondiente, con la cual se perfila como un contacto de comunicación sobre cuestiones relacionadas con el tratamiento de datos. Se le considera su actividad bajo el más estricto deber de secreto y contará con suficiente autoridad dentro de la empresa, reportando sus funciones al más alto nivel, con autonomía e independencia. Todas estas competencias son mucho más amplias que las ejercidas hasta ahora por el responsable de seguridad según la LOPD y su Reglamento, el cual no era una figura obligatoria, aunque muchas empresas contaban con ella para coordinar y controlar únicamente las medidas de seguridad y su cumplimiento. El DPO será obligatorio en las AAPP, como se ha mencionado, y en las empresas privadas también, en función del volumen y tipo de información personal que traten. La necesidad de un profesional formado en protección de datos personales (o también con la posible denominación profesional de la privacidad), conjugaría aspectos de conocimientos en derecho y en informática, pudiendo interactuar con otros profesionales para la consecución de objetivos comunes. Hasta ahora los profesionales de la privacidad carecieron de regulación profesional específica, lo cual indujo a diferentes tipos de organizaciones hacia el intrusismo profesional en España. La profesionalidad debería poder acreditarse, para elaborar propuestas, soluciones, informes o sistemas acordes con la legislación que atañe a la protección de datos personales. La LOPD funcionó jurídicamente como una norma garantista de DDFF, muy exigente, compleja dentro del Ordenamiento jurídico español como norma administrativa, pero hasta la entrada en vigor del RGPD el legislador permitió la fijación de las condiciones

para la aplicación de la normativa que regula el cumplimiento de un derecho fundamental en manos de personas sin cualificación profesional demostrada⁵⁹⁵. En este momento la AEPD todavía no ha perfilado adecuadamente sus funciones para España.

15.4. La anonimización y la seudonimización.

El RGPD apuesta firmemente por lo que denomina *seudonimización*, palabra que todavía no se encuentra en nuestro Diccionario de la Real Academia Española de la Lengua, por lo que en el análisis de tesis se ha optado por la voz *anonimización*, utilizada por la doctrina y por el GT29, que tampoco se encuentra como tal en el Diccionario, pero sí se puede referenciar al verbo anonimizar, con el significado de *expresar un dato relativo a entidades o personas, eliminando la referencia a su identidad*. La anonimización no tiene todavía un marco jurídico definido. Otro asunto importante consiste en señalar las diferencias entre los conceptos anonimizar y seudonimizar, que autores como GIL mencionan, basándose en el Dictamen 05/2014 del GT29 sobre técnicas de anonimización, de 10 de abril y en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, sobre privacidad y comunicaciones electrónicas. Para anonimizar cualquier dato personal es necesario eliminar los elementos suficientes para que no puede identificarse al titular (interesado). El tratamiento se considera que debe ser irreversible⁵⁹⁶. La idea subyacente es que el resul-

⁵⁹⁵ Véase a este respecto las ideas de MARTÍNEZ MARTÍNEZ, R., "El rol de los profesionales de la privacidad", *Hacia un nuevo derecho europeo de protección de datos*, Valencia, 2015, pág. 549.

⁵⁹⁶ La Directiva 2002/58/CE se refiere en el considerando 26 a la anonimización y a los datos anónimos para que los datos sobre tráfico utilizados para la comercialización de los servicios de comunicaciones o para la prestación de servicios de valor añadido deban también eliminarse o hacerse anónimos tras la prestación del servicio. El artículo 26.1 dispone que los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación, junto con el artículo 9.1, el cual establece que en caso de que puedan tratarse datos de localización, distintos de los

tado de la anonimización, entendida esta como una técnica aplicada a los datos personales, debe ser, de acuerdo con el actual estado de la tecnología, tan permanente como el borrado, con otras palabras: debe garantizarse que es imposible tratar los datos personales. La seudonimización consiste en una técnica diferente, en sustituir o reemplazar un atributo de un grupo de datos por otro atributo, aleatorio o simplemente como cifrado o nombre supuesto. Esta técnica permite la reidentificación, bien por el uso de la clave de encriptación o cifrado o por la relación masiva de bases de datos. El artículo 4.5 RGPD define seudonimización como el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. Para la AEPD son datos personales anonimizados, aquellos que cabría atribuir a una persona física mediante la utilización de información adicional y deben considerarse información sobre una persona física identificable. La anonimización es una forma de eliminar las posibilidades de identificación de las personas físicas. La AEPD reconoce que el avance de la tecnología y la información disponible dificultan las garantías al anonimato

datos de tráfico, relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido. Las normas ISO 29100 definen la anonimización como el proceso por el cual la información de identificación personal se modifica de forma irreversible de tal manera que el responsable del tratamiento no puede identificar, directa o indirectamente, ya sea por sus propios medios o en colaboración con algún tercero, a la persona asociada a dicha información personal. Para la normativa ISO, lo esencial es la irreversibilidad del proceso de modificación de datos personales. Como un comentario añadido, en Alemania también se aplican los conceptos de anonimización según las normas ISO y para Francia los datos no dejan de ser datos personales aun siendo anónimos, es decir, siendo muy difícil su reidentificación. La AEPD utilizaría la dirección menos restrictiva, dirigiéndose hacia la palabra anonimización, pero aceptando la posible reidentificación.

absoluto, especialmente a lo largo del tiempo, pero, en cualquier caso, la anonimización será una garantía para la privacidad.⁵⁹⁷.

Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.

Por lo tanto, ni los principios de protección de datos ni el RGPD (se entiende que también toda la regulación actual sobre protección de datos) deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable o deje de serlo.

La aplicación de la anonimización a los datos personales reduce los riesgos para los titulares de datos, proporcionando a los responsables y a los encargados del tratamiento una herramienta para cumplir sus obligaciones de protección de datos. Pero la introducción explícita de la anonimización en el presente Reglamento no excluye ninguna otra medida relativa a la protección de los datos, aunque se persigue incentivar la aplicación de la anonimización en el tratamiento de datos personales con suficientes medidas técnicas y de gestión, permitiendo que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concre-

⁵⁹⁷ AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Orientaciones y garantías en los procedimientos de anonimización de datos personales."]. p. 2. Como se puede comprobar, la AEPD utilizar la voz española anonimizar para lo que el RGPD define como seudonimizar, aunque la autora GIL haya expresado muy claramente las diferencias en función de anteriores textos de la UE, como son el Dictamen 05/2014 del GT29 sobre técnicas de anonimización, de 10 de abril y en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, sobre privacidad y comunicaciones electrónicas, ambos textos mencionados.

ta, posibilitando la identificación si fuera necesaria⁵⁹⁸. Destaca el uso de datos personales con fines estadísticos y científicos, en los que se debe respetar al máximo la identidad del titular, por lo que la anonimización se convierte en un buen recurso para la licitud del tratamiento, junto con el cifrado (artículo 89.1 RGPD). Pero en general, la anonimización es una excelente herramienta para proteger datos personales ante los usuarios de los sistemas informatizados, pues pueden tratar datos sin conocer la identidad de sus titulares, con lo cual el beneficio se produce tanto para el responsable del tratamiento como para el propio usuario, normalmente un trabajador o funcionario, que no tiene por qué hacerse con una responsabilidad que no le corresponde, llevando a efectos buena parte de los principios de protección junto con el deber de secreto y confidencialidad. Es también una de las herramientas propuestas por el principio de protección de datos desde el diseño y por defecto y es la primera medida a tener en cuenta en la seguridad del tratamiento (artículo 32 a) RGPD). Los códigos de conducta la deben incluir (artículo 40.2 d) dentro de sus normas más básicas. Entre los riesgos que la anonimización no evita, se encuentran las técnicas de reidentificación o inferencia⁵⁹⁹. La anonimización debe eliminar o reducir al mínimo los riesgos de

⁵⁹⁸ Considerando 26, 28, 29, 78, 156 entre otros.

⁵⁹⁹ Inferencia es una técnica informática por la cual se deduce con muchas posibilidades de certeza el valor de un atributo a partir del valor de otros atributos en su conjunto. La reidentificación tiene una similar definición, aunque son necesarios más datos correctos. A este respecto véase la AEPD AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Orientaciones y garantías en los procedimientos de anonimización de datos personales."]. La AEPD considera que la reidentificación es una identificación indirecta como la puede tener lugar como consecuencia de información de una o varias fuentes que por sí misma o en combinación de otros factores puede permitir la reidentificación de las personas cuando sus datos hubieran sido anonimizados. Por ejemplo, la combinación de sexo, edad, lugar de nacimiento y padecimiento de una determinada enfermedad pueden permitir la identificación indirecta de una persona concreta. Véase también las ideas de GIL GONZÁLEZ, E., *Big Data, privacidad y protección de datos.*, Madrid, 2016, pág. 83 y ss.. oponiéndose a la anonimización y con muchos más razonamientos se opone a la seudonimización, pues considera que no es efectiva como técnica de protección ante los sistemas de *big data*. En otro sentido, COTINO HUESO, L., *Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías.*, Valencia, 2010, pág. 386 y ss.. También GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015. en varias páginas de la obra, resaltando la exposición de la página 35, en la que duda de la técnica como efecti-

re-identificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, sin distorsión de los datos reales. Un análisis masivo de los datos o *big data* que puedan derivar de los datos anonimizados debe ser tan correcto en sus resultados como el resultado del análisis que pudiera obtenerse si hubiera sido realizado con datos no anonimizados. Lo que se necesita es la denominada ruptura de la cadena de identificación de las personas. A través de protocolos de actuación se pueden prever las consecuencias de una eventual re-identificación de las personas que pudiera generar un perjuicio o merma de sus derechos o también una hipotética pérdida de información por negligencia del personal implicado, o por falta de una política de anonimización adecuada o por una revelación de secreto intencionada que diera lugar a la pérdida de las variables de identificación o claves de identificación de las personas. Las técnicas informáticas para proceder a la anonimización son realmente complejas y lógicamente forman parte de los conocimientos profesionales de los técnicos en esa materia. La AEPD ha reconocido como principios de la anonimización la gestión proactiva de la protección de datos, la privacidad por defecto, la privacidad objetiva (riesgo asumible de re-identificación), la plena funcionalidad o utilidad final de los datos anonimizados y la privacidad para todo el ciclo de gestión de la información personal, junto con la información y formación de los responsables y usuarios de datos en los sistemas informatizados, asunto este de suma importancia para los DDFF de los titulares de datos personales, pues un sistema informático no libera información personal por sí mismo, es necesario que una acción humana lo realice. La relevancia del respeto a los DDFF formaría parte de la conciencia individual, con beneficios en la efectividad de las conductas.

va. MARTÍNEZ OTERO, J., "El derecho al olvido en Internet", *Revista de Derecho Político*, nº 93, 2015, pág. 103-142, pág. 114 y ss. El autor resalta la necesidad de la anonimización en las Sentencias y actuaciones administrativas para la protección de los derechos a la intimidad, a la reinserción social o al libre desarrollo de la personalidad, entre otros afectados por la protección de datos, y rechaza los métodos técnicos de reidentificación. Se recuerda la importancia de la anonimización para el tratamiento de datos de salud, con referencias en ese epígrafe. Como referencia práctica véase DORSCHER, J., *Praxishandbuch Big Data. Wirtschaft - Recht - Technik.*, Wiesbaden, 2015, pág. 185-189.

15.5. Principio o norma de neutralidad tecnológica

El considerando 15 RGPD enmarca la protección de los datos de las personas físicas en lo que denomina neutralidad tecnológica, por la cual la protección de datos no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del RGPD. El principio de neutralidad tecnológica se encontraba ya en la regulación contenida en la Directiva 2002/58 sobre privacidad en las comunicaciones, afirmando a su vez que la Directiva 95/46/CE cubría cualquier forma de tratamiento de datos, tanto automatizado como no automatizado. Los dispositivos que conforman las redes de comunicaciones tenían suficiente regulación para su fabricación, pero se hizo también necesario que los fabricantes de dichos componentes de servicios de telecomunicaciones electrónicas incorporaran más protección a sus productos para garantizar la intimidad del usuario y la protección de sus datos. Como afirma la autora GARRIGA DOMÍNGUEZ, el principio de neutralidad tecnológica se formula para equilibrar la relación entre el usuario de productos tecnológicos y los diversos operadores en el mercado de la tecnología, pues el primero tiene una carencia de conocimientos sobre la actividad del segundo que resulta en una descompensación evidente⁶⁰⁰. El principio de neutralidad tecnológica se encuentra íntimamente relacionado con los otros principios que se van

⁶⁰⁰ GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales*, Madrid, 2015, pág. 243 y ss. Muchos de los servicios ofrecidos en internet, se ofrecen por defecto con una total deshabilitación de los datos personales, cuando debería ser al contrario, el usuario, titular de datos, debería habilitar las aplicaciones para exponer sus datos y el operador debería ofrecer sus aplicaciones protegiéndola, pues el desconocimiento de las tecnologías por parte del interesado le convierte en ignorante de las consecuencias, mientras que el operador sí debería conocerlas cuando genera específicamente aplicaciones que exhiben datos personales. No se trata de que se censure información, se trata de proteger al usuario en sus derechos fundamentales y en que sea consciente de los riesgos de su publicación.

a mencionar, el de privacidad desde el diseño y por defecto; así también, se incluyen en aspectos técnicos el respeto a los DDFF, comparable a las exigencias de seguridad para otros usos de tecnologías, como pueden ser máquinas industriales de fabricación de objetos, que deben incorporar dispositivos de seguridad para prever conductas que puedan dañar la integridad de la vida y la salud de los usuarios y que además, deben obtener certificaciones determinadas que garanticen dicha seguridad. Se puede apreciar que el principio de privacidad desde el diseño sería un importante factor en el respeto de los DDFF de los usuarios, titulares de datos personales, ante otros derechos como puede ser la intimidad o la libertad⁶⁰¹.

15.6. Principio de privacidad desde el diseño y por defecto.

El principio de la privacidad desde el diseño parte de la obligación del responsable del tratamiento sobre la evaluación de todos los procesos de información desde la perspectiva de su implicación en la protección de datos personales. Desde el año 2007 la Comisión había estudiado un conjunto de medidas tecnológicas para proteger el derecho a la intimidad a través de la supresión o la reducción del tratamiento de datos personales, facilitando a su vez el cumplimiento de la normativa sobre protección de datos y sin menoscabar la funcionalidad del sistema. Es lo que se denominó Tecnolo-

⁶⁰¹ Ídem. La autora realiza un estudio sobre otros autores, en especial cita a Ann CAVOUKIAN, promotora de la filosofía de la seguridad de datos desde el diseño, la cual engloba los sistemas de tecnologías de la información, las prácticas de negocio responsable y el diseño físico e infraestructura de la red de comunicaciones. Es una de las referencias en cuestiones de seguridad tecnológica aplicada constantemente por los arquitectos de sistemas informáticos e ingenieros de telecomunicaciones. Los 7 principios se pueden resumir en medias proactivas y no reactivas ante una violación de la seguridad, la privacidad por defecto, la privacidad incrustada formando parte de los sistemas tecnológicos, la funcionalidad total, sin que ninguna parte interviniente en el proceso sea minusvalorada, seguridad de extremo a extremo para que los datos cuenten con la máxima y misma protección desde el inicio del tratamiento hasta su destrucción, visibilidad y transparencia para usuarios y proveedores, y por último, el respeto por la protección de datos personales de los titulares, que se traducirá en mejores resultados para todas las partes intervinientes y en un mayor respeto al conjunto de DDFF.

gías de Protección de la Intimidad (*Promoting Data Protection by Privacy Enhancing Technologies* (PET) Se basa en los principios elaborados a partir de 1990 por Ann Cavoukian en siete principios fundamentales para unificar la trilogía que pudieran configurar los sistemas de aplicaciones tecnológicas (software + hardware), las prácticas empresariales responsables en los DDFF y el diseño físico de infraestructuras de comunicaciones en red. El RGPD puede ser que los tuviera en consideración para la redacción de sus normas, aunque la norma europea no menciona que se deban cumplir los principios de privacidad desde el diseño, sino que considera la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales, una exigencia para la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de su normativa. Así, el responsable del tratamiento, podrá demostrar la adopción de políticas internas y la aplicación de medidas que cumplan los principios de protección de datos desde el diseño y por defecto. La norma enumera algunas de esas medidas, entre las cuales se incluye reducir al máximo el tratamiento de datos personales, anonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que estén basados en el tratamiento de datos personales o que traten datos personales para cumplir su función, se motivará a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos.

Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos y la norma presta especial interés al tratamiento de datos en un tercer país para que se apliquen los principios de protección de datos desde el diseño y por defecto. El artículo 25 RGPD se dedica a esta temática, pudiéndose activar mecanismos de certificación para su comprobación

y eficacia, al igual que el artículo 47, que regula las Normas Corporativas Vinculantes, establece en su apartado 2.c) la obligación de establecer normativas internas según los principios de protección de datos desde el diseño y por defecto. Con este tipo de prácticas, se extiende la visión empresarial más allá del propio cumplimiento de la normativa y se convierte en un garante de DDFF, lo cual significa mucho para la sociedad actual, eliminando la costumbre de pensar en *ganadores y perdedores*, generando la sensación de calidad, seguridad y confianza que inspiran a la modernidad hacia el desarrollo social⁶⁰².

15.7. Principio de transparencia.

El artículo 5.1 afirma que los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado, estableciendo tres principios fundamentales: *licitud, lealtad y transparencia*. En el capítulo III, Derechos del interesado, se desarrollan el principio de transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado, ya comentados. La norma europea dedica especial interés al principio de transparencia en la gestión y tratamiento de datos personales. En varios considerandos se explica lo que el RGPD entiende por transparencia en relación a las diversas cuestiones que expone y regula. Se requiere transparencia a los operadores económicos para garantizar un nivel coherente de protección de las personas físicas en toda la UE y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, junto con la seguridad jurídica que aporta una normativa común. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y entendible, por medio de un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afecta-

⁶⁰² Considerando 78 y 108 entre otros.

das y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Por todo ello, el principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, como se ha reseñado, y, además, en su caso, se visualice. Por ejemplo, a través de un sitio web en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender⁶⁰³. La norma invita a los responsables de datos personales a fomentar y aumentar la transparencia y el cumplimiento del RGPD, con el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados (titulares de datos personales) evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes. Este punto es sumamente importante. Las certificaciones son muy apreciadas por la regulación europea y parece ser que el RGPD las promueve para regular la protección de datos, con una regulación específica en los artículos 42 y 43, sumamente amplios. Tomando como referencia la definición estipulada en normas ISO, se puede entender que la certificación es la acción llevada a cabo por una entidad independiente de las partes interesadas mediante la que se manifiesta que una organización, producto, proceso o servicio, cumple los requisitos definidos en unas normas o especificaciones técnicas y de procesos de trabajo. Constituyen un elemento diferenciador en el mercado, mejorando la imagen de productos y servicios ofrecidos, generando seguridad y confianza entre las partes que intervienen en los procesos empresariales. La eficacia es la respuesta a la normativa generada por la propia organización interesada para ofrecer a sus clientes, accionistas, empleados, AAPP y en general, a la sociedad en la que operan con mejores herramientas para sus decisiones de gestión, pues con los certificados se simplifican muchos procesos⁶⁰⁴. La norma europea presenta incluso la posibilidad de lograr el denominado en el

⁶⁰³ Considerandos 13, 39, 58, y 100, entre otros textos del RGPD.

⁶⁰⁴ Las organizaciones buscan proveedores cuya gestión y/o productos cuenten con el aval de una entidad de confianza, lo que se denomina *valor competitivo diferencial*, en España, por ejemplo, las certi-

artículo 42.5 RGD, *Sello Europeo de Protección de Datos*. Lo que también existirá será la certificación que apruebe la Autoridad de control española, sea de organismos que dicha autoridad apruebe, sea de la propia Autoridad de control, con los requisitos necesarios para ser considerado como tal. Sobre el principio de transparencia parece desarrollarse toda la nueva regulación europea, con el objetivo de ofrecer soluciones adecuadas y eficaces en todos los posibles tratamientos de datos personales, teniendo en cuenta las nuevas técnicas y telecomunicaciones, que son cada vez más amplias y cuentan con mayor calado social. Ante las innumerables ventajas de todos esos elementos, se encuentra la obligación de reforzar la protección de los DDFF, y la herramienta más adecuada, según los legisladores y en un recorrido de más de cincuenta años, es el derecho a la protección de datos personales con los instrumentos que puedan y deban mejorarse, ante el tratamiento de datos. El principio de transparencia permite conocer quién es la persona que decide los tratamientos, su análisis y valoración de las conclusiones con la consiguiente acción que repercuta en terceros.

15.8. Obligación de evaluación del impacto de las tecnológicas empleadas en el tratamiento de datos.

Se elimina la obligación de inscripción de ficheros para notificar a las Autoridades de control sobre los tratamientos de datos (el importante Considerando 89 RGD, como ya se ha comentado en otro espacio). Se sustituye esa obligación que no fue efectiva por procedimientos y mecanismos eficaces que se centren en los tipos de operaciones

ficaciones en ISO y los sellos de calidad se ofrecen por AENOR, entre otras internacionales, como *Bureau Veritas*. Existe desde hace algunos años la certificación en ISO 27001 de sistemas de gestión de la información. Se piensa desde esta tesis, que la AEPD abrirá otro tipo de certificaciones en dirección a la protección del derecho fundamental a la protección de datos personales, tal y como se regula en el RGD. En una línea de análisis del principio de transparencia en las AAPP por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno (la denominada Ley de transparencia), con una posición interesante respecto a la protección de datos véase PIÑAR MAÑAS, J., *Transparencia, acceso a la información y protección de datos*, Madrid, 2014, pág. 13 y ss.

de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial. En tales casos, el responsable debe llevar a cabo, antes del tratamiento, *una evaluación de impacto* relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con la normativa europea. Aquí la norma no ha quedado clarificada en la definición de qué son las evaluaciones de impacto relativas a la protección de datos. Se espera que la AEPD o Autoridad de control correspondiente, aclare esta obligación. ¿Es una auditoría externa? ¿Puede ser un proceso de certificación? Porque el RGPD invita a las empresas a elaborar Códigos de conducta para facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las PYMES. Dichos Códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento. Se está, por tanto, ante una invitación a la autorregulación empresarial en materias de DDFF, acompañada de prácticas de certificación, para fomentar la transparencia y el cumplimiento de la nueva norma.

El artículo 35 RGPD establece lo que denomina evaluación de impacto relativa a la protección de datos personales. Antes del tratamiento de datos y cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, *el responsable del tratamiento está obligado a su evaluación,*

recabando el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos, la cual se requiere para los casos en que se lleva a cabo una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; también para el tratamiento a gran escala de las categorías especiales de datos (artículo 9.1 RGPD) o de los datos personales relativos a condenas e infracciones penales (artículo 10 RGPD) o para la observación (visualización) sistemática a gran escala de una zona de acceso público, aspectos todos ellos que afectan a los DDFF. La Autoridad de control competente para cada Estado miembro realizará un listado con los tipos de tratamientos que requieran una evaluación de impacto, comunicando ese listado al Comité y siguiendo los mecanismos de coherencia para los casos en que se adopten medidas que impliquen a varios países de la UE o a tratamientos de datos personales que afecten a la libre circulación de datos en la Unión. El artículo 35 RGPD realiza un listado de cuestiones que deben tenerse en cuenta dentro de la evaluación de impacto, como son la descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; la evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; la evaluación de los riesgos para los derechos y libertades de los interesados, y las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas. Se deben presentar ciertas cuestiones como muy difíciles de entender por los responsables de tratamiento de datos personales. Un ciudadano con formación en su profesión no va a comprender fácilmente la implicación de los DDFF en su actividad. La Autoridad de control (se espera que la AEPD o Agencia con las mismas competencias) deberá definir esta obligación, como se ha comentado, aclarando sus requisitos.

Los Derechos Fundamentales y las normas de protección de datos personales.
Práctica empresarial y ciudadana.

Dña. María Montserrat Velasco Nájera

Dirigida por: Dr. D. Antonio Magdaleno Alegría, Profesor de la Universidad de Cantabria.

Página 475 | 606

CAPÍTULO QUINTO. SOLUCIONES GLOBALES A PROBLEMAS GLOBALES. AUTOREGULACIÓN EMPRESARIAL Y CERTIFICACIÓN DE TITULARES DE DATOS PERSONALES, UN OBJETIVO MUNDIAL.

Ante una mayor proyección de las acciones humanas dentro de un mundo sin fronteras, una nueva concepción de los sistemas normativos se convierte en una necesidad. El sistema regulatorio que pretenda una proyección hacia el futuro debe abarcar un ámbito del derecho cada vez mayor, en cuanto a su territorialidad y sujetos de derechos, convirtiendo la apertura de los sistemas jurídicos en un asunto básico y trascendente cuando se cuestiona la protección de los DDFF. Desde el inicio de esta exposición, se ha razonado desde una perspectiva global, humana, como son los DDFF en general y al igual que, por lógica, se presenta el derecho fundamental a la protección de datos personales. La difusión del tratamiento de datos personales precisa de una actitud mundial de respeto al derecho fundamental a la protección de datos, al estar también implicados otros DDFF. Como ha quedado establecido en este texto, los datos se exportan a diversos sistemas jurídicos, los cuales deben comprometerse al respeto de los DDFF, para que sean eficaces frente a los ciudadanos, desplegando toda una serie de garantías para su protección⁶⁰⁵. Al igual que en otros asuntos trascendentes

⁶⁰⁵ Se trata de un derecho a protección, dentro de la doctrina. Véase al respecto la exposición de ALEXY, R., *Teoría de los derechos fundamentales (Theorie der Grundrechte, 1986)*, Madrid, 1993, pág. 435 y ss. Son “los derechos del titular de derecho fundamental frente al Estado para que éste lo proteja de intervenciones de terceros” (...) “No sólo la vida y la salud son bienes posibles de protección, sino todo aquello que, desde aspectos iusfundamentales, es digno de ser protegido, por ejemplo, la dignidad, la libertad, la familia y la propiedad. No menos variadas son las formas posibles de protección. Ellas abarcan, por ejemplo, la protección a través de normas del derecho penal, de normas de derecho procesal, de acciones administrativas y de la actuación fáctica. Lo común detrás de estas variedades es el hecho de que los derechos a protección son derechos subjetivos constitucionales frente al Estado para que éste realice acciones positivas fácticas o normativas que tienen como objeto la delimitación de las esferas de sujetos jurídicos de igual jerarquía como así también la imponibilidad y la imposición de esta demarcación.” El autor cita a KANT: “El derecho es, pues, el concepto propiamente dicho de las condiciones bajo las cuales es posible conciliar la arbitrariedad del uno con la arbitrariedad del otro, de acuerdo con una ley universal de la libertad”

para la humanidad, el consenso y el acuerdo se tornan imprescindibles en estas cuestiones sobre el derecho a la protección de datos personales, donde se encuentran involucrados los propios ciudadanos con su uso y disfrute de los medios tecnológicos, los gobiernos que deben establecer la norma para el desarrollo del contenido material del derecho y en un rol muy ventajoso las empresas de bienes y servicios de todo tipo, que han encontrado en el mundo de las comunicaciones y de los sistemas informatizados una magnífica plataforma para sus actividades económicas de todo tamaño. Desde los más pequeños empresarios, autónomos, hasta los grandes consorcios internacionales de empresas, operan en el (espacio denominado) *ciberespacio*, donde los datos personales generan negocios basados en perfiles de conducta y en comunicaciones. El objetivo de la regulación en materia de protección de datos personales no sería una normativa europea o regional (bien hacia una dirección transatlántica o bien hacia una dirección transpacífica), mucho mejor se trataría de establecer las bases de normalización de relaciones entre todos los operadores mundiales, unificando criterios legales para evitar fragmentaciones jurídicas, resolviendo el problema de la seguridad en internet, tanto para el intercambio de bienes y servicios como en actividades culturales, políticas, e incluso religiosas o de salud, entre otros posibles ámbitos de la humanidad. En ese escenario, los DDFF serían la base (abstracta) de la realidad jurídica o normativa (concreta) dentro de los diferentes Estados. Ninguna doctrina negaría la existencia de unos fundamentos o principios de carácter universal que pudieran ser complementados (sin contradicciones a su contenido esencial) por una normativa autorregulada y pactada entre los diferentes operadores sociales aludidos, siempre bajo control de su ejecución desde el Estado de Derecho. Es lo que ARENAS RAMIRO denominó *armonización global*, con la ambición de ir mucho más lejos que las parciales regulaciones nacionales (o *nacionalistas*, como podrían ser los espacios legislativos cerrados, con el significado negativo que pudiera contener ese término)⁶⁰⁶.

⁶⁰⁶ ARENAS RAMIRO, M., "Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades", *Hacia un nuevo derecho europeo de protección de datos*, Valencia, 2015, pág. 325. De esta forma, en las ideas expuestas por la autora, se reforzaría el Derecho.

1. Algunas ideas previas sobre conceptos utilizados en la práctica.

1.1. La autorregulación.

La autorregulación se define por la acción y efecto de regularse (a uno mismo). Significa ajustar, medir o computar algo por comparación o deducción, reglar o poner en orden, ajustar el funcionamiento de un sistema a determinados fines, determinar las reglas o normas a las que debe ajustarse alguien o algo. Puede ser sinónimo de re-ajustar, como aumentar o disminuir coyunturalmente una cuestión o situación⁶⁰⁷.

Los sistemas de autorregulación empresarial son la respuesta a la exigencia de la sociedad para que existan unas garantías de confianza y credibilidad en la gestión de las empresas dentro de una civilización avanzada. La autorregulación empresarial no pretendería ser un sustituto del control legal, sino servir de útil complemento a éste, a ser posible mediante la co-regulación. Una forma de autorregulación son los códigos de conducta (o deontológicos) elaborados por las empresas de un determinado ámbito y actividad para regular aspectos que conciernen a sus relaciones entre sí y a los consumidores y usuarios que consumen sus bienes y servicios.

Una norma generada por autorregulación es de adhesión voluntaria, producto del consenso, suele estar basada en la experiencia y en el desarrollo tecnológico y aprobada por lo que se denomina Autoridad u organismo regulador. Pero puede ser considerada, si así ha sido pactado por las partes o regulado por ley, de cumplimiento obligatorio y su incumplimiento entrañaría consecuencias sancionadoras o si procede, incluso punitivas. Las normas autorreguladas suelen aportar garantías en cuanto a los niveles de calidad y seguridad para las empresas adheridas, con lo cual se posicionan mejor en el mercado y constituyen una importante fuente de información sobre los procedimientos que ejecutan dentro de la organización adherida para otras empresas, las AAPP o consumidores en general.

⁶⁰⁷ Salvo que se especifique, se engloba bajo el concepto de autorregulación los códigos tipo, los códigos deontológicos y la co-regulación. Posteriormente, se identificarán las diferencias.

Aportando algunos matices adicionales, las diferencias entre regulación tradicional y autorregulación se podrían definir en la siguiente comparativa:

Regulación tradicional	Autorregulación
Adopción tradicional de normas jurídicas, a través del legislador o el gobierno democrático.	Los propios actores adoptan los códigos de conducta que consideran necesarios por consenso, aceptación o acuerdo.
Autoridad democrática competente	Procesos de control independientes
Se fijan los objetivos e intereses en la generalidad de la sociedad	Se fijan las normas que los interesados consideran apropiadas para una empresa o un sector de actividad.
Las sanciones en caso de incumplimiento se imponen con las garantías del Estado de Derecho.	Las soluciones a los conflictos se producen por medio de la mediación o el arbitraje, al margen del Derecho estatal, en un principio. Por lógica, las líneas estatales de la defensa del Derecho, siempre están abiertas.
Los interesados reciben la norma	Los interesados aplican la norma auto-gestionada.
Lentitud e ineficacia	Exceso de voluntarismo que puede conducir también a la ineficacia si no existen controles estatales y normativa coactiva prevista.

Se ha denominado co-regulación a la autorregulación regulada por las Instituciones para adoptar sistemas de cooperación entre AAPP, Autoridades políticas, empresas y la sociedad civil. El poder público a través del legislador integra las reglas para desarrollar normas de autorregulación en un sector o una actividad, en la que todos los implicados colaboran. Es el sistema que más se ha implementado en los sectores de telecomunicaciones y tecnología, por el ya comentado problema de lentitud en la regulación tradicional. Este sistema permite que el control permanezca dentro de las

instituciones del Estado y los diferentes actores socioeconómicos se impliquen en la solución⁶⁰⁸.

1.1.1 La autorregulación en los antecedentes de la normativa sobre protección de datos.

Desde la legislación de los años noventa del pasado siglo XX hasta el nuevo RGPD, se estableció una propuesta de códigos de conducta o de autorregulación de sectores de actividad que, bajo una normativa marco o limitativa, generaría una serie de normas autorreguladas, los denominados por la LOPD como códigos tipo o de conducta, que serían controlados por la AEPD o autoridad de Protección de datos personales. Los códigos de conducta desarrollan normas éticas (establecen una norma de conducta a seguir por los implicados en su desarrollo y cumplimiento) y normas técnicas (para hacer efectiva la protección de datos y su tratamiento por medio de procedimientos de seguridad). Como ha quedado expuesto, son los profesionales que tratan datos personales, tanto de forma lógica como física, los que deben respetar y hacer efectivo el derecho fundamental a la protección de datos personales y el resto de derechos que

⁶⁰⁸ El Ministerio del Interior alemán dedica una serie de documentos a la protección de datos personales, promoviendo sin duda alguna la autorregulación. Véase KRANIG, THOMAS ; EIFERT, MARTIN; "Selbstregulierung und wettbewerbsrechtliche Elemente im Datenschutz der Zukunft"].

https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Datenschutz/ergebnisse_papel_3_de.pdf?__blob=publicationFile El legislador debería adelantarse al futuro, en vez de arrastrar el pasado de los hechos. No sería posible una configuración económica globalizada a nivel mundial, en la que todos quieren participar por diferentes motivaciones (económicas, empresariales, culturales, progreso personal, intercambios, relaciones afectivas) sin una democrática participativa y estos dos factores no podrían unirse a un Estado que protegiera intereses nacionalistas, cerrados y anclados en un espacio territorial inexistente. El Estado debería ceder, de alguna manera, competencias que de hecho cede, como pueden ser la gestión técnica de los sistemas informáticos para la gestión de la Administración electrónica, que se manifestó más segura y más eficaz que la tradicional. A favor de una autorregulación regulada para la protección de datos, la propuesta de ROSSNAGEL, A., "Selbstregulierung im Datenschutz", *Medien, Ordnung und Innovation*, , 2006, pág. 298 y ss.

utilizan datos personales para su consecución o que no autorizan su uso para finalidades distintas de las que son obligadas por las AAPP (como se ha expuesto, derechos a la intimidad, a la imagen, al honor, a la libertad, a la protección de menores, entre otros afectados). La regulación internacional se caracterizó por una laxa intervención en internet que propició en todos estos años un máximo aumento de uso de servicios de telecomunicaciones interconectados entre sí (internet, radio, televisión, telefonía)⁶⁰⁹. Los Estados fueron conscientes de los riesgos, pero los ponderaron en función

⁶⁰⁹ Por ejemplo, se recuerda la Resolución de la Comisión sobre la Comunicación relativa a los contenidos ilícitos y nocivos en internet de 1997, en la cual se eligió preferiblemente el modelo de autorregulación eficaz ante la alternativa de formas de legislación represiva (DOCE C 150, de 19 de mayo de 1997, p. 38) Es un claro ejemplo de la política y decisiones de la UE respecto a los contenidos en internet. La Comisión no consideró necesario establecer un régimen sancionador en ese momento, pues debían ser definidos “cada nivel de responsabilidad” y establecidas las distinciones entre “el suministrador de acceso, el suministrador de servicios y el usuario” (...) “1. Proclama solemnemente que la libertad de expresión es y sigue siendo una exigencia absoluta de una sociedad democrática; 2. Subraya que toda persona tiene derecho a comunicar o recibir libremente información a través de cualquier medio de difusión, sin perjuicio de las limitaciones previstas en el artículo 8 y en el artículo 10, apartado 2 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales del Consejo de Europa; 3 . Recalca que los preocupantes fenómenos observados en Internet, a los que se debe hacer frente, no

deben prevalecer sobre la profunda revolución cultural hecha posible por Internet; 4. Apoya con decisión el desarrollo de los sistemas telemáticos en redes, se congratula por sus repercusiones culturales, económicas y sociales, y reconoce que la libre circulación de la información encuentra en ellos un medio sustancial de progreso; 5. Señala que los servicios de Internet, con sus posibilidades de comunicación interactiva, correo electrónico rápido y barato y multimedios, pueden beneficiar a amplios sectores de la población, incluidas las mujeres, y toma nota de que en varios Estados autoritarios y represivos los servicios de Internet, dada su posibilidad de anonimato, interactividad y rapidez, han desempeñado un papel importante en la comunicación entre personas perseguidas y otras víctimas con el resto del mundo;” Destaca además una distinción jurídica fundamental “que se ha de hacer entre contenido ilícito, que pertenece al ámbito de la ley, y contenido nocivo, que afecta a los menores y pertenece esencialmente al ámbito de la moral, esté canalizado por Internet o por otros medios de comunicación”. Otro ejemplo fue la Resolución sobre “Europa y la sociedad de la información. Recomendaciones al Consejo Europeo y sobre una comunicación de las Comunidades Europeas sobre Europa en marcha hacia la sociedad de la información. Plan de actuación” DOCE C 230, de 28 de octubre de 1996, Deci-

de los beneficios, y optaron por permitir una red de telecomunicaciones con mínimas restricciones de contenidos y de accesos y a favor de la autorregulación como sistema dentro de la UE para configurar un marco normativo⁶¹⁰. En esa línea se configuraron posteriores normas europeas y españolas, como se observa en la LSSI y en la actual LOPD. Pero el gran reto de la autorregulación en la normativa de protección de datos personales no se presenta dentro de la posibilidad normativa sino en el ámbito de la eficacia en su cumplimiento. La normativa autorregulada por las empresas tiene fuertes controversias en sus resultados actuales, pues lo deseable sería una mayor implicación en la defensa de los DDFF por parte de las empresas y una concienciación de los usuarios/titulares de DDFF sobre los derechos que deben defender y tener como ciertos. Una cultura anárquica propició la incompatibilidad del avance técnico, junto con un avance cultural, jurídico, de conciencia ciudadana, siendo ambos dispares. No se puede pretender que se protegiera lo que no se apreciaba, ni por las empresas, que dentro de su actividad económica debían limitarse dentro de un uso legítimo de los datos personales, ni por los titulares, que sólo veían en las redes de telecomunicaciones una forma más de establecer relaciones, entendiendo como tal el intercambio de comercio, la visualización de contenidos de todo tipo o el ocio. Ante la falta de eficacia, la normativa de la UE fomentó la responsabilidad directa de las empresas y de los profesionales operadores en las redes de telecomunicaciones, en la gestión de los riesgos que se relacionaban con su actividad a través de la autorregulación normativa, con el desarrollo de *normas técnicas* que garantizaran los derechos afectados por su actividad.

La situación de *dependencia de la técnica* fue lo que muy probablemente incitará al legislador a adoptar marcos de desarrollo de normas autorreguladas. El componente técnico de la protección de datos personales fue difícil de asumir conceptualmente en

sión nº 276/1999/CE del Parlamento Europeo y del Consejo, de 25 de enero de 1999 por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales, DOCE L 33, de 6 de febrero de 1999, p. 1

⁶¹⁰ Considerando P, junto con puntos 14, 28, 29, 36, entre otros de la Resolución de la Comisión sobre la Comunicación relativa a los contenidos ilícitos y nocivos en internet de 1997.

la normativa jurídica y cambió más rápidamente que las leyes estatales. Por otro lado, se propagó el éxito internacional de las normativas técnicas ISO, las cuales se promovieron debido a la eficacia generada por sus normas, al ser internacionalmente admitidas. Se recuerda que la norma autorregulada es siempre un complemento de las leyes estatales y una alternativa a la desregularización. Junto con estas garantías, los códigos de conducta o códigos tipo para la protección de datos personales contienen mecanismos de certificación del cumplimiento de su normativa –lo que se ha denominado *autorregulación declarativa*- y mecanismos de resolución extrajudicial de conflictos –también denominada *autorregulación resolutive* -por medio de sanciones- previsto en el contenido de sus códigos⁶¹¹.

1.1.2 La autorregulación en las relaciones internacionales empresariales.

El fenómeno de la protección de datos es global y las soluciones deben tener esa misma naturaleza para ser eficaces y efectivas. Las empresas deberían ser los entes impulsores de una regulación frente a los diferentes enfoques legislativos por medio de mecanismos de autorregulación internacional. Es lo que se denomina *interoperatividad*. Los Estados se fueron organizando en grupos regionales, por culturas o por conductas, pero en todos los casos los intereses comerciales que ofrecían las tecnologías de la información y las telecomunicaciones estaban ya en la realidad de los ciudadanos o querían estarlo.

En el modelo regional atlántico, los acuerdos se fueron realizando entre la UE y EEUU. El modelo autorregulatorio de protección de datos o de protección de la privacidad en EEUU se opondría, al menos en una primera apreciación, al modelo europeo, pero los

⁶¹¹ Véase a este respecto DARNACULLETA I GARDELLA, M., *Derecho administrativo y autorregulación: la autorregulación regulada*, Girona, 2002, pág. 462 y ss. Otro autor es LÓPEZ JIMÉNEZ, D., "La protección de datos de carácter personal en el ámbito de las redes sociales electrónicas. El valor de la autoregulación. ", *Anuario de la Facultad de Derecho*, nº 2, 2009, pág. 237-278. con tempranas propuestas para las redes sociales en materia de autorregulación.

diferentes gobiernos de ambos lados del Atlántico, a lo largo de los años, estuvieron acercando posiciones, pues se defendían intereses económicos importantes. Como se analizó en el epígrafe sobre TID (Transferencias Internacionales de Datos), el modelo de los EEUU no tendría una regulación gubernamental excesiva, pues se valoraría más por su sociedad el desarrollo de la economía con el firme convencimiento de que el mercado se autorregula por sí mismo dentro de la materia de protección de datos, a través de los consumidores, sus compras de bienes y servicios y su adscripción fidelizada a visualizaciones de formatos, a través de los medios de telecomunicación⁶¹². Es un hecho cierto que la protección de datos personales no se considera en EEUU un derecho fundamental como sí lo es en Europa, pero sus legisladores y ciudadanos considerarían el concepto de *privacy* como una parte integrante de sus valores, por lo que se tiene muy en cuenta por las empresas, en especial las que tienen una actividad

⁶¹² Se recuerda que sólo existen regulaciones sobre protección de datos personales en tres sectores de actividad, ya comentados, pero que se traen a este epígrafe como resumen y recordatorio: La denominada Privacy Act o Ley de Privacidad de 1974, evolución jurídica de la Freedom of information Act FOIA o ley de libertad de información de 1966, que, como se analizó, tiene muchos puntos de convergencia con el derecho europeo a la protección de datos personales. La Ley de portabilidad y responsabilidad de seguros de salud (Health Insurance Portability and Accountability Act -hipaa) de 1967, la Ley para la protección de la privacidad infantil en línea (Children's Online Privacy Protection Act -coppa) de 1998, y la Ley de transacciones de crédito equitativas y precisas (Fair and Accurate Credit Transactions Act -facta), de 2003. También existen regulaciones para el ejercicio del derecho de oposición del titular respecto a la utilización de sus datos con fines publicitarios como el *National Do Not Call Registry*, (registro para no ser objeto de llamadas de publicidad) previsto por la Ley de Telemarketing (*Telephone Consumer Protection Act of 1991*) y administrado por la Comisión Federal de Comercio (*Federal Trade Commission*), la Comisión Federal de Comunicaciones (*U.S. Federal Communications Commission*), y el Departamento de Justicia, además de diversas agencias gubernamentales de los Estados, según corresponda, y métodos de investigaciones, requerimientos y sanciones de carácter civil. Se aprecia también la diferencia entre ambos sistemas jurídicos en un ejemplo de elaboración de normas administrativas realizado por ARROYO JIMÉNEZ, L., "Participación electrónica y elaboración de normas administrativas en España y en los Estados Unidos de América", *Centro de estudios europeos Luis Ortega Álvarez. Universidad de Castilla-La Mancha.*, nº 1, 2016. Esta alusión es a título orientativo, no es una referencia, al formar parte de una ponencia y no estar permitida su alusión como referencia académica.

basada en Internet, y en la confianza de los consumidores mundiales, las cuales mostraron su interés por unificar criterios de actuación en cuanto a la protección de datos personales o *privacy*. Se recuerda en este punto la iniciativa de RALLO LOMBARTE con la mencionada *Propuesta conjunta para la protección de la privacidad en relación con el tratamiento de datos de carácter personal* en 2009 o también el acercamiento de las visiones europea y norteamericana con el *Sistema de Reglas Transfronterizas de Privacidad* para la consecución de un modelo de autorregulación y certificación (regional, entre EEUU y Europa, con el acuerdo Privacy SHIELD, reciente norma autorregulatoria con certificaciones y sellos de privacidad) que creó mecanismos de interoperabilidad entre los dos modelos de protección de datos. Se pueden destacar los siguientes conceptos dentro de la regulación establecida en el Privacy SHIELD⁶¹³. Por una parte, se observaría la voluntariedad en la autocertificación de las empresas estadounidenses, con el compromiso del cumplimiento de los principios previstos en la normativa europea; por otra, el cumplimiento de los requisitos de forma y de contenido de dicha normativa, y por último la sanción a las empresas que habiendo sido consideradas como certificadas, incumplan la norma autorreguladora, en especial frente a la protección de datos de los consumidores, considerado como una violación de la buena fe, expresión de la cultura norteamericana, en donde la confianza es una base fundamental del sistema jurídico. Las Autoridades estadounidenses en general (Administrativas, judiciales o de comercio) aplican el máximo rigor a los incumplimientos empresariales de la normativa autorregulada, considerados como desleales o

⁶¹³ Véase si es de interés el resumen en la web http://europa.eu/rapid/press-release_IP-16-2461_es.htm “El 2 de febrero de 2016, la Comisión Europea y el Gobierno de los Estados Unidos alcanzaron un acuerdo político sobre un nuevo marco para los intercambios transatlánticos de datos personales con fines comerciales: el Escudo de la privacidad UE-EEUU (IP/16/216). La Comisión presentó los textos del proyecto de decisión el 29 de febrero de 2016. Tras el dictamen del Grupo de Trabajo del Artículo 29 (autoridades de protección de datos) de 13 de abril y la Resolución del Parlamento Europeo de 26 de mayo, la Comisión culminó el procedimiento de adopción el 12 de julio de 2016”. Destaca en esta nota de prensa el resumen del nuevo acuerdo http://europa.eu/rapid/press-release_IP-16-2461_es.htm El texto completo se encuentra en español <http://www.boe.es/doue/2016/207/L00001-00112.pdf> Se recuerda lo aportado en otros epígrafes de este análisis, para no reiterar contenidos.

engañosos para los ciudadanos, pero no lo valorarían como una violación de DDFF, de hecho, se promueven soluciones de conflictos referidas al arbitraje y a los métodos empresariales para solventarlos. Es de lógica jurídica, que los Tribunales de los Estados miembros de la UE no perderían sus competencias ni su ámbito de aplicación en una normativa autorregulada, pues los problemas reales no se presentan en cuanto al ámbito de la definición normativa, sino en su congruencia con un nuevo supuesto real.

Otro instrumento de normas autorreguladas en EEUU a nivel internacional son las Reglas Corporativas Vinculantes o *Corporate Binding Rules (CBR)*. Se trata de normas internas empresariales (pueden considerarse códigos de conducta o códigos tipo) generadas por un grupo empresarial multinacional para establecer la gestión de la privacidad en el tratamiento de datos personales entre diferentes ubicaciones físicas (localizaciones en diferentes Estados), entre las que pueden existir diversas normativas sobre protección de datos personales o incluso, ninguna normativa. Se recuerda también lo que se trató en referencia a las TID. Las empresas desean acreditar que desarrollan suficientes garantías en el tratamiento de datos personales a través de las CBR. Las transferencias internacionales de datos hacia empresas que no pertenezcan al mismo grupo no tienen cobertura dentro de las CBR. Deben contar, además, con la conformidad de las Autoridades de control del Estado miembro de la UE correspondiente. Los beneficios de estas prácticas autorreguladas estriban en que serán habilitadas para realizar transferencias internacionales de datos entre ellas, se les permite armonizar sus prácticas de protección de datos, también prevenir riesgos derivados de las TID, exteriorizar las políticas de privacidad adoptadas por el grupo empresarial y armonizar las directrices de actuación para sus trabajadores y colaboradores externos en cuanto al tratamiento de datos personales⁶¹⁴.

⁶¹⁴ Como afirmó PIÑAR MAÑAS (exdirector de la AEPD) “Finalmente, el instrumento de las CBR se admitió como complemento del marco regulador.(...) Ése es, quizá, el futuro a seguir: potenciar y fomentar el juego entre regulación y autorregulación, revisando la teoría de las fuentes, dando paso a la regulación y reconocimiento de los códigos de conducta, pero dando asimismo la última palabra a las normas jurídicas, y en primer término a la Ley, sobre todo cuando (y este es nuestro caso) hablamos de un derecho fundamental, como es el derecho a la protección de datos, cuya definición y garantía no pue-

Un ejemplo de relaciones internacionales en materia de protección de datos personales y autorregulación lo representa la creación del sistema de reglas transfronterizas de privacidad conocido por sus siglas en inglés CBPRS (*Cross Border Privacy Rules System*)⁶¹⁵. Es un acuerdo de otro sector regional mundial en torno al Océano Pacífico, denominado en castellano Foro de Cooperación Económica Asia-Pacífico y conocido también por sus siglas en inglés APEC (*Asia-Pacific Economic Cooperation*)⁶¹⁶.

Los Estados miembros del APEC generaron el denominado *Marco de Privacidad*, que lo componen *nueve principios orientadores* y una *Guía de implementación de protección de datos personales*. Las bases del sistema se basan en la autoevaluación de las reglas aceptadas por los Estados miembros, la revisión de su cumplimiento, el reconocimiento de la certificación por un tercero o entidad certificadora y la resolución de controversias por medio de la voluntariedad. Se estipulan algunos requisitos de forma y de contenido a mantener por las empresas, no excluyendo la posibilidad de sanciones. El sistema de la CBPRS mantiene las regulaciones de los Estados miembros, no las modifica, más bien las complementa, pues no impone una regulación única, siendo un mo-

de dejarse en manos de la autorregulación, pero cuya efectividad depende en gran medida de instrumentos como los códigos de conducta." PIÑAR MAÑAS, J., "Códigos de conducta y espacio digital. Especial referencia a la protección de datos", *Códigos de conducta y actividad económica: una perspectiva jurídica*, Madrid, 2012, pág. 176-177. Se ha referenciado el libro del que este artículo forma parte, pues se encontraba en otra fuente desaparecida www.datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid, 2010, Nº 44.

⁶¹⁵ Véase si es de interés la web <http://www.cbprs.org/>

⁶¹⁶ Véase si es de interés la web <http://www.apec.org/> La APEC se creó en 1989 con la finalidad de consolidar el crecimiento y la prosperidad de los países del Pacífico, en asuntos relacionados con el intercambio comercial, la coordinación económica y cooperación interestatal. Los Estados que conforma la APEC no forman parte de un Tratado, se consideran un Foro. Las decisiones se toman por consenso y por declaraciones no vinculantes. La Secretaría General, con sede en Singapur, se encarga de coordinar su funcionamiento. En estos últimos meses se comentaron sus actividades por la existencia y vigencia del Acuerdo Transpacífico de Cooperación Económica o (*Trans-Pacific Partnership*), TPP; acuerdo de similares características que el ya mencionado Tratado entre EEUU y la UE de Asociación Transatlántica para el Comercio y la Inversión, TTIP por sus siglas en inglés (*Transatlantic Trade and Investment Partnership*)

delo de autorregulación regional con certificaciones de la propia organización. Permite una interrelación o interoperatividad entre los diferentes sistemas de protección de datos de los Estados miembros, posibilitando la coexistencia de las diversas culturas que lo conforman.

Las características de la autorregulación empresarial (voluntariedad, flexibilidad, adaptación, especialización, suplementariedad al sistema jurídico estatal) pueden ser siempre completadas por los procedimientos estatales y las instituciones o autoridades que cada Estado considere más convenientes para proteger a sus ciudadanos en materia de protección de datos personales.

1.2. Los códigos de conducta o códigos tipo.

No toda la normativa considerada autorregulada se transforma en códigos de conducta (las normas ISO, por ejemplo). Pero los códigos de conducta sí forman parte de lo que se considera norma autorregulada. Los códigos de conducta son normas elaboradas por asociaciones, colectivos u otros organismos para aplicar una forma deontológica (ética o basada en valores) de actuación en sus relaciones empresariales. No están exentos de polémica doctrinal. Apelar a la ética no siempre presenta normativas clarificadoras. La ética se desarrollaría entre aspectos subjetivos mientras que la regulación debe tener presente aspectos objetivos⁶¹⁷. Sin embargo, se sigue utilizando la

⁶¹⁷ Véase a este respecto la exposición de DE LA CUESTA RUTE, J., "La autorregulación como regulación jurídica.", *Ponencia presentada al I Congreso Internacional Códigos de Conducta. Mercado, Publicidad y Mercados Financieros*, nº , 2008. El autor no considera aceptable recurrir a la ética (lo considera explorable, pero no aceptable) pues entiende la ética desde una concepción realista donde "la autonomía del orden moral no puede significar otra cosa que no sea la imposibilidad de que ninguna instancia ajena al propio sujeto de la acción pueda obligarle a obrar de acuerdo a la norma moral; la autonomía personal no puede entenderse en el sentido de que esa norma sea fruto de la conciencia subjetiva. Definir a la regulación como autónoma solo expresa que las reglas reguladoras no proceden de los poderes públicos; la reconducción de la autorregulación al campo de la ética por ese simple motivo supo-

expresión *códigos de conducta* quizá con la pretensión de extender más ampliamente la vinculación de los implicados en la autorregulación.

La AEPD denomina a los códigos deontológicos o de conducta como códigos tipo, consistiendo su definición en un instrumento de autorregulación, entendiendo ésta como la capacidad de las organizaciones y entidades para regularse a sí mismas. Dentro del ámbito de la protección de datos de carácter personal la AEPD y la LOPD consideraron que esa capacidad está orientada a la adopción de reglas o estándares específicos para armonizar los tratamientos de datos efectuados por quienes se adhieran al código tipo o lo promuevan y a facilitar el ejercicio de los derechos de los afectados con una evidente mejora en el cumplimiento de la normativa sobre protección de datos personales. El artículo 32 LOPD estableció que mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que regulen las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la LOPD y sus normas de desarrollo.

Los códigos tipo adecuaron lo establecido en la LOPD y en su Reglamento a las particularidades de los tratamientos efectuados por quienes se adhirieron a los mismos. La naturaleza jurídica de estos instrumentos regulatorios sería de carácter voluntario en la adhesión y de vinculación de su contenido hacia las partes intervinientes. Se exigía su inscripción y depósito en el Registro General de Protección de Datos de la AEPD, sin perjuicio de su inscripción, cuando corresponda, en los Registros que fueran creados por las Comunidades Autónomas, de acuerdo con lo dispuesto en el artículo 41.2 LOPD. La AEPD publicitó los códigos tipo inscritos, preferentemente a través de me-

ne un reduccionismo inaceptable que injuria no sólo a la ética, sino incluso al derecho y, estoy por decir, que a la lógica y al sentido común.”

dios informáticos o telemáticos en su página web⁶¹⁸. El nuevo RGPD invita a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por la norma europea de protección de datos, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta pueden, en particular, establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento. Al elaborar un código de conducta, o al modificar o ampliar dicho código, las asociaciones y otros organismos que representan a categorías de responsables o encargados deben consultar a las partes interesadas, incluidos los interesados (titulares de datos, se supone, por la terminología del texto europeo) cuando sea posible, y tener en cuenta las consideraciones transmitidas y las opiniones manifestadas en respuesta a dichas consultas. A fin de aumentar la transparencia y el cumplimiento del RGPD, se *promueve la creación de mecanismos de certificación, sellos y marcas de protección de datos*, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes⁶¹⁹. Como puede apreciarse, el texto europeo emplea el vocablo *código de conducta*, mientras la LOPD y el Reglamento se expresan con el término *código tipo*. Será esta una de las cuestiones que se deberán resolver en un futuro próximo por el legislador o la AEPD.

La adhesión del responsable o del encargado del tratamiento de datos personales a un código de conducta o a un mecanismo de certificación aprobado por una Autoridad de protección de datos puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable o para mitigar las consecuencias de una san-

⁶¹⁸ Bajo el link https://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/index-ides-idphp.php se puede consultar esta documentación. En este momento los códigos publicados agrupan los sectores económicos sanitario, de gestión de cobros, de seguros del automóvil, de intermediación inmobiliaria, comercio y publicidad online, una sola universidad (Castilla-La Mancha) y una sola agrupación de entes locales, la de Entidades Locales de la Comunidad Autónoma del País Vasco.

⁶¹⁹ Considerandos 98,99, 100 y 148 RGPD, entre otras menciones. Artículos 24, 28, 32, o 35 RGPD

ción, por ello se considera como una propuesta muy importante a la que atender (artículo 24.3 RGPD y para las Transferencias Internacionales de Datos sin aprobación de la Autoridad de control artículo 46.2.e) RGPD, por ejemplo). Los códigos de conducta y las certificaciones se regulan específicamente en los artículos 40 a 43 RGPD.

1.3. La certificación para empresas.

La certificación en la gestión empresarial nació de una necesidad probatoria de calidad en sus procesos. La calidad se entiende como un conjunto de aptitudes que confieren suficiente seguridad y confianza para satisfacer unas determinadas necesidades explícitas o implícitas en una relación empresarial, bien entre empresas o bien entre éstas y otros operadores de una sociedad, como pueden ser consumidores y usuarios o AAPP⁶²⁰. La RAE define la calidad como propiedad o conjunto de propiedades inherentes a algo, que permiten juzgar su valor, y es sinónimo de buena calidad la superioridad o excelencia. La calidad se ha convertido en algo más que la descripción del grado de satisfacción que proporciona un producto o servicio para desarrollarse toda una cultura, una filosofía que rige los principios de la gestión de la organización en cualquier empresa con significación económica, como una constante en todos sus movimientos. Certificar se define como la emisión de un documento que confirme la com-

⁶²⁰ Estos caracteres expuestos como definición de la certificación forman parte de la norma ISO 8402, la cual pertenece a la normativa internacional ISO 9000. Otra definición puede ser “actividad de carácter voluntario que permite establecer la conformidad de una entidad (empresa, producto o persona) con los requisitos definidos en una determinada norma, mediante la emisión por parte de una tercera parte de un documento fiable que así lo demuestre” aportada por CHAMORRO MERA, ANTONIO ; MIRANDA GONZÁLEZ, FRANCISCO JAVIER ; RUBIO LACOB, SERGIO ;, “Clarificando el concepto de certificación. El caso español”, *Boletín económico de ICE, Información Comercial Española*, nº 2825, 2004, pág. 1001-1016. De los mismos autores véase también MIRANDA GONZÁLEZ, FRANCISCO JAVIER ; RUBIO LACOB, SERGIO ; CHAMORRO MERA, ANTONIO ;, *Introducción a la gestión de la calidad*, Madrid, 2007. Véase como interesante la web del Gobierno de España sobre certificación <http://www.minetad.gob.es/telecomunicaciones/es-ES/Servicios/Certificacion/Paginas/index.aspx>

pleta adhesión a unas normas (que suelen ser técnicas en el caso de las ISO, pero pueden ser de gestión o de procedimientos) de una persona, una empresa o un producto⁶²¹. Las certificaciones se han extendido en los últimos 20 años; de hecho, en el

⁶²¹ Las normas ISO (*International Standardization Organization*) tienen su antecedente en la normalización y nacieron a finales del siglo XIX, con la Revolución Industrial, ante la necesidad de una producción masiva de calidad. Una definición de normalización puede ser "la actividad propia a dar soluciones de aplicación repetitiva a problemas que provienen esencialmente de las esferas de la ciencia, de la técnica y de la economía, con vistas a la obtención del grado óptimo, en un contexto dado. Se manifiesta generalmente, por la elaboración, la publicación y la aplicación de normas. De manera concisa normalizar es simplificar, unificar y especificar con el fin de lograr la eficiencia y eficacia de la empresa." Realizada por ESCALERA ALMENDROS, CARLOS ; PASCUAL FAURA, MARCELO ;, "La normalización y certificación como ventaja competitiva para la empresa española", *Boletín económico de ICE, Información Comercial Española*, nº 2820, 2004, pág. 1001-1012. La primera Guerra Mundial (1914-1918) dio un impulso a la normalización ante la necesidad de abastecer a los ejércitos y reparar los armamentos a través de la industria privada, a la que se le exigía unas especificaciones de intercambiabilidad y ajustes precisos. La normalización limitó la diversidad antieconómica de componentes, piezas y suministros, y favoreciendo su intercambiabilidad, facilitando la producción en serie, la reparación y mantenimiento de los productos y servicios, así como facilitando las relaciones externas entre países que necesitan piezas estándares, y ofreciendo garantías de cumplimiento de requisitos del cliente. El 22 de diciembre de 1917, los ingenieros alemanes Naubaus y Hellmich, constituyeron el primer organismo dedicado a la normalización: NADI *Normenausschuß der Deutschen Industrie* (Comité de Normalización de la Industria Alemana). Este organismo comenzó a emitir normas bajo el acrónimo DIN (*Deutsche Industrie Norm* o Norma de la Industria Alemana). En 1926 el NADI cambió su denominación por DNA *Deutscher Normenausschuß* - (Comité de Normas Alemanas), que, si bien siguió emitiendo normas con el acrónimo DIN, estas pasaron a significar *Das Ist Norm* (esto es norma). En 1975, cambió su denominación por DIN *Deutsches Institut für Normung* (Instituto Alemán de Normalización). En los países industrializados se implementaron otros sistemas de normalización, por ejemplo, en 1919, Inglaterra constituyó la organización privada *British Standards Institution* (BSI) y en Francia, en 1918 se constituyó la Asociación Francesa de Normalización (AFNOR). En 1926 se creó en Londres la *International Federation of the National Standardizing Associations* (ISA). Esta organización internacional coordinó los diferentes organismos nacionales y nació con una vocación internacional. Después de la Segunda Guerra Mundial, en 1947 se creó la *International Organization for Standardization* - (ISO) Organización Internacional para la Normalización, como se conoce en este momento. Su sede internacional se encuentra en Ginebra y es un organismo dependiente de la ONU. La denominada familia de normas ISO tiene como máximo exponente la norma ISO 9000. Las certificaciones en ISO (Certificado de

ámbito empresarial se habla de la *era de las certificaciones*. Las certificaciones son exigidas y muy valoradas por las grandes corporaciones industriales, por las AAPP en cuanto a los contratos con terceros, y por los particulares como una garantía de servicio o de calidad. El auge de las certificaciones ha generado que no se limiten a su concepto estricto de calidad, ni sólo al sector industrial o de producción de bienes. En este momento se han desarrollado para otros sectores sociales, como recursos humanos o el medio ambiente⁶²². La certificación tiene un carácter voluntario, por eso se vincula a la autorregulación y a los códigos de conducta o códigos tipo. En esto se diferencia de la homologación, la cual tiene un carácter de obligatoriedad, de sometimiento de una actividad o resultado a la calificación de una Autoridad oficial, como una instancia que procede a la verificación del resultado o del proceso que se pretende homologar con las normas vigentes y autoriza a continuar con una actividad. Como ejemplo, las siglas o *marcado CE*, las cuales homologan un producto con los niveles de protección del interés colectivo impuesto por la normativa de la Unión Europea, lo que garantiza la libre circulación del producto en todos los Estados miembros⁶²³.

Las certificaciones pueden dividirse en dos categorías que se entrelazan en la realidad, atendiendo a la naturaleza del organismo normalizador/certificador. Por un la-

Conformidad) se expiden por entidades de verificación del cumplimiento de la normativa, controladas a su vez por organismos nacionales que regulan la actividad de certificación. Véase www.iso.org.

⁶²² Véase ESCANCIANO GARCÍA-MIRANDA, C., "Certificación ISO 9000 en España. Dificultades versus satisfacción empresarial", *Dirección y organización: Revista de dirección, organización y administración de empresas*, , nº 27, 2002, pág. 148-156.

⁶²³ El *marcado CE* es el proceso mediante el cual el fabricante o el importador informa a los usuarios y autoridades competentes de que el equipo comercializado cumple con la legislación de la UE y sus Directivas. Cuando un producto esté cubierto por varias Directivas que dispongan la colocación del marcado "CE", éste señalará que el producto cumple las disposiciones aplicables de todas esas Directivas de aplicación al mismo. Sin embargo, en caso de que una o varias autoricen al fabricante a elegir, durante un periodo transitorio, aplicarlas o no (en cuyo caso deberán cumplir la legislación nacional que esté vigente), el marcado "CE" se referirá únicamente a la conformidad con las disposiciones de aquellas Directivas que se hayan aplicado, y deberán indicarse en los documentos establecidos por los procedimientos de evaluación de la conformidad únicamente las referencias de tales Directivas. Véase www.marcado-ce.com

do, las *certificaciones de naturaleza pública*, en las cuales intervienen en el proceso las AAPP como certificadores. Por otro, las *certificaciones de naturaleza privada*, donde las funciones de certificación se realizan por empresas u organismos privados. Existen otras muchas categorías de certificaciones, como pueden ser en función del objeto de la certificación (sistemas de gestión de calidad, los más habituales; sistemas de prevención de riesgos laborales o recursos humanos ya mencionados, entre otras); en función de la empresa certificada o en función de la actividad económica. Resaltable es la certificación relativa al comercio electrónico y la gestión de tecnología, la gestión en seguridad y protección de datos (no específica para datos personales), ya mencionada, y otras que estén relacionadas. Se espera que en próximas fechas los organismos certificadores generen nuevos tipos de certificados para cumplir los mandatos y sugerencias del nuevo RGPD.

1.4. La identidad electrónica: la certificación, la firma digital, el certificado electrónico y el Documento Nacional de identidad electrónico (DNle).

La denominada certificación electrónica tiene relación con la firma electrónica, la firma digital, el DNle y el certificado electrónico, pero todos estos conceptos están sujetos a matizaciones.

La firma digital es un sistema que sirve para demostrar la autenticidad de un mensaje digital o de un documento electrónico. Prueba que el mensaje no fue alterado durante la transmisión y procede del remitente. Se utiliza especialmente en transmisiones bancarias o transacciones financieras.

La firma electrónica es un conjunto de datos relativos a la persona consignados electrónicamente, que pueden ser usados como medio de identificación del firmante, con el mismo valor probatorio que una firma manuscrita. La ley 59/2003, de 19 de diciembre, de firma electrónica, es su texto regulador. El remitente y el destinatario se reconocen mutuamente a través de la firma electrónica. Tiene valor legal mientras

que la firma digital no tiene esa presunción de veracidad. La firma electrónica es verificada por el denominado certificado electrónico emitido por una autoridad de certificación que garantiza la veracidad de la firma electrónica. Se utilizan, tanto el certificado electrónico como la firma electrónica, para las comunicaciones con las AAPP desde la puesta en marcha de la Administración electrónica. Cualquier ciudadano puede solicitar un certificado digital y una firma electrónica a través de las autoridades de certificación como puede ser el expedido por la Fábrica Nacional de Moneda y Timbre o FNMT, que resulta ser el más conocido y utilizado en España⁶²⁴. El departamento se denomina CERES (*CERTificación ESpañola*), y ofrece los certificados electrónicos reconocidos por la mayoría de las Administraciones Públicas. La Autoridad de certificación además de emitir certificados electrónicos de usuario, ofrece sus Servicios de Certificación a empresas y AAPP que garantizan los principios de Autenticación, Integridad, Confidencialidad y No Repudio (AICN) en las comunicaciones a través de redes abiertas. Existen también otras entidades que realizan estos servicios, como el Ministerio de Defensa, la Agencia Tributaria, la Dirección General de la Policía y la Guardia Civil, junto con alguna Agencia de Tecnología y Certificación Electrónica de Comunidades Autónomas.

Como se puede observar, la firma electrónica se convierte en un elemento identificador de la persona física o jurídica. En el caso de las personas físicas, se complementa con el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el Documen-

⁶²⁴ Según la AEPD “El certificado de usuario expedido por la Fábrica Nacional de Moneda y Timbre se basa en la versión 3 de la recomendación X.509 del ITU-T (*International Telecommunication Union*) Entre otros, contiene datos de identificación del usuario como el NIF o DNI., apellidos y nombre o razón social, número del certificado, fecha de concesión del certificado, fecha de expiración del certificado. clave pública, y firma digital de la Entidad certificadora. Este conjunto de datos junto con la clave privada almacenada en el navegador o servidor web del propietario del certificado permite garantizar que, utilizados por funciones de obtención de firmas digitales y cifrado, las conexiones entre navegadores y servidores Web se realizan con autenticidad, confidencialidad, integridad y no repudio de los mensajes intercambiados.”

https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/cuestiones_administracion/index-ides-idphp.php

to Nacional de Identidad y sus certificados de firma electrónica. La creación del Documento Nacional de Identidad electrónico (DNle) fue considerada una necesidad para otorgar identidad personal a los ciudadanos, para su personalización con autenticidad en la nueva Sociedad de la Información y los servicios públicos informatizados a través de las redes de comunicaciones, pero también constituyó un formidable impulso a los sistemas de informatización de la sociedad. Se considera que el DNle es la adaptación del tradicional documento de identidad a la nueva realidad de una sociedad interconectada por redes de comunicaciones. Ofrece la oportunidad a cada ciudadano de realizar múltiples gestiones con seguridad a través de medios telemáticos y garantizando la identidad de los participantes en la comunicación⁶²⁵.

Se deduce de todos estos elementos de la sociedad de la información que están en conexión íntima y precisa con la protección de datos personales. Con la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que consagra el derecho de éstos a comunicarse con las Administraciones por medios electrónicos se consagró la necesidad de respetar en cualquier caso el derecho fundamental a la protección de datos personales en las interconexiones con las AAPP, con una seguridad física de acceso a los sistemas informatizados, con mayor protección a los datos especialmente sensibles, estableciendo los supuestos en los que una cesión de datos es obligada o necesaria, sin olvidar el consentimiento del interesado cuando las AAPP recoge datos personales para ofrecer servicios no estrictamente administrativos como los de noticias y alertas o para la introducción de *cookies*, estableciendo también procesos para garantizar la calidad, la autenticidad y la integridad de los datos, elementos imprescindibles para que los ciudadanos tengan confianza en los servicios públicos. Los derechos del titular se mantienen ante las AAPP (se recuerda, acceso,

⁶²⁵ Véase como interesante la web del Gobierno de España <http://firmaelectronica.gob.es/Home/Ciudadanos/Firma-Electronica.html> en la que se explican en lenguaje muy inteligible todos los requisitos y aspectos de la firma electrónica. También el documento con definiciones sobre terminología de MINISTERIO DEL INTERIOR. COMISIÓN TÉCNICA DE APOYO A LA IMPLANTACIÓN DEL DNI ELECTRÓNICO, "DNI electrónico. Guía de referencia Básica.", *Grupo de trabajo de divulgación y comunicación. Policía Nacional.*, nº 1, 2016.

rectificación, cancelación y oposición, es también probable que se incorporen las normativas del nuevo RGPD)⁶²⁶.

En cuanto a un ámbito privado, es obvio que las empresas y organizaciones pueden exportar todos los derechos, las obligaciones y las experiencias de las AAPP a sus procesos de comunicación y de negocio, a través de los instrumentos de identificación propuestos. La cuestión que se puede plantear es ¿por qué no proliferan los usos de certificados y firma electrónica en el denominado *ciberespacio* o espacio de las telecomunicaciones por internet para todas las empresas y particulares que interactúan a través del mismo? Las entidades financieras, por ejemplo, sí han realizado avances en esta materia de identificación de usuarios, pero otras empresas se mantienen al margen. No progresan los cambios al respecto, por razones difíciles de comprender desde el punto de vista de los DDFF, pues normativa existe, mejorable o no, para servir de *norma abstracta* a una gestión autorregulada, pero sobre todo para el cumplimiento de la ley y el respeto a los DDFF.

2. La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI)

la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), tenía como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). También incorporó parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, de confor-

⁶²⁶ TRONCOSO REIGADA, A., "La administración electrónica y la protección de datos personales", *Revista jurídica de Castilla y León*, nº 16, 2008, pág. 31-113.

midad con lo establecido en ella, una acción de cesación contra las conductas que contravengan lo dispuesto en esta Ley⁶²⁷.

Frente a las ventajas de la denominada sociedad de la información, la LSSI presentó una serie de inconvenientes o de incertidumbres jurídicas que era preciso establecer en un marco jurídico adecuado, que generase en todos los actores intervinientes la confianza necesaria dentro del nuevo espacio no territorial⁶²⁸. La citada norma parte de un concepto amplio de *servicios de la sociedad de la información*, que comprende la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio, como el que efectúan los periódicos o revistas que pueden encontrarse en la red, las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio, por ejemplo), siempre que represente una actividad económica para el prestador de los servicios ofrecidos *online*. Los aludidos

⁶²⁷ La LSSI no estuvo exenta de controversias legislativas, como en otras ocasiones. Véase a este respecto JIMENA QUESADA, L., "La técnica legislativa y otros aspectos constitucionales relativos a la Ley de servicios de la sociedad de la información y de comercio electrónico", *Revista de Derecho*, nº 2, 2002. El autor estableció un análisis general sobre la LSSI destacando que "la Ley produce una cierta parcelación normativa en lo que afecta al conjunto de ordenamiento estatal, lo que no queda justificado por el hecho de que el propio Legislador haya sido consciente de dicha circunstancia, como puede leerse expresamente en la Exposición de Motivos." (...) "es verdad que resulta complicado dotar de unidad a la normativa estatal en este ámbito de la sociedad de la información y del comercio electrónico, presentándose difícil, por ejemplo, la elaboración de un texto refundido en la materia, puesto que esa misma parcelación normativa se produce en el ámbito del Derecho Comunitario, que es precisamente objeto de transposición al ámbito interno de acuerdo con las pautas y plazos marcados por la Unión Europea."

⁶²⁸ Entre otras, se recuerda la expansión de las redes de telecomunicaciones, mejora de la eficiencia empresarial, el incremento de las posibilidades de elección de los usuarios y la aparición de nuevas fuentes de empleo de y a través de ellas todo tipo de intercambios informativos o culturales.

servicios se ofrecen por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades descritas, incluido el comercio electrónico⁶²⁹.

Como se puede apreciar, existe regulación. Se aplica desde un punto de vista subjetivo a los prestadores de servicios establecidos en España, y la LSSI entiende por establecimiento el lugar desde el que se dirige y gestiona una actividad económica, en concordancia con el concepto de domicilio fiscal recogido en las normas tributarias españolas y que resulta compatible con la noción material de establecimiento predicada hasta ahora por la normativa de la UE. El lugar del establecimiento es un asunto muy importante para la efectividad del Derecho en cuestiones de telecomunicaciones, como ya se analizó en otros epígrafes, porque es un elemento esencial al depender del lugar del establecimiento (jurídico) el ámbito de aplicación, no sólo de esta Ley, sino de todas las demás disposiciones del ordenamiento español que les sean aplicables, en función de la actividad que desarrollen. Asimismo, el lugar de establecimiento del prestador determina la ley y las autoridades competentes para el control de su cumplimiento, de acuerdo con el principio de la aplicación de la ley del país de origen que inspiró la Directiva 2000/31/CE. La Ley resultó hasta ahora igualmente aplicable a quienes sin ser residentes en España prestaran servicios de la sociedad de la información a través de un *establecimiento permanente* situado en territorio español, y la aplicación de la LSSI en este caso es parcial, pues sólo tiene efectos a los servicios que se presten desde España. Se estableció igualmente como principio la libre prestación en España de servicios de la sociedad de la información para países del EEE (se recuerda, Espacio Económico Europeo) y sólo se podían restringir en los supuestos previstos en la Directiva 2000/31/CE, que consistían en la producción de un daño o

⁶²⁹ ADSUARA VARELA, B., "Algunas consideraciones previas sobre el comercio electrónico", *Información Comercial Española, ICE: Revista de economía*, , nº 813, 2004, pág. 15-26. El artículo es aclaratorio respecto a los contenidos y definiciones propuestas en la LSSI. Para el autor internet y las redes de telecomunicaciones son canales de promoción empresarial que alcanzan a más número de potenciales interesados, pero los derechos aplicables, son, en esencia, los mismos que para las comunicaciones tradicionales.

peligro grave contra ciertos valores fundamentales como el orden público, la salud pública o la protección de los menores. Igualmente, podría restringirse la prestación de servicios provenientes de los Estados miembros cuando afecten a alguna de las materias excluidas del principio de país de origen, que la Ley concretó en su artículo 3, y se incumplan las disposiciones de la normativa española que, en su caso, resultara aplicable a las mismas. La Directiva 2000/31/Ce estableció el principio denominado como *de país de origen* para la aplicación de su normativa, considerado por la doctrina como un mecanismo para garantizar la libertad de prestación de servicios de la sociedad de la información en el EEE.

La LSSI reguló un aspecto importante tanto para el usuario como para la protección de los derechos en general, cual fue la anotación del nombre o nombres de dominio de Internet que correspondan al prestador de servicios en el registro público en que, en su caso, dicho prestador conste inscrito para la adquisición de personalidad jurídica o a los solos efectos de publicidad, con el fin de garantizar que la vinculación entre el prestador, su *establecimiento* físico y su *establecimiento* o localización en la red de telecomunicaciones, que proporcionaría su dirección de Internet, fuera fácilmente accesible para los ciudadanos y las AAPP. Esta es la razón por la que todas las empresas con ámbito de actuación en el EEE están inscritas en un registro público, generalmente será el Registro Mercantil, pues su actividad está sujeta sobre todo a las leyes impositivas fiscales de los Estados miembros correspondientes y a otras leyes muy importantes, como son las de pago de cotizaciones sociales, cumplimiento de normativas sobre productos o medioambiente⁶³⁰.

⁶³⁰ La LSSI tiene incidencia directa en los usuarios/consumidores y en las empresas/operadores mercantiles dentro y fuera de internet. Reguló conductas que no eran muy conocidas en su momento y que ahora mismo, salvo casos muy concretos, se ignoran. El particular no suele recurrir a las leyes si no se siente vulnerado, es infrecuente conocer la ley antes de contratar. La empresa también ignora buena parte de las regulaciones que le son aplicables a su actividad, que aun siendo en el ciberespacio, sigue sometida a multitud de regulaciones, entre otras la Ley 26/1984, de 19 de julio, General de Defensa de los Consumidores y Usuarios; la Ley 34/1988, de 11 de noviembre, General de Publicidad; la Ley 26/1991, de 21 de noviembre, sobre contratos celebrados fuera de establecimientos mercantiles, la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista; la Ley 7/1998, de 13 de abril, so-

Otro importante aspecto que estableció la LSSI fueron las obligaciones y responsabilidades de los prestadores de servicios que realicen actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en la red. Los prestadores de estas actividades tendrían un deber de colaboración para impedir que determinados servicios o contenidos ilícitos se sigan divulgando. Las responsabilidades que pueden derivar del incumplimiento de estas normas no son sólo de orden administrativo, sino de tipo civil o penal, según los bienes jurídicos afectados y las normas que resulten aplicables⁶³¹.

Los destinatarios de servicios fueron especialmente protegidos por la LSSI, de forma que éstos pudieran gozar de garantías suficientes a la hora de contratar un servicio o bien por Internet⁶³². Con esta finalidad, la Ley impuso a los prestadores de servicios la obligación de facilitar el acceso a sus datos de identificación a cuantos visiten su sitio en Internet; la de informar a los destinatarios sobre los precios que apliquen a sus servicios y la de permitir a éstos visualizar, imprimir y archivar las condiciones generales a que se sometía, si procedía, el posible contrato. Cuando la contratación se

bre Condiciones Generales de la Contratación; y las mencionadas Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal o la Ley 59/2003, de 19 de diciembre de firma electrónica. Véase VELEIRO REBOREDO, B., "Incidencia de la normativa en las empresas que prestan sus servicios a través de Internet", *Boletín económico de ICE, Información Comercial Española*, nº 2812, 2004, pág. 1000-1016. Véase también como interesante la página web del Gobierno de España para la LSSI <http://www.lssi.gob.es/empresas/Paginas/empresas.aspx>

⁶³¹ Véase los comentarios a la LSSI desde la perspectiva del Derecho internacional privado en CASTELLANOS RUIZ, E., "Las normas de Derecho Internacional Privado sobre consumidores en la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico.", *Cuadernos de derecho transnacional*, nº 2, 2009, pág. 134-159. Comentario de arts. 26 y 29 de la LSSI relativas a la Ley aplicable a los contratos electrónicos y la determinación del lugar de celebración de los contratos online.

⁶³² El acceso a internet como servicio universal fue un elemento en disputa durante un tiempo, pues no se podía garantizar técnicamente el ejercicio del derecho de acceso a todas las telecomunicaciones. Véase REVUELTA PÉREZ, I., "Incidencia de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico en el servicio universal de telecomunicaciones. La inclusión del acceso a internet.", *Revista de Derecho*, nº 2, 2003.

efectuaba con consumidores, el prestador de servicios debería, además, guiarles durante el proceso de contratación, indicándoles los pasos que han de dar y la forma de corregir posibles errores en la introducción de datos, y confirmar la aceptación realizada una vez recibida.

En lo referente a las comunicaciones comerciales (publicidad o *banners*), la Ley estableció que éstas debían identificarse como tales, y prohibió su envío por correo electrónico u otras vías de comunicación electrónica equivalente, salvo que el destinatario hubiera prestado su consentimiento para recibir publicidad.

Por otro lado, la LSSI favoreció desde su normativa la contratación de bienes y servicios por vía electrónica, estableciendo el denominado *principio espiritualista* que rige la perfección de los contratos en el Derecho español, la validez y eficacia del consentimiento prestado por vía electrónica. Estableció que no era necesaria la admisión expresa de esta técnica para que el contrato surta efecto entre las partes, y aseguró la equivalencia entre los documentos en soporte papel y los documentos electrónicos a efectos del cumplimiento del requisito de *forma escrita* que figura en diversas leyes de nuestro ordenamiento español. Se modificaron en su contenido los artículos 1.262 del Código Civil y 54 del Código de Comercio en la Disposición adicional cuarta de la LSSI, unificando los criterios dispares que existían en referencia al momento y lugar de la celebración de los contratos, con una solución única que resultó válida para otros tipos de contratos celebrados a distancia, cuestión sumamente trascendente para la contratación electrónica. Se excluyeron de esta regulación lo relativo a medicamentos y productos sanitarios, que se sometieron a una norma específica, por su especial naturaleza.

Muy interesante resulta la promoción de los códigos de conducta sobre las materias reguladas en la LSSI, pues se consideró que son un instrumento de autorregulación especialmente apto para adaptar los diversos preceptos de la LSSI a las características específicas de cada sector empresarial. La LSSI recurrió igualmente al arbitraje y a los procedimientos alternativos de resolución de conflictos (mediación) como formas de

dirimir las disputas o demandas en la contratación electrónica⁶³³. Se perseguía por el legislador europeo garantizar el acceso a las reclamaciones contra operadores comerciales por procedimientos sencillos y por medios telemáticos (*online*) sin que los tradicionales medios de resolución de conflictos, el acceso a los Tribunales, fueran restringido⁶³⁴. La LSSI establece un régimen sancionador que se presume eficaz con la intención de disuadir a los prestadores de servicios del incumplimiento de la Ley. La competencia sancionadora corresponde a diferentes Organismos Públicos⁶³⁵. Por últi-

⁶³³ Esta cuestión se encuentra relacionada con la Directiva 2013/11/UE relativa a la resolución alternativa de litigios en materia de consumo por la que se modifica el Reglamento 2006/2004 y la Directiva 2009/22/CE y también con el Reglamento UE 524/2013 sobre resolución de litigios en línea, ambas regulaciones publicadas en el Diario oficial de la UE el 18 de junio de 2013. Véase, entre otros, RALUCA STROIE, I., "Alternativas a la resolución de conflictos en materia de consumo: la Directiva 2013/11/UE del parlamento europeo y del consejo y el reglamento (UE) 524/2013 del Parlamento europeo y del Consejo, de 21 de mayo de 2013", *Publicaciones jurídicas. Universidad de Castilla-La Mancha. CESCO. Centro de Estudios de consumo.*, nº 1, 2013. Los litigios en materia de consumo no se habían canalizado adecuadamente por la vía de la mediación o del arbitraje, con sistemas heterogéneos en los diferentes Estados de la UE. Para tramitar los asuntos en litigio, se recomienda y potencia el uso de medios electrónicos. Véase como interesante la página web sobre tramitación de conflictos online <https://webgate.ec.europa.eu/odr/main/?event=main.home.show#legislation-modal> Esta página web ha sido creada por la UE "para ayudar a los consumidores no satisfechos. Permite presentar reclamaciones sobre productos o servicios adquiridos online y encontrar un tercero neutral (*organismo de resolución de litigios*) que las tramite. En algunos países también se permite que las empresas presenten reclamaciones contra consumidores. Los empresarios y profesionales de esos países pueden utilizar este sistema para hacerlo. Todos los organismos de resolución que aparecen en esta web han sido verificados para garantizar que cumplen nuestras normas y están registrados ante las autoridades nacionales." Será realmente un avance la resolución efectiva de conflictos online para consumo (OCR), como describe recientemente GARCÍA MONTORO, L., "El sueño de la resolución online de conflictos de consumo, cerca de convertirse en una realidad.", *Publicaciones jurídicas. Universidad de Castilla-La Mancha. CESCO. Centro de estudios de consumo.*, nº 1, 2016.

⁶³⁴ Véase a este respecto GONZÁLEZ GRANDA, P., "Protección judicial de consumidores y usuarios en el ámbito del comercio electrónico", *Indret: Revista para el Análisis del Derecho*, nº 4, 2007.

⁶³⁵ Artículo 43 LSSI: La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, al Ministro de Industria, Energía y Turismo, y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la

mo, un detalle interesante, pues la LSSI formula una normativa para que las personas con discapacidad accedan a los medios de telecomunicaciones en red (internet).

El derecho fundamental a la protección de datos personales se menciona en el artículo 1 como elemento a tener en consideración dentro de la regulación de la LSSI. Así mismo, el artículo 8.1 LSSI, alude al ordenamiento jurídico en general para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando éstos pudieran resultar afectados, es decir, derechos constitucionalmente protegidos, por lo que en todos los casos en los que la Constitución y las leyes reguladoras de los respectivos derechos y libertades así lo prevean de forma excluyente, sólo la autoridad judicial competente podrá adoptar las medidas previstas en el artículo 8 LSSI (junto con otros, en esa misma línea protectora de DDFF), en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información (se entiende que de expresión también). En el caso de las comunicaciones comerciales por vía electrónica (artículo 19 LSSI) se respetará siempre las disposiciones de la LOPD y el Reglamento, en especial para la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales, además de solicitar su consentimiento según dicha regulación de protección de datos personales.

El RGPD consideró que la normativa establecida en su articulado debería entenderse sin perjuicio de la aplicación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, en particular de las normas en materia de responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15. El objetivo de dicha Directiva fue contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los

Información. No obstante, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley.

Estados miembros, y se recuerda que la LSSI fue la Ley española que desarrolló en el Derecho español esa Directiva, como se ha expuesto⁶³⁶.

3. La autorregulación y las empresas.

Teniendo en cuenta el debate actual en el ámbito empresarial sobre la protección de datos de carácter personal y la normativa para su desarrollo, existen posibilidades bien asumidas, desarrolladas y comprobadas de autorregulación, entendiendo ésta como asunción de una normativa voluntariamente acordada por una empresa, un grupo de empresas o actividad profesional. La propuesta de un *código de conducta de la economía* como una herramienta efectiva para una mejor protección de datos tiene como premisa que la ley, por sí misma, no puede aportar una solución a cada caso planteado por la realidad, y aún menos eficazmente puede regularse cada situación concebible. Si se consideraran las reglas de la protección de datos como *normas abstractas*, se permitiría el camino hacia normas vinculantes y eficaces realizadas a través de un código de conducta, lo que permitiría soluciones (resultados) equilibradas y legales para casos más concretos, pasando desde lo abstracto (de la norma) a lo concreto (la realidad) sin derivar en una normativa extenuante y poco eficaz⁶³⁷. El legislador está obligado a proteger los DDFF de los ciudadanos. En la sociedad de la información y la comunicación los límites a esta función se presentan en la velocidad de la innovación tecnológica y el carácter transfronterizo de las relaciones, entre otros límites que no son asumibles por las técnicas tradicionales del poder legislativo, sino

⁶³⁶ Considerando 21 y artículo 2.4. RGPD.

⁶³⁷ Los DDFF estarían delimitados internamente y limitados externamente, en palabras de MAGDALENO ALEGRÍA, A., *Los límites de las libertades de expresión e información en el Estado social y democrático de Derecho.*, Madrid, 2006, pág. 114. “Se identifica la delimitación de un derecho fundamental por parte de la Constitución como la definición inicial de las facultades que lo integran. Por el contrario, cuando se limita un derecho fundamental se hace desde el exterior al mismo, o se restringen sus iniciales facultades con el objeto de compatibilizarlo con los derechos de los demás o de asegurar la protección de otros bienes o valores constitucionalmente reconocidos.”

simplemente son límites de la realidad (limitación externa). Las regulaciones tradicionales coexisten en muchas ocasiones con zonas grises de legislaciones internacionales y nacionales, lo cual aporta aún más inseguridad jurídica a la protección de los datos personales y a los DDFF en general. Por lo tanto, lo que el legislador comenzó a vislumbrar con claridad es que resultaban necesarios diferentes enfoques regulatorios, combinados por diversos actores del escenario social, tanto empresariales como de los ciudadanos. Se hablaría entonces de una *co-regulación*, para el caso en que empresas y ciudadanos optaran por regular una actividad, o también de una autorregulación, para el caso en que una empresa, grupos de empresas o profesiones, opten por generar una normativa técnica y deontológica (de conducta) en la que los DDFF tengan su debida importancia. Sobre la base de un mandato legal, en ambas situaciones descritas se pueden generar rápidamente normativas que sean actuales, flexibles, con respuestas a nuevos planteamientos y a nuevos retos⁶³⁸.

Por otra parte, se conseguiría una mayor confianza para los medios de comunicación y los sistemas informatizados, los cuales parecieron verse inmersos en una serie de escándalos sobre el uso de datos personales, sin que la reacción del legislador constituyera una respuesta clara y eficaz. La lentitud de los procedimientos legislativos frente a la rapidez mediante la que se producen los cambios tecnológicos conlleva una normativa incapaz de proteger de manera eficaz los datos personales. La única forma de invertir el proceso es frenar la innovación tecnológica y su influencia social, lo que es prácticamente imposible de revertir o de controlar, pues se produjeron en los años transcurridos suficientes cambios sociales, de usos, de conductas, para que tal come-

⁶³⁸ En Alemania se desarrollaron experiencias con un resultado positivo en la protección a la infancia y a la juventud en los medios de comunicación, la protección del medio ambiente o la seguridad de los productos industriales. En cuestiones de protección de datos personales véase BODENSCHATZ, N., *Der europäische Datenschutzstandard*, Frankfurt am Main, 2010, pág. 124 y ss. La autora destacó la importancia de la seguridad de los datos en general junto con la protección de los datos personales, presentándolo como una oportunidad para que las empresas mejoraran su nivel de aceptación comercial y social a través de la autorregulación. En el año 2010 ya existía el proyecto de la UE para la creación de una certificación o sello europeo de protección de datos, denominado *EuropPriSe* (*European Privacy Seal*) En este sentido, las ideas de SPINDLER, G. (Catedrático de la Universidad de Göttingen).

tido sea imposible o la sociedad se enfrentaría a una crisis político-económica sin precedentes.

La posible solución se encontraría en la promoción de normas claras, específicas, concretas y admitidas por un amplio espectro social, en las que los DDFF sean respetados con el convencimiento generalizado de que son normas positivas para todas las partes involucradas en su protección (*principio de transparencia*). Sobre esta base normativa, se podrían desarrollar otras reglas de conducta vinculantes para las partes que las elaboren o que se adhieran a las ya generadas por otros. En todas ellas, *la voluntad de las partes se convierte en el eje central de la eficacia normativa y, por ende, de la legalidad*. Se puede hablar en este caso de *marcos normativos abstractos que se concretan en instrumentos de reglas específicas*, las cuales pueden ser mucho más rápidas en su adaptación que la normativa legal, a través de normas del poder legislativo, y tendrán mejores respuestas ante los retos, los riesgos y las posibles aportaciones sociales del futuro, que siempre está por determinar. Se ahorraría también el Estado de derecho continuas modificaciones legales, que consumen tiempo, medios y recursos sin fin, para terminar obsoletas antes de su entrada en vigor. Como consecuencia de todo ello, el ciudadano tendría una respuesta a su necesidad de confianza en el sistema democrático, una mayor seguridad, jurídica, de conducta de los actores económicos, políticos y sociales. La seguridad y la confianza son la base de la calidad, tanto de servicios como de productos, por lo que el avance social se fortalecería desde estas actuaciones.

No se trata tanto de generar un nuevo sistema jurídico o nuevos DDFF. Se trata más bien de un nuevo enfoque de la normativa actual. La norma debe, sin duda, adaptarse a los nuevos cambios, pero los valores básicos de una civilización no varían tanto en el tiempo y son aceptados por todas las partes mayoritariamente. Además, en el ciberespacio y en la realidad material rigen los mismos DDFF, la norma es sólo la forma de los DDFF en diferentes situaciones, que quizá para el ciberespacio necesitan de adaptación. Un ejemplo, la validez civil de una firma personal como prueba de aceptación, y como ejercicio de la libertad personal. En el ciberespacio o mundo virtual no es posible escribir con ningún medio conocido, por lo que se creó la firma digital para au-

tentificar la personalidad del sujeto que realiza un acto jurídico, como puede ser una compraventa online, con aceptación de eficacia jurídica por todas las partes intervinientes.

La autorregulación, los códigos de conducta (y si se quiere añadir, también la co-regulación) pueden ser una alternativa a la regulación normativa para los casos concretos en los que la seguridad de los servicios informatizados y de las comunicaciones por internet son una prioridad para los DDFF de los titulares de datos personales. Sería una forma de *autolimitación*. Tanto la seguridad informática como las comunicaciones están en manos de profesionales que, en general, no tienen conocimientos jurídicos, pero cuyas actividades afectan a los DDFF de las personas, en especial al derecho a la protección de datos personales. Como se vio en la denominada Sentencia *Google*, la solución a la protección de los DDFF de un grupo de ciudadanos pasaba por una solución técnica dentro de los motores de búsqueda, pero, además, se debían tener en cuenta los derechos de otros que podían verse afectados por las decisiones de la empresa demandada. También las empresas de información periodística mostraron su preocupación ante lo que consideraron una situación inaceptable entre el derecho a la libre expresión e información y el derecho a la protección de datos personales, ambos fundamentales. Si se consiguiera una regulación pactada entre empresas del sector de la información para proteger los DDFF de las personas, en especial su derecho a la protección de datos, las situaciones como la propuesta en la Sentencia *Google* quedaría solucionada antes de que tan siquiera apareciera, pues los datos de nombres de personas identificables quedarían eliminados de los buscadores con el paso de cierto tiempo, como sucede con los nombres en las Resoluciones y Sentencias judiciales. Las reglas abstractas sobre protección de datos permitirían este tipo de acuerdos entre las partes implicadas. Otro ejemplo pudiera ser la seguridad de los datos en general, por la que todos los datos deben ser protegidos de la pérdida o del acceso por terceros para su protección, en función de la evolución tecnológica; tales afirmaciones fueron realizadas por diferentes regulaciones, no sólo por la normativa sobre protección de datos personales (las denominadas normas ISO 27000, ya comentadas). El estado de las tecnologías y su evolución no se pueden circunscribir en una

concreta ley, pues no sería realista intentarlo tan siquiera. En cambio, sí se han producido buenos resultados en la aplicación a la seguridad de los datos (en general, no sólo de carácter personal) de la normativa ISO, por ejemplo, la cual se adaptaba muy rápidamente a las necesidades empresariales, concretando la normativa legal al mismo tiempo que precisaba los procedimientos necesarios para garantizar el objetivo de la seguridad en los sistemas informatizados. El cumplimiento voluntario de una normativa abstracta para concretar las necesidades y la evolución técnica, se muestra como una forma de cumplir la legalidad eficientemente en la realidad física. Además, se debe añadir que la auténtica protección de datos siempre se basará en técnicas de administración de accesos a los datos, tanto físicas como lógicas. Será el acceso por los usuarios que tratan datos de carácter personal los que generen tanto la seguridad como el riesgo para los sistemas, y, por tanto, para la seguridad de los datos, personales o no personales⁶³⁹

3.1. La autorregulación como oportunidad y como riesgo.

Los riesgos de la autorregulación o de los códigos de conducta estriban en la disposición de las partes hacia el cumplimiento voluntario de la norma que ellos mismos se han otorgado. Existirían diferentes posiciones en cuanto a su resultado. A favor de la autorregulación de las empresas se expone como primer punto que contarían en este asunto una *motivación de mercado*, a través de los beneficios que les puede suponer una gestión acorde con el respeto a las personas, lo que significa respeto a los DDFF, transferidos a los ciudadanos que adquieren sus productos y servicios como un factor positivo. Una conducta empresarial que sea negativa para un sector social debería tener como resultado una pérdida de mercado. Esta posición se basa en la premisa de

⁶³⁹ Para una empresa su patrimonio se encuentra en los datos que son tratados en sus sistemas informáticos. Desde datos de marketing y ventas, a investigación y desarrollo, procesos industriales, producción, proveedores, finanzas, entre otros ejemplos. Todo ello debe estar debidamente administrado y controlado, no sirven otros métodos que los técnicos de seguridad de datos.

la influencia social en el mercado. Aunque las empresas son operadores cuyo fin es el beneficio económico, se ha demostrado también que la sociedad puede y debe influir en sus resultados de negocio a través de la compra de productos o servicios más acordes con lo que consideren los consumidores que les reportaría un beneficio (social) al conjunto de los ciudadanos⁶⁴⁰. En otra vertiente más crítica, se analizaría la actual situación económica desde una perspectiva negativa para una buena parte de la sociedad, la cual estaría más pendiente de los precios y de su exigua capacidad de adquisición de productos que de la calidad en la gestión empresarial, al igual que buena parte de la sociedad no quiere informarse, no tiene una motivación hacia el bienestar social, tiende al egoísmo utilitarista sin pensar en su influencia⁶⁴¹. Para este sector social, la norma autorregulada y actualizada para la eficacia de los derechos, pasa

⁶⁴⁰ Ejemplos para ilustrar esta afirmación se encuentran en la Ley de protección a menores ante producciones audiovisuales, redes sociales y ventas de productos; en la regulación publicitaria (Autocontrol en España); en la protección a personas con discapacidad para proteger su vulnerabilidad, productos éticos como la banca cívica o ética, certificados de *comercio justo*, entre otros ejemplos. Se consiguió que las empresas, a su vez, ganen en prestigio y que las AAPP no las tengan constantemente envueltas en procedimientos administrativos o judiciales, costosos y largos, que vulnera su imagen ante los ciudadanos, consumidores de sus productos y servicios. Ejemplo: caso “*el Cuco*”, en el que fue entrevistado el cómplice del asesinato de una joven. El escándalo social derivó en una campaña para no comprar los productos que se anunciaban en el programa. Las empresas anunciantes promovieron el cierre del formato televisivo ante la caída de ventas.

⁶⁴¹ La compra de productos baratos, producidos en situaciones y condiciones inhumanas no se publica con suficiente asiduidad. En las ocasiones que se produjo (por ejemplo, asunto “*Nike*”, denunciado por *Safe the children* como empresa de explotación infantil) tuvo una rotunda respuesta que obligó a rectificar, en todo o en parte, a las empresas. Véase como interesante el artículo de Clemente Barahona, “*La globalización del abuso*” en la página web de la Universidad de Santiago de Compostela donde se proponen casos reales sobre esta temática <http://firgoa.usc.es/drupal/node/26786> Se aporta también a título de comentario la publicación moda.es con el título “*Los códigos deontológicos de los gigantes de la moda*” <file:///D:/Downloads/los-codigos-deo.pdf> en cuyo texto se expone que “la subcontratación en países del Tercer Mundo es una práctica habitual en la moda, pero tiene un riesgo: los abusos que puedan cometer los proveedores y por los que *debe responder la marca*. Para evitar que las malas prácticas de sus proveedores les perjudiquen, las compañías han elaborado en esta última década sus propios códigos de conducta, documentos que recogen normas éticas para sus proveedores.” Se añade a estas publicaciones la certeza de la influencia de las redes sociales para desarrollar conductas.

completamente inadvertida. Aunque esta realidad existe, no por ello se deberían relajar las iniciativas que busquen una mejora social. Muy al contrario. Se deberían extender aún más por el legislador, hasta llegar a niveles de suficiente conocimiento general para que formaran parte de la convivencia.

Jurídicamente, el éxito de las normativas autorreguladas residiría en una norma abstracta clara, definida, para generar normas específicas, concretas y flexibles, como se ha expuesto. Las empresas que realizaran códigos de conducta o normas de autorregulación, con sellos de confianza, serían identificadas por la sociedad como fiables y gozarían de una posición preferente en el mercado. Es cierto que conseguir un acuerdo de todos los actores en un sector de mercado se puede convertir en una tarea ardua, pero no serían menos ciertos los beneficios económicos que se lograrían si un amplio espectro de empresas consiguiera autorregularse respecto al cumplimiento de los DDFF en general y respecto al derecho a la protección de datos personales específicamente, pues otorgaría mayor y mejor cobertura a otros derechos. La extensión a nivel global (mundial) de la autorregulación, teniendo como herramientas únicamente normas abstractas, como son los DDFF admitidos en una gran parte de naciones, en especial con las que la UE tiene relaciones comerciales, podría convertirse en una oportunidad para conseguir la responsabilidad imprescindible en el cumplimiento de normas necesarias para el avance social y también, de toda una civilización, que se concretan desde hace muchos años en los DDFF. La eficacia de la autorregulación en los estándares técnicos industriales y la propuesta de llevar estos mismos mecanismos de técnica normativa a otros elementos de la sociedad no se presenta imposible o descabellada. Sería necesaria la implicación de todas las instituciones tanto nacionales, regionales, como internacionales en su desarrollo y en su aplicación, para que las obligaciones voluntariamente asumidas por los operadores económicos tuvieran un nivel de exigencia en su cumplimiento internacional (global) y un acceso a la justicia garantizada a todas las partes intervinientes en caso de que se incumplieran las normas autorreguladas, un importantísimo aspecto de nuestro sistema de protección. La autorregulación permitiría que se desarrollaran normas acordes con todos los posibles sistemas jurídicos, desde una premisa: el respeto a los DDFF en acuerdos de mínimos

para el contenido y la aplicación de los mismos. En el marco de una normativa institucional se pueden generar otros marcos normativos que cumplan con los mandatos constitucionales y que desplieguen efectos jurídicos. El marco normativo institucional debería contener los criterios que unifican a las empresas y grupos implicados, los procedimientos bajo los que sería posible establecer la normativa que conforme sus relaciones y la que estableciera soluciones a los posibles conflictos, una forma de norma procesal. Surge, sin duda, la cuestión del cumplimiento de las normas autorreguladas o el control de los códigos de conducta vinculantes. En este caso, las Autoridades independientes de autorregulación, serían una herramienta eficaz y aceptada por todas las partes, tanto en asuntos que puedan solventarse a través de la mediación en un conflicto como en aquellas otras ocasiones en que el arbitraje debería asumirse como vinculante para las partes (como sucede con el sector de la publicidad o en algunos consejos audiovisuales, por ejemplo). Como otro factor importante para la eficacia de la norma autorregulada, la Autoridad independiente de autorregulación estaría dotada por la ley de amplias competencias de sanción para los casos de incumplimiento. La normativa desarrollada por el legislador sería la mínima posible para garantizar los aspectos de un posible código de conducta para la protección de datos personales y otros DDFF. Aquí también se abre un posible punto de confluencia entre las empresas, el legislador, los líderes políticos y los ciudadanos⁶⁴². Con su par-

⁶⁴² Como ejemplo de gestión en la que se implicaron diferentes operadores sociales fue el Plan Estratégico de la AEPD 2015-2019. Se abrió un periodo de consultas durante el cual se manifestaron todo tipo de propuestas (cifradas en más de 400 aportaciones de ciudadanos, responsables de tratamiento, expertos en protección de datos y organizaciones públicas y privadas) las cuales se consideraron por la AEPD como de valioso contenido informativo. Véase en la web http://www.agpd.es/portalwebAGPD/LaAgencia/common/Cuadro_aportaciones_Plan.pdf#Propuestas%20recibidas La AEPD “se enfrenta en paralelo a un reto de gran envergadura en 2017: sentar las bases para que tanto las entidades como los profesionales de la privacidad puedan adaptarse de forma paulatina al nuevo Reglamento europeo de Protección de Datos, que será de aplicación directa en mayo de 2018. En este sentido, la Agencia contempla prestar especial atención a las pymes, que constituyen el 99% del tejido empresarial español, para facilitarles herramientas y orientaciones que les permitan cumplir con la nueva legislación. Todo ello sin dejar de lado otros bloques relevantes como el lanza-

ticipación en el desarrollo, contenido y aplicación de la normativa autorregulada se produciría que, por una parte, las empresas participantes en la autorregulación serían las beneficiarias de sus resultados; por otra parte, las normativas establecidas y aceptadas en los códigos de conducta deberían tener rango de ley entre las partes, con los efectos legales pertinentes en cada sistema jurídico. Así, se generaría un efecto legitimador de la normativa autorregulada (o co-regulada), las empresas tendrían una mejor aceptación por su probada responsabilidad social y todo ello derivaría en un aumento de la seguridad jurídica que beneficiaría a la gestión empresarial. Y, por último, la autorregulación debe formar parte del debate político y de nuevas iniciativas legislativas; el legislador no solamente establecería el marco regulatorio (*delimitación interna* de los DDFF), también debería comprobar que los objetivos propuestos y establecidos por la autorregulación normativa se consiguen, y algo más importante, debería también comprobar que los medios o herramientas por las que se llegara a los objetivos propuestos por las partes, son realmente legítimos y conforme al ordenamiento jurídico en general; así, el legislador debería evaluar el impacto de la norma en su vertiente de resultados, en su efectividad y si ese mismo objetivo propuesto se podría o debería conseguir por otros medios. La autorregulación no puede ser entendida como eximente del poder legislativo en sus obligaciones, sino *como complemento* a una legislación que, inevitablemente, puede tener un carácter general. La presión reguladora de los poderes públicos hacía el fomento e incluso la imposición, en ciertos casos, de la autorregulación bajo un marco legislativo, se puede comprender como una forma de reconocimiento a las empresas.

La formulación de posiciones en contra de la autorregulación en materia de DDFF se refirieron a la desconfianza de los actores públicos en la gestión empresarial⁶⁴³. Si

miento de nuevas herramientas de prevención y concienciación para los ciudadanos y el análisis por menorizado de nuevas tecnologías que puedan tener un gran impacto sobre la privacidad”.

https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_12_01-ides-idphp.php

⁶⁴³ En un sentido muy crítico véase ERMIDA URIARTE, ÓSCAR; GIANIBELLI, GUILLERMO; ÁLVARO, ORSATTI, *Responsabilidad social empresarial: perspectivas jurídicas para estrategias sindicales*, Pluna-Uruguay, 2010, pág. 15 y ss. Los autores resaltaron los abusos que pudieran ser cometidos por las

bien es cierto que ciertas empresas operadoras en internet promovieron sus intereses económicos bajo el refugio de la autorregulación (con especial énfasis en las más extendidas, ya apuntadas), lo que también es digno de reseñar fue la respuesta de la sociedad y las Instituciones a esos abusos. No se puede hablar de gobiernos totalitarios en el caso de nuestros Estados constitucionales europeos, aunque los medios técnicos existentes podrían ser utilizados por un régimen totalitario con máxima eficacia en sus fines ilícitos. Precisamente la oposición a la autorregulación de las empresas debería aportar la solución, para controlar la observancia de los DDFF y del cumplimiento de la CE, ese sería una tarea muy apreciable en manos de los medios de comunicación y de información: atender al cumplimiento de la norma autorregulada junto con las Autoridades certificadoras y de control, tanto europeas como de los Estados miembros, en especial la incidencia de la consideración global de una empresa frente a los consumidores, gestando una tendencia normativa de previsión y de consenso ante el derecho fundamental a la protección de datos personales, derecho que a su vez se convierte en garante de otros DDFF, como ha quedado expuesto en anteriores epígrafes. Se tendería a considerar un concepto amplio para el derecho a la protección de datos personales, no limitándolo a los datos que puedan determinar la identidad de una persona ni sólo a la posible situación de que pueda ser identificable por métodos de singularización, extendiendo la protección de los DDFF a la elabora-

empresas, previniendo al legislador frente a posibles disposiciones en cláusulas de Derecho privado. Como herramientas posibles esgrimieron el control legítimo y necesario de los sindicatos. Aunque fue un estudio dirigido a los países del continente americano, sus observaciones son interesantes, en especial respecto a la responsabilidad social de la empresa. Muy crítico en una línea de protección estatal fue RODOTÁ, S., "Democracia y protección de datos."]. https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/DemocraciaMadrid_mayo_05.pdf Según el autor, "una política prisionera de la tecnología puede dar la impresión de mayor eficiencia, pero hace más débil la democracia." En otro sentido, como ejemplo reciente de iniciativa autorregulatoria en Andalucía véase LÓPEZ JIMÉNEZ, D., "La autorregulación de las TIC por parte de las empresas de economía social: D´Confianza como modelo de referencia.", *Revista Internacional del Mundo Económico y del Derecho*, nº VII, 2014, pág. 1-28. D´Confianza es un sello o certificado de cumplimiento normativo autorregulado como iniciativa en el marco de la denominada Economía Social.

ción de perfiles, mucho más importantes para la gestión empresarial e invasivos para los ciudadanos que los datos singularizados de nombre o dirección, por ejemplo. A tenor de las nuevas y progresivas tecnologías se tendería a pesar en una protección que abarque más *aspectos técnicos de seguridad* desde el diseño y por defecto y menos declaraciones de posibles derechos, a una transparencia en la protección de datos, en cuyo caso la *difusión en campañas informativas* se tornaría imprescindible para concienciar a los ciudadanos sobre sus DDFF y donde el deber de información sobre todos los aspectos relacionados con los riesgos sería el pilar fundamental para el consentimiento del titular, para que los ciudadanos pudieran conocer todo lo relativo a sus derechos en materia de protección de datos personales, tanto a nivel administrativo como civil y penal. Importancia tiene también todo lo relacionado con cesión y acceso a los datos, sobre todo cuando el responsable fuera objeto de una acción ilícita de acceso (lógico o físico) a sus instalaciones⁶⁴⁴.

⁶⁴⁴ Véase los estudios de DAVARA RODRÍGUEZ, M., "Firma electrónica y autoridades de certificación. El notario electrónico. ", *El acceso a los documentos municipales*, Madrid, 2002. El autor realizó un análisis sobre la importancia de los medios tecnológicos y la formación de personal adecuado para la gestión de datos personales, en especial certificaciones y firma electrónica. Afirmó con toda razón y conocimiento que la seguridad comienza en la utilización de un servidor seguro, el enlace entre internet y el usuario. Un servidor seguro es aquel que utiliza protocolos de comunicaciones cifrados, de forma que la información (los datos) no pueden ser tratada ni conocida por otros sujetos que no estén autorizados, aunque la comunicación fuera interceptada. Un servidor seguro se encuentra certificado por terceros, denominados, como se comentó, Autoridades de certificación. Las tres características que propone el autor para un servidor seguro son: identificación de las partes, integridad y conservación del mensaje en su transmisión y recepción, junto con la confidencialidad y privacidad de la información. Una comunicación a través de un servidor seguro y certificado tiene generalmente un símbolo en el navegador (candado, llave o similar). Aun no existiendo la seguridad total, sí es cierto que las tecnologías avanzan hacia sistemas de comunicación cada vez más seguros, si el usuario quiere utilizarlos. Anterior a este texto, el artículo del mismo autor DAVARA RODRÍGUEZ, M., "Validez y eficacia jurídica de los documentos generados por medios informáticos o telemáticos: la autenticación de intervinientes y contenidos.", *Revista Calalana d'Arxivística*, nº 14, 1999, pág. 13-34. En relación a la seguridad en las comunicaciones para los servicios de *cloud*, véase de nuevo COTINO HUESO, L., "Algunas cuestiones clave de protección de datos en la nube. Hacia una "regulación nebulosa"", *Revista catalana de dret*

En cuanto al posible régimen sancionador, la sanción más cuantiosa para una empresa proviene de su mercado, no de los poderes públicos. La autorregulación no podría consistir en una normativa cerrada, denominada deontológica, pero que en su contenido intentara evitar responsabilidades para las empresas. Tampoco parece ser la solución un fuerte régimen sancionador de carácter administrativo impuesto por la denominada Autoridad de control. La normativa autorregulada no puede tampoco basarse en la limitación excluyente de los DDFF, sino en su proporcionalidad ante determinadas situaciones. Otro asunto a determinar sería la amplitud de su marco normativo, de su ámbito de aplicación. Existirán situaciones empresariales en las que sería imprescindible su regulación para toda una profesión (por ejemplo, profesiones colegiadas) pues su carácter extremadamente confidencial y de secreto así lo estima. En otros casos, cada empresa podría establecer una normativa autorregulada para lo que fuera conveniente, sin olvidar la simplicidad y efectividad que promueven los certificados de normalidad empresarial (ISO, ya mencionado) para el cumplimiento de las obligaciones comprometidas por las empresas, retirando su sello y certificación otorgados en casos de incumplimiento. La doctrina no omitió las reservas que la propia capacidad de prevención propondría, por ello no se olvidarían de que al promocionarse la autorregulación se deberían potenciar también las exigencias de cumplimiento efectivo de las normas autorreguladas y aprobadas por el legislador o por el organismo competente designado por el sistema jurídico (Agencia, Instituciones de control). No se debería olvidar la figura del DPO (delegado de protección de datos, en español, ya comentado) en la promoción de la efectividad normativa, junto con los principios de privacidad desde el diseño y por defecto junto con el principio de transparencia, mencionados y regulados en el RGPD⁶⁴⁵.

públic., nº 51, 2015, pág. 86-103, pág. 90 y ss. . El autor propuso la existencia de un regulador nebuloso (*cloud regulator*) para aportar seguridad a la red de comunicaciones.

⁶⁴⁵ ARENAS RAMIRO, M., "Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades", *Hacia un nuevo derecho europeo de protección de datos*, Valencia, 2015, pág. 363.

3.2. La certificación de los ciudadanos. El control de la información personal.

En cuanto a los ciudadanos, es esencial que aprecien el valor de las identidades certificadas por sus Estados. Al igual que para ejercer otros actos en la sociedad democrática se solicita la identidad, sería muy importante que la participación y las actuaciones en el ciberespacio estuvieran cubiertas por la identidad de los actores, debidamente cifrada en las conexiones, lo cual existe en este momento y es objeto de continuas innovaciones, por su importancia técnica de seguridad en general. Ello no obsta para permitir el uso de internet sin exhibir la identidad propia, a través de un pseudónimo, por ejemplo, pero para las empresas proveedoras de servicios no deberían existir identidades encubiertas, como *de facto* no existen. Si la opinión o la conducta se ejerce libremente, se presupone que las responsabilidades también. Como expone COTINO HUESO, en una sociedad avanzada para una nueva visión de Estado, la transparencia es “*la fibra misma de la modernidad*”⁶⁴⁶; los ciudadanos no deben temer la

⁶⁴⁶ COTINO HUESO, LORENZO; SAHUQUILLO OROZCO, JOSÉ LUIS; CORREDOIRA ALFONSO, LORETO;., *El paradigma del Gobierno Abierto*, Madrid, 2015, pág. 5 y ss. . En el prólogo de la obra, el autor realiza importantes reflexiones: “la transparencia está llamada a convertirse en una pieza central de la regeneración democrática. Sobre todo, y, ante todo, porque sólo bajo su bandera será posible que grandes franjas de ciudadanía no contemplen la política desde el prisma principal de la desconfianza: la transparencia puede ser una palanca insoslayable para volver a propiciar la politización de los conflictos, una politización que no se confunda con los intereses partidistas. La transparencia, igualmente, debe ser una herramienta indispensable para renovar las teorías y prácticas de los movimientos sociales: la ruptura del velo de secreto que aún oculta algunos espacios sagrados de lo político permitirá vertebrar con más eficacia y raciocinio las agendas reivindicativas, con conocimiento suficiente de las consecuencias de esas mismas demandas. La responsabilidad puede ser un instrumento decisivo en el renacimiento de la responsabilidad política (se añade, y social) como una de las categorías axiales de lo democrático, pero responsabilidad, ahora, no sólo concebida como hostigamiento de los poderes ejecutivos sino, también, como responsabilidad compartida por todos los actores sociales implicados en la dialéctica democrática.” (...) “La transparencia no es una finalidad en sí misma.” (...) “lo esencial en la profundización democrática en la que se debe inscribir la reivindicación de transparencia es la definición de los fines que se quieren alcanzar con el uso de los mecanismos disponibles.” La transparencia

transparencia de un Estado social, democrático y de Derecho, deben practicarla para aportar a la vida política su significado. Las redes de comunicaciones no deberían ser un vehículo para conductas antijurídicas. Muy al contrario, supusieron un avance social importantísimo y pueden ser la base del futuro político y plural, pues, aunque internet fue desde sus inicios una evidencia de problemática regulación, el futuro bien podría ser que una co-regulación adecuada al Derecho, a las finalidades, a los operadores, al funcionamiento técnico, a la realidad y a los usos en internet se convirtiera en una solución⁶⁴⁷. La libertad no se manifiesta de forma encubierta, la libertad se caracteriza por la responsabilidad y el respeto. Las lesiones a la privacidad y a la protección de datos son, sin embargo y a pesar, continuas. Esa sensación de no-regulación por parte de las empresas y de libertad por parte de los usuarios en cuanto a las actividades en internet sólo puede calificarse como autoengaño, apariencia, inconsciencia o incultura. Cualquier actividad en el ciberespacio deja un rastro mucho más sensible en cuanto a DDFF que si se usan medios convencionales para la misma actividad ilícita. La autorregulación descartaría a los *no-certificados* en la normativa de protección de datos (las empresas excluidas) pues beneficiaría a los cumplidores de una normativa europea que generan un plus adicional para incentivar la confianza de los usuarios. En la otra vertiente, a los usuarios la certificación de sus identidades les proveería de una herramienta eficaz para gestionar su autodeterminación informa-

para todas las partes integrantes de las relaciones, no sólo para alguna de ellas. En otra parte de este texto, COTINO avanza también una frase significativa: los problemas se resuelven “usando el nivel del albañil y no el péndulo”, a lo que se añade desde la modernidad del siglo XXI que no es necesario usar ladrillos y cemento, existen paneles autoportantes.

⁶⁴⁷ COTINO HUESO, L., “Algunas cuestiones clave de protección de datos en la nube. Hacia una “regulación nebulosa””, *Revista catalana de dret públic.*, nº 51, 2015, pág. 86-103, pág. 93. El autor cita la Declaración de Independencia del Ciberespacio de 1996, John Perry Barlow, Fundador de Free, Fronteras Electrónicas en Davos (Suiza). Se tiene en cuenta que co-regulación no tiene el mismo concepto de autorregulación, aunque, como se dijo, en este estudio se habla de todas estas acepciones sobre la base de las aclaraciones efectuadas al inicio del presente tema. Véase también sobre transparencia democrática la aportación de RODOTÁ, S., “Las lecciones de wikileaks: nueva transparencia y nueva distribución del poder”, *Transparencia, acceso a la información y protección de datos.*, Barcelona, 2015.

tiva⁶⁴⁸. Desde los inicios del uso de internet ya se apuntaba la falta de conocimientos sobre el funcionamiento de las redes de comunicaciones. No existe el anonimato dentro de internet, los derechos y obligaciones siguen vigentes exactamente igual que en todos los ámbitos de la realidad. La ciudadanía se debería dirigir hacia la exigencia de comunicaciones cifradas, donde sólo el usuario/titular de datos personales tenga potestad para descifrarlas⁶⁴⁹. Así, no sólo los datos personales, sino todo el contenido de las comunicaciones quedaría protegido ante posibles violaciones de DDFF⁶⁵⁰. En realidad, si la protección de los datos personales se realiza desde una perspectiva técnica, se deberían aplicar los procedimientos técnicos informáticos y de telecomunicaciones elementales de seguridad para conseguirla. El más importante de todos los posibles procedimientos es el denominado *control de accesos*, tanto lógico como físico, a los

⁶⁴⁸ Un ejemplo muy positivo: la empresa de distribución Amazon. Cuando un usuario registrado se conecta, lo hace bajo una validación de seguridad, pues se inscribió como cliente, la empresa gestiona sus datos bajo normas muy seguras y su acceso cuenta con tres niveles de confirmación cuando se realiza una adquisición. Amazon ofrece un formidable servicio a los que denomina *clientes Premium* con ventajas y servicios adicionales. La resolución de los conflictos es muy ágil y siempre se tiene una respuesta.

⁶⁴⁹ No se está hablando de actuaciones de los Cuerpos y Fuerzas de seguridad del Estado. En esos casos, cuando intervienen las instituciones de Seguridad estatal, no existen barreras en cuanto a los datos que deseen o necesiten conseguir para la resolución de un asunto. Existen las limitaciones del Estado de derecho.

⁶⁵⁰ Al igual que la conducción de un vehículo o el ejercicio de determinadas profesiones, o la tenencia de una tarjeta de crédito y de una cuenta bancaria necesita de numerosas certificaciones, el ejercicio del derecho a la comunicación e interacción por las redes de telecomunicaciones se vería fortalecido por la certificación de los usuarios que acceden a las páginas de servicios empresariales. Si para una transacción económica el usuario se identifica en una comunicación segura, no puede ser un impedimento identificarse también para compartir experiencias con otros usuarios en redes sociales o mantener un *blog* de opinión o de cultura, aunque dentro de la red social el usuario mantenga un pseudónimo. La promoción de cuentas de usuario denominadas como *validadas* sería lo más óptimo para el respeto de los DDFF. La regulación ya existe, como se ha comentado, para las AAPP. Las empresas sólo deberían aceptarlas en sus normas autorreguladoras para todos los usuarios. En este momento, solamente los usuarios de redes sociales que aportan una contraprestación económica a la gestión de su perfil, cuentan con la garantía de su identidad confirmada. Son las cuentas verificadas o cuentas de usuario VIP para personas con perfil público.

sistemas donde se ubican los datos de todo tipo. El control de accesos se consigue con claves personales e intransferibles de las personas físicas que acceden a los sistemas. Por tanto, si se tiene claro que no existe seguridad sin control de accesos autenticado, y que, sin esa seguridad, la protección es imposible, no tiene sentido oponerse a la actuación de los ciudadanos en internet por medio de certificaciones personales. Sería una decisión personal participar en una situación desregulada e incluso ilícita, como lo es en la realidad ajena a internet. Si el usuario decidiera formar parte de ese tipo de situaciones, pondría voluntariamente en evidente riesgo o peligro sus DDFF, especialmente su derecho a la protección de datos personales. Ante una situación así, se pensaría que el Estado de Derecho habría realizado su compromiso de protección y sólo la voluntad del usuario sería la responsable de las consecuencias negativas.

Por otra parte, las empresas tendrían también una base de reclamaciones para casos de impagos, por ejemplo, y el usuario difícilmente podría ser suplantado en su personalidad. Pero el legislador, sin razón aparente, no decidió en dirección a la identidad confirmada digital obligada, cuya regulación existía por la ley (ya mencionada en el espacio de análisis para ese concepto), y pretendería solucionar los casos de incidencias entre empresas y ciudadanos con la regulación establecida en la LOPD (o alguna norma similar en el futuro) por la que, por ejemplo, el responsable del fichero o tratamiento debería articular los procedimientos necesarios para garantizar la comprobación efectiva de la identidad del titular de los datos, como pudieran ser menores de edad o sus tutores legales, mantener los datos personales para que sean veraces o realizar el principio de calidad de los datos (se remite a los epígrafes correspondientes)⁶⁵¹.

⁶⁵¹ ÁLVAREZ RIGAUDIAS, C., "El poder del usuario digital", *Hacia un nuevo Derecho Europeo de protección de datos*, Valencia, 2015, pág. 280-282. Como la autora propuso, se llegó a procedimientos absurdos, como solicitar la copia del DNI o del libro de familia en papel para una adquisición de productos electrónica. En el mismo sentido véase ALAMILLO DOMINGO, I., "La identidad electrónica en la red.", *Derecho y redes sociales*, Madrid, 2010, pág. 37 y ss. El autor ofreció un análisis exhaustivo de los posibles sistemas de identificación en internet, redes sociales y Administración electrónica, que en ese momento podrían haber estado operativas. Se piensa que, en la actualidad, los avances son todavía

Se tiene la esperanza de que los usuarios validados en internet sean provistos de suficiente tecnología como para ejercitar sus derechos ARCO (junto con el derecho de supresión comentado y dentro de las posibles normas que establezca para el futuro la Autoridad de control) a través de las certificaciones personales, teniendo derechos de acceso, rectificación, cancelación y oposición sólo con activar su clave de cifrado ante las bases de datos de las empresas, sin necesidad de recurrir a engorrosos procedimientos para el ejercicio de su derecho a la protección de datos. Si internet avanza en ese sentido, será mucho más eficaz el cumplimiento de los DDFF. El principio de transparencia y el principio de privacidad por defecto deberían centrarse en la consecución de estos aspectos técnicos. En palabras de DAVARA RODRÍGUEZ, "el gran problema que impide en la práctica la utilización masiva de Internet es la falta de conocimientos, formación e información que permita otorgar la confianza necesaria para su uso; se trata de un problema de confianza basado en la falta de seguridad que rodea a la denominada red de redes; falta de seguridad física, falta de seguridad lógica y, cómo no, falta de seguridad jurídica⁶⁵²".

3.3. Realidades de autorregulación en sectores empresariales.

La autorregulación como alternativa a las leyes realizadas íntegramente por el poder legislativo presenta realidades empresariales que se podrían analizar desde el punto de vista jurídico, en cuanto a la protección de datos personales.

La gestión de las empresas no se define en la ley, son ellas mismas las que gestionan dentro del marco legal sus relaciones con trabajadores, colaboradores, clientes, proveedores, inversores y AAPP. No existe una verdad definitiva de la gestión empresarial, en gran parte, porque es una entidad dotada del dinamismo necesario para res-

mayores hacia una autodeterminación informativa del ciudadano. El autor consideraría la identidad y la firma electrónica como *un ancla entre dos mundos, real-físico y real-electrónico*, p. 45 y ss.

⁶⁵² DAVARA RODRÍGUEZ, M., "Firma electrónica y autoridades de certificación. El notario electrónico. ", *El acceso a los documentos municipales*, Madrid, 2002, pág. 149.

ponder a los estímulos sociales y, por ende, del mercado. Hay cuestiones que se presentan totalmente claras, como son la obligación del cumplimiento de los contratos, la llevanza de la contabilidad, el pago de las prestaciones sociales y tributarias, el cumplimiento de la ley en general y por supuesto el respeto y cumplimiento de los mandatos constitucionales y de los DDFF. Son normas de prohibición o de mandato, no se deben realizar actividades defraudadoras. Por otro lado, existe la obligación de un comportamiento ético en sus directivos y trabajadores, como puede ser el secreto de la información privilegiada y su prohibición de uso en beneficio propio o de personas cercanas, un ejemplo que roza lo ilícito cuando no se cumple. En todo lo demás, en los sistemas de gestión, en la organización para el cumplimiento de su misión empresarial y de cómo cumplir los mandatos legales, *la empresa tiene total autonomía*, como no podría ser de otra forma al ser un sujeto jurídico de derecho privado. En una empresa moderna y social, prevalecerá la transparencia como principio fundamental, para que la información que sea tratada pueda comprobarse fehacientemente. Esa combinación de ley, gestión empresarial y autorregulación se presenta como una buena alternativa ante los vacíos regulatorio en materia de protección de datos. Deberían promulgarse solamente leyes necesarias para su completo cumplimiento, no para obtener un interminable listado legal con variantes *ad infinitum*. Sería un marco estable, justo y seguro para que los ciudadanos se desarrollen con mínimos problemas en él. La autorregulación se presentaría en sociedades libres y de amplias competencias ciudadanas dentro de un marco (se reitera) de transparencia positiva con información veraz, comprobable y auditable por entes independientes, imparciales y competentes para determinados casos, que emita también informes sobre lo que no se informa o no se realiza adecuadamente; evolucionando más allá, que proponga mejoras al sistema, tanto legal como de norma autorreguladora. Si se llegó a una sociedad donde se premia la conducta legal satisfactoria y contributiva, el siguiente paso sería la responsabilidad corporativa social de regulación por norma autogenerada. El antecedente se encuentra en los códigos éticos profesionales, que funcionan desde hace siglos.

Para un escenario autorregulado, serían necesaria como premisa la visión sistemática de toda la organización, lo que implicaría abordar la realidad desde relaciones de

causalidad, no lineales, entre los operadores del sistema. La gestión del conocimiento es siempre colectiva y compartida, no existen sistemas sin interactividad. En la realidad, las capacidades de aprendizaje continuo (tanto de la experiencia positiva como de los errores), el desarrollo de la creatividad, de la innovación, de los modelos mentales reestructurados y la responsabilidad personal de todos los integrantes formarían la base del modelo para la implementación de la norma autorregulada en materia de protección de datos personales.

Como se ha presentado en este análisis, las opciones pueden cifrarse en dos: la norma autorregulada para sólo una empresa o, como alternativa deseable, para todo un sector de actividad. Por su importancia, se analizarán las realidades de normas autorreguladas por sectores, mencionando alguna empresa en particular por su dimensión expansiva mundial.

3.3.1 Autocontrol para las empresas de publicidad.

Autocontrol es la denominación que determina la Asociación para la regulación de la comunidad comercial. Se creó en 1995 por los principales anunciantes, agencias y medios de comunicación con el objetivo de promover una buena publicidad, interpretándose como tal que la información publicitaria fuera *veraz, honesta y leal* dentro del espacio publicitario español, siguiendo otras iniciativas internacionales. Se consideró una exigencia de la sociedad a la que otorgaron una respuesta, sin pretender ser sustitutos del control legal, actuando como un complemento útil mediante la co-regulación. La trascendencia de la autorregulación en las empresas vinculadas a la publicidad tendería a ser mundial, con acuerdos específicos que abarcan todos los continentes en la denominada *World Federation of Advertisers* (WFA) o Federación Mundial de Anunciantes.⁶⁵³ Sería sumamente fácil deducir que los principales anun-

⁶⁵³ Sobre las actividades de Autocontrol, véase su página web <http://www.autocontrol.es/> La dimensión internacional de Autocontrol es considerable. Forma parte de la *European Advertising Standards*, EASA, la Alianza Europea para la Ética en la Publicidad.

cientes son a su vez, las principales empresas que operan en el mundo, las grandes corporaciones, las cuales, a su vez, son los entes que realizarían los mayores tratamientos de datos personales para cualquier tipo de finalidad. De todo ello se deriva la importancia de sus actuaciones para el cumplimiento de los DDFF y específicamente, el derecho a la protección de datos personales.

En el año 2013 se firmó un acuerdo de colaboración entre Autocontrol y la AEPD en materia de protección de datos personales para conseguir el seguimiento del uso de *cookies* a través del servicio *Cookie Advice*, y cumplir con el artículo 22.2 de la LSSI (se recuerda, Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico), una iniciativa que se adelantaría a los posibles efectos dañinos del uso de *cookies* por las empresas en internet, como servicio de consultoría de la Asociación, para ayudar a las empresas en la adecuación de sus formatos y contenidos en cuanto a uso de *cookies*⁶⁵⁴. La AEPD acogió el sistema de autorregulación de Autocontrol muy

http://www.autocontrol.es/pdfs/autor_Europa_Decl_principios_%C3%A7omunes.pdf Como se refleja en su texto, “La autorregulación publicitaria es la respuesta de la industria publicitaria al reto de tratar las cuestiones atinentes a las comunicaciones comerciales a través de un ejercicio voluntario y comprometido de responsabilidad social en lugar de una legislación detallada. Mediante la autodisciplina publicitaria, la industria demuestra su capacidad para regularse a sí misma de forma responsable, promoviendo activamente los más elevados niveles de corrección ética en las comunicaciones comerciales y salvaguardando los intereses de los consumidores.”

⁶⁵⁴ Las herramientas informáticas denominadas *cookies* (galletas) no son programas que se instalen en un equipo, son datos que no pueden tratar información de los equipos en los que operan. Su finalidad es detectar la navegación en el equipo que está conectado a una página determinada o un grupo de páginas vinculadas entre sí. Es cierto que puede almacenar información de navegación para generar un perfil de usuario, sin embargo, para que estos perfiles sean vinculados con una identificación personal, el titular de los datos debería haber aportado esa información personal, bien a esa página o bien a otra vinculada. Debido a los sistemas de análisis de grandes cantidades de datos, se puede vincular información a un lugar que coincida con un determinado dato de telecomunicaciones, pero identificar al individuo que navega resulta muy difícil, por razones obvias: en un mismo equipo pueden navegar varios perfiles de usuarios, además de no poder controlar con total certeza si es la misma persona física la que navega, aunque el usuario sea único y coincida, pues pudiera darse que bajo el mismo usuario y contraseña operasen varias personas. Es un asunto que sólo la Seguridad Nacional de los diferentes países dominan con menor margen de error.

satisfactoriamente. Su colaboración se basaba en el intercambio de información sobre empresas que pudieran ser objeto de controversias extrajudiciales en el seno de la Asociación para que se trasladara esa información a la AEPD, con independencia de sus competencias. Al mismo tiempo, la AEPD informaría a la Asociación de cualquier diligencia o requerimiento a una empresa asociada, en relación a la instalación de *cookies*. La AEPD tendría en consideración los informes que generase la Asociación y así mismo, Autocontrol emitirá un informe de su actividad de consulta y verificación en el uso de las *cookies*. Esta colaboración que se podría asimilar a un acuerdo de autorregulación entre ambas entidades, se desarrollaría también en el ámbito formativo, de divulgación o de estudio que las partes considerasen conveniente, junto con otras 19 entidades que forman parte de Autocontrol.

3.3.2 Autorregulación para empresas con actividades en Internet.

Completando el epígrafe anterior, Autocontrol también generó el denominado *Código Ético de Comercio Electrónico y Publicidad Interactiva*, presentado en el año 2002 y con varias modificaciones hasta la versión de 2015 que adoptó las modificaciones introducidas por la Ley 9/2014, de 9 de mayo, de Telecomunicaciones y la Ley 3/2014, de 27 de marzo, por la que se modificaba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre⁶⁵⁵. Autocontrol y la Asociación Española de la economía digital (ADIGITAL), a través de la marca o sello *Confianza Online* pretendería proteger los ámbitos de la comunicación comercial en cuanto a la publicidad interactiva, la publicidad en internet y el comercio electrónico. Además, se ocuparía de resolver problemas relacionados con protección de menores, accesibilidad y usabilidad, junto con la privacidad y protección de datos personales.

⁶⁵⁵ Disponible en http://www.autocontrol.es/pdfs/cod_confianzaonline.pdf y en la propia AEPD. La página web de Confianza Online es <https://www.confianzaonline.es/>

El Código Ético de Confianza Online promovió la autorregulación para afrontar los retos del futuro mercado global y la promoción de sellos de calidad o de certificación que a nivel internacional se generan por las empresas, considerados como herramientas imprescindibles para completar los sistemas tradicionales de las estructuras jurídicas, para garantizar un modelo seguro y una protección eficaz de los derechos a todas las partes implicadas. La AEPD lo reconoció como Código Tipo en su Resolución de 7 de noviembre de 2002. El sello de Confianza Online fue reconocido en julio de 2005 como Distintivo público y publicado en el BOE en octubre del mismo año. Posteriormente se realizaron sucesivas adaptaciones al texto del Código, el cual en su última versión recogería una revisión de sus normas para adaptarlas a las modificaciones de las leyes mencionadas. El ámbito de aplicación del Código se manifiesta en cuestiones que afecten a la publicidad, comercio electrónico y protección de datos personales cuando realicen las entidades adheridas publicidad o transacciones contractuales con consumidores a través de medios electrónicos de comunicación a distancia, en especial, a través de internet (artículo 2). Se aplicaría igualmente el Código de *Confianza Online* cuando una entidad adherida trate datos que se encuentren registrados en soporte físico que los hagan susceptibles de tratamiento, así como a toda modalidad de uso posterior de dichos datos, sea como responsable o como encargado del tratamiento de datos personales. Quedarán exceptuados de esta consideración los ficheros y tratamientos de datos que se determinen por la normativa aplicable. El Código dedicó un Título completo, el IV, a la protección de datos personales. En el artículo 23 se constata la conexión entre el texto autorregulado y las normas de protección de datos personales. En cuanto a DDFF, el artículo 23.3 estableció expresamente que las entidades adheridas deberán respetar la privacidad de los usuarios, así como asegurar el secreto y seguridad de los datos personales, adoptando para ello las medidas técnicas y organizativas necesarias, habida cuenta del estado de la tecnología, la naturaleza de los datos y los riesgos a los que están expuestos, lo cual conectaría lógicamente la seguridad de los datos personales con el establecimiento de la seguridad técnica informática y de telecomunicaciones en general. El artículo 23.4 estableció que, además, las entidades adheridas deberían apoyar iniciativas para ayudar a educar al con-

sumidor sobre cómo proteger su intimidad en los medios electrónicos de comunicación a distancia, aspecto que se podría considerar sumamente importante. Todavía no se ha actualizado este Código de *Confianza Online* a la normativa del nuevo RGPD, se espera para próximas revisiones. En la última versión, no se habían abordado el análisis masivo de datos (*big data*) para usos de publicidad, marketing y promociones, no sólo online, sino de todo tipo, también para oferentes fuera de internet, para empresas productoras o para análisis sociológicos, ampliando su ámbito de actuación a estos sistemas de análisis masivo de datos que preocuparían a la doctrina jurídica por sus implicaciones en los DDFF, ya comentados. Se tiene la esperanza de que una entidad como Autocontrol consiga realizar un texto autorregulado de incidencia mundial que sea cada vez más respetuoso con los derechos de las personas, con los derechos sociales y también que eduque a las empresas implicadas sobre estos asuntos. Se recuerda que gran parte de los medios de comunicación basan sus ingresos económicos en la publicidad, por lo que la incidencia de sus actuaciones se manifestaría contundentemente en los cambios empresariales para la mejora del sistema normativo y su eficacia en general, y en especial, para la protección de los DDFF por medio de la protección de datos personales.

Existirían también críticas ante el sello de *Confianza Online* por parte de pequeñas organizaciones empresariales que no verían aliciente a este sistema privado e inspirado por y para grandes organizaciones. Ante ese otro escenario, las Administraciones de diferentes CCAA crearon otros instrumentos basados en el arbitraje de consumo, donde a las empresas adheridas al sistema Arbitral de Consumo se les otorga un sello de calidad promovido por las AAPP y deben cumplir ciertas normas que se podrían considerar co-reguladas. Por ejemplo, la Junta de Andalucía, el Gobierno de Aragón o la Comunidad de Madrid.⁶⁵⁶

A. Especial referencia a las redes sociales

⁶⁵⁶ Véase si es de interés <http://arbitrajedeconsumo.mspsi.es> del Ministerio de Sanidad, Servicios Sociales e Igualdad.

Se podrían apuntar el año 2012 como la fecha en la que las redes sociales a través de internet tuvieron su crecimiento exponencial transformando la sociedad en tal grado que la doctrina afirmó asistir a una *nueva revolución social*, con una fuerza extraordinaria que afectó a los conceptos de libertad, publicidad, seguridad, derecho, economía, relaciones personales o trabajo. Los diversos conceptos de red social se acuñaron en anteriores etapas de la humanidad, no son novedosos del siglo XXI, pero no tuvieron nunca antes en la Historia tal trascendencia. Se consideraba red social a un patrón de relaciones sistemático, o en palabras de LEINHARDT (1977), como *sistema de relaciones sociales que articulan a diferentes entidades sociales*⁶⁵⁷.

Es doctrina ampliamente formulada que existe una evidente dificultad en internet para regular el tratamiento de datos personales, dentro de una normativa uniforme. La adopción de elementos autorregulatorios se basaría precisamente en la necesidad de un consenso de mínimos sobre el respeto a los datos personales dentro de los diversos modelos jurídicos que operan en los territorios desde donde podrían ser tratados datos personales. Que las empresas operadoras en internet fueran las que ofrecieran la posibilidad de ampliar su protección dentro del respeto a los DDFF se plantearía como un avance y una promoción de los derechos y libertades para todo el planeta, generando, como se comentó, mayor confianza y mejora de la actividad empresarial, que se traduciría en mejores resultados económicos. Las empresas podrían suministrar mejor protección a un sector de actividad determinado, pues se adaptarían a un nuevo escenario sin problemas de trámites legislativos, más rápidamente. La autorregulación generaría Códigos de conducta privados, diversas normas generales de protección de datos y sellos o marcas que identificarían a los operadores adheridos en internet. Los Códigos, como se ha mencionado, generarían normas de procedimiento para la resolución de conflictos y para la comprobación del cumplimiento de las normas autorreguladas dentro de sus empresas.

⁶⁵⁷ GONZÁLEZ TABLAS-SASTRE, R., "La revolución social de las redes sociales en internet", *Nuevas tecnologías y Derechos Humanos*, Valencia, 2014, pág. 113 y ss.

Pues bien, en cuanto a las redes sociales, la doctrina se enfrenta a una fuerte discusión sobre su regulación. Desde posiciones defensoras de una libertad total en las redes sociales a las que imponen determinados gobiernos para evitar la emisión de intercambios de relaciones personales, opiniones de todo tipo y comunicaciones visuales. Las redes sociales serían esencialmente *autorreguladas* por las propias empresas que las gestionan, pues normalmente el sistema jurídico democrático no conseguiría entrar a normalizar las conductas que se explicitan a través de ese medio de comunicación social, negocio lucrativo para muchos operadores; y en el caso de gobiernos que limitan los medios de comunicación, es obvio que la autorregulación como libertad de normalización de conductas, no existe. Ciertamente sería igualmente que ninguna persona resultaría obligada a participar con sus datos en las redes sociales, que no tiene por qué exhibirse ninguna conducta que pudiera resultar dañina para el usuario, y que las ventajas de las redes sociales, en especial las profesionales, serían muy amplias. Pero existen determinados riesgos que la AEPD analizó (se comentó en otros epígrafes) en los que los usuarios no son conscientes del precio que pagan por la forma de comunicación en la que participan, y por supuesto, las empresas proveedoras de plataformas de redes sociales no eliminarían, aunque existen movimientos a favor de una mayor protección en las redes sociales, especialmente en el caso de menores o de personas vulnerables⁶⁵⁸.

⁶⁵⁸ Véase en general al respecto la obra colectiva coordinada por RALLO LOMBARTE, A., *Derecho y Redes Sociales*, Navarra, 2010. La definición de redes sociales fue apuntada en concreto por ÓRTIZ LÓPEZ, P., "Redes sociales: funcionamiento y tratamiento de información personal", *Derecho y redes sociales*, , 2010, pág. 23 y ss. que tomó la definición de la Directiva 98/34/CE, artículo 1.2, que fue en diferentes ocasiones modificada para llegar a la Directiva 2000/31/CE de Comercio Electrónico, la cual sirve de antecedente normativo a la LSSI (Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico). Su enunciado fue ampliamente contemplado como redes sociales online y definido como "*aquellos servicios de la sociedad de la información que ofrecen a los usuarios una plataforma de comunicación a través de internet para que estos generen un perfil con sus datos personales, facilitando la creación de redes en base a criterios comunes y permitiendo la conexión con otros usuarios y su interacción.*" También mencionó la autora la teoría de los 6 grados de KARINTHY ampliada por el sociólogo WATTS, por la cual todo ser humano está conectado con toda la humanidad por cadenas de contactos sociales de 6 grados. No es objeto de esta tesis, pero se apunta, como orienta-

La posibilidad de que las grandes redes sociales llegarán a un acuerdo para promover los DDFF dentro de sus contenidos, incluso premiando las conductas respetuosas, no ya censurando las impropias o las dañinas, sería un avance global dentro de las conductas de todos los participantes en las redes sociales. La autorregulación se presentaría como una gran oportunidad y un reto, a pesar de que en internet concurren diferentes sistemas jurídicos. Como expresó BOIX PALOP, internet (y las redes sociales, se podría añadir) "*lejos de deslegitimar la intervención pública, no viene sino a reforzar la importancia de la labor de creación del correcto marco para la realización de las actividades informativas*"⁶⁵⁹. La tarea del legislador sería garantizar siempre la libertad en internet, evitando la confluencia de poderes que deseen controlarla o desvirtuarla. La autorregulación, por su parte, podría aportar eficacia en la resolución de conflictos dentro del ámbito de las redes sociales, promoviendo en primer lugar, conductas de respeto de los DDFF y facilitando la privacidad de los usuarios. Los entornos dinámicos de las redes sociales propiciarían las normas autorreguladas de protección de datos personales. Hasta este momento, solamente alguna de las grandes empresas de red social (Facebook, Google) presentaron cierto interés en autorregularse para la

ción. Se recuerdan también los Dictámenes del GT29 y diversos estudios sobre redes sociales y menores dentro de la UE, como por ejemplo en la web <https://ec.europa.eu/digital-single-market/self-regulation-better-internet-kids> en la que se promueve una mejor autorregulación para alcanzar objetivos de protección a menores en las redes sociales. Véase también respecto a los menores y las redes sociales el análisis de DE MIGUEL MOLINA, MARÍA; OLTRA GUTIERREZ, JUAN VICENTE; "La autorregulación europea de las redes sociales: análisis de las políticas de uso de la imagen de menores en España", *Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías*, Valencia, 2010, pág. 476 y ss.. Los autores realizaron un estudio sobre la base normativa propuesta por la UE en el año 2010. En sus conclusiones también se adhieren a la posición de que la solución óptima para la protección del usuario, especialmente el menor de edad, sea el uso del e-DNI o documento similar.

⁶⁵⁹ BOIX PALOP, A., "Libertad de expresión y pluralismo en la red", *Revista española de derecho constitucional*, nº 65, 2002, pág. 133-182, pág. 135 y ss. El autor promovió la idea de que las redes de comunicación a través de internet, sería asociado a los conceptos de difusión de información. Si bien sería en gran medida cierta esta afirmación, se distingue la estructura de la red social dentro de las comunicaciones en general, por el modelo de negocio de la red social, que se basa en la publicidad personalizada ofertada al usuario.

posible protección de datos personales, pero el contenido de las denominadas políticas de privacidad en estas empresas no expresaría ni mucho menos el posible contenido de la norma de protección de datos personales que se promovería por los legisladores europeos. Con la entrada en vigor del RGPD, las adaptaciones para Europa estarían todavía por definirse⁶⁶⁰. Lo que sí parece haber sido comprendido en los últimos años sería el concepto de responsabilidad en el uso de las redes sociales, sin que se conviertan en un espacio de impunidad. Las prácticas abyectas y no deseadas por la mayoría de usuarios pueden ser presentadas ante los administradores de la red en que se producen y el usuario interrumpe su visionado de contenidos provenientes de otros que no desea conocer. Incluso la red excluiría a los usuarios que realicen prácticas no permitidas por sus normativas. Como ya se comentó en otros epígrafes, las consecuencias de las conductas ilícitas en el ciberespacio generan responsabilidades en el sistema jurídico real, no existe la impunidad dentro de las redes sociales. Estas nor-

⁶⁶⁰ Como ejemplos sirvan los contenidos de Google bajo el epígrafe Códigos de autorregulación en <https://www.google.es/intl/es/policies/privacy/frameworks/>. La empresa confirmaba en ese texto que cumplía la normativa del marco del Escudo de Privacidad (*Privacy Shield Framework*) ante el cual estaban certificados, al igual que los estándares del sector relacionados con la transparencia y la capacidad de elección en anuncios online. En cuanto a la política de privacidad, no admitiría comentarios a favor de la privacidad, más bien es un listado de acciones que la empresa realiza con una descripción final a cada párrafo, en la que afirman que siempre actúan para mejorar, bien sus ofertas, bien sus servicios, bien la percepción del usuario. Leerse los contenidos de la política de privacidad de Google y generar un análisis serviría para otro texto académico. Véase en <https://www.google.es/intl/es/policies/privacy/> y en <https://privacy.google.com/take-control.html>. Al menos en estos momentos se preocupan de que el usuario pueda modificar las condiciones de privacidad, pero no lo presentan por defecto, sino que es posterior a la activación de la cuenta en la red de Google. <https://www.facebook.com/about/basics/how-others-interact-with-you/untagging/>. En otras empresas, el procedimiento sería muy similar. Por ejemplo, para Facebook, un ciudadano que resulte ser incluido en una imagen dentro del perfil de otro, podría solicitar su exclusión, pero debe ser usuario de Facebook para solicitarlo, lo cual no dejaría de ser un absurdo, junto con otra paradoja, que puede ser objeto de Facebook sin ser usuario de la red social, al incluirse por un tercero. Ese riesgo o peligro del efecto globalizador es lo que la doctrina denuncia en sus análisis desde hace años. Véase al respecto VILASAU SOLANA, M., "Privacidad, redes sociales y el factor humano", *Derecho y redes sociales*, Madrid, 2010, pág. 61.

mas de conducta para usuarios serían los denominados límites autogenerados por las empresas, bien valorados por la doctrina en general, calificados como una *corriente reprivatizadora o desreguladora* para acceder a formas flexibles de autorregulación⁶⁶¹.

B. Especial referencia a las grandes corporaciones de venta y alquiler de bienes y servicios.

Aunque a través de las actividades de Autocontrol mencionadas, las grandes corporaciones desarrollan una autogestión de su protección de datos personales, sería también interesante añadir que todas las empresas que operan por internet en la venta de bienes y servicios deben cumplir la legislación europea y, por ende, la española, además de las normativas de los países en los que se encuentran los compradores de esos bienes y servicios. Un aspecto que no estuvo excesivamente clarificado fue la norma aplicable a los contratos electrónicos y la determinación del lugar de celebración de los contratos online (reserva de un hotel, alquiler de un vehículo, compra de un artículo de consumo, por ejemplo). Este tipo de actividades se considerarían suje-

⁶⁶¹ Véase en este sentido el análisis de PATRICIA ROJAS, Á., "La responsabilidad de las PSSI y la libertad de expresión.", *Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías.*, Valencia, 2010, pág. 296. El acrónimo PSSI corresponde a la definición de *persona física o jurídica que proporciona un servicio en la sociedad de la información*. La autora pondría especial atención a la definición de la noción *conocimiento efectivo* de determinados hechos por parte de los administradores de las redes sociales. En cuanto a la construcción de una red social más respetuosa con la privacidad, véase MEGÍAS TEROL, J., "Privacy by design, construcción de redes sociales garantes de la privacidad", *Derecho y redes sociales*, Madrid, 2010, pág. 319 y ss. El autor desarrolló los principios, medias técnicas y organizativas, protecciones de seguridad e información hacia los usuarios que una red social debería contemplar para considerarse jurídicamente respetuosa con la protección de datos personales y la privacidad. Se puede comprobar en su lectura que la autorregulación por las empresas de la protección de datos personales es completamente viable, aunque existieran diferentes sistemas jurídicos entre los usuarios. El autor aplicó en 2010 los conceptos de privacidad desde el diseño y por defecto junto con el principio de transparencia, presentes en el nuevo RGPD como mandato.

tas a la normativa de Derecho internacional privado, destacando en la LSSI los artículos 26 a 29. Este asunto tendría una fundamental trascendencia para fijar las posibles reclamaciones⁶⁶². En el caso de normas sobre protección de datos personales, se deberá aplicar la normativa comentada del nuevo RGPD en estos aspectos, que posibilita normativas de autorregulación en esta materia, siempre que se cumplan los mandatos legales. En este sentido, es obvio que las grandes corporaciones intentarán siempre proteger sus intereses en muchos aspectos; positivamente a favor del consumidor se manifiestan prácticas de resolución de conflictos muy rápidas realizadas por grandes empresas (Amazon, por ejemplo) que sin dilación y por el simple hecho de manifestar una disconformidad, proceden a su solución, por ejemplo, para el caso de no desear recibir más publicidad o para que los datos personales sean cancelados. Otras empresas, sin embargo, tienen todavía un importante recorrido en estas cuestiones.

C. Especial referencia a las entidades de crédito y financieras.

Las entidades de crédito y financieras presentaron un código de conducta aprobado por la AEPD en 2014. La polémica Asociación Nacional de Establecimientos Financieros de Crédito o ASNEF, por su incidencia en los años de crisis económica y social, pretendía como objetivos el establecimiento de un procedimiento de conducta de obligado cumplimiento para las empresas del sector, coordinando la actuación de las mismas en la protección de los datos personales de los interesados, también facilitar y agilizar el ejercicio de los derechos de carácter personal y la adopción de un marco de publicidad necesaria, dada la forma planteada en el ámbito de la defensa contra las conductas atentatorias al patrimonio económico de los consumidores y ciudadanos, disminuyendo, a través de la publicación de su funcionamiento, la aparición de

⁶⁶² Véase para este asunto y como ejemplo las ideas de CASTELLANOS RUIZ, E., "Las normas de Derecho Internacional Privado sobre consumidores en la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico.", *Cuadernos de derecho transnacional*, nº 2, 2009, pág. 134-159.

factores de inquietud social. Es un ejemplo de código para que otras empresas cuyos objetivos sean compartidos se adhieran al mismo. Otro código de conducta que la AEPD publicó en el año 2015 es de la Asociación Nacional de Entidades de Gestión de cobro, ANGEKO, que agrupó a las empresas de recobro, denominadas como tal las entidades que tuvieran como objeto social la prestación de servicios de recobro de cantidades impagadas, tanto por vía amistosa como por vía judicial, entendiendo como servicios de recobro las actividades relacionadas con la recuperación de impagados. Se trata en ambos casos (ASNEF y ANGEKO) del sector financiero y la importancia que tendría para el mismo la información personal, tanto para cuestiones de crédito como para el cobro de posibles deudas.

En el fichero ASNEF existiría lo que el código denomina *derecho de autoinclusión*, por el cual cualquier persona, por sí misma o a través de su tutor legal, podrá solicitar la inclusión de sus datos personales en el fichero ASNEF PROTECCIÓN con la finalidad de proteger su identidad, solvencia patrimonial y/o evitar que sus bienes económicos pudieran verse afectados por el extravío o robo de su documentación o por la concurrencia de estafa por suplantación de su personalidad. En cuanto al código tipo de ANGEKO, se comprometerían a proteger el derecho fundamental a la protección de datos de todos los afectados. Se tendrían serias dudas sobre tal afirmación, partiendo de la base de que se fuerza necesaria en muchos casos una investigación sobre los deudores para su localización y situación patrimonial, que se presta a cuestiones también privadas y que abarcaría incluso a las personas que conviven o tienen contacto con el afectado. Actuaciones que (sin valorar su legitimidad) no dejarían de realizarse sin el consentimiento de las personas investigadas.

Ambos códigos desean ser una norma autorregulada, de compromiso obligatorio y se presentaron con vocación de servicio. Se dudaría, como se ha comentado, de su efectividad, pues la sola actividad financiera necesita de datos (personales y no personales) de terceros sin su consentimiento para su gestión.

3.3.3 Autorregulación para los medios de comunicación audiovisual.

El asunto de la autorregulación de los medios de comunicación audiovisual se une con otro epígrafe tratado en esta exposición sobre los DDFF y la información personal que se publica en los mencionados medios. Existiría en España y Europa un código deontológico del periodismo, más como una declaración de intenciones que como una norma obligatoria⁶⁶³. Pero no se contempla la cuestión desde el mismo punto de vista en referencia a los medios de comunicación, es decir, las empresas cuya actividad es la difusión de contenidos informativos o de otro calado social, como entretenimiento, cultura u ocio. Existiendo esta cuestión, se mencionan los códigos de conducta (o

⁶⁶³ Se mencionan los siguientes textos:

El código deontológico de la Federación de Asociaciones de Periodistas de España (FAPE) que se puede consultar en su página web <http://fape.es/home/codigo-deontologico/> . El código deontológico español no mencionó la expresión protección de datos personales en todo su texto; sí realizaría algún tipo de alusión a datos que pudieran generar discriminación o perjuicios, como son datos referentes a la raza, religión origen social, sexo, minusvalía psíquica o física si su alusión es despectiva o no son relevantes para la información (Principios Generales, punto 7 a) y b)

El Código deontológico europeo de la profesión periodística, cuyo texto en español se publica en http://www.asociacionprensa.org/es/images/Codigo_Deontologico_Europeo_de_la_Profesion_Periodistica.pdf .

Y como otra mención el Código Internacional de Ética Periodística de la UNESCO aprobado en París en abril de 1954

<http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/images/wmn/code%20of%20Ethics%20Collegio%20de%20periodistas.pdf>

Todos los textos contemplan diversos puntos en común, como puede ser la publicación de datos sobre aspectos de raza, sexo o religión de las personas implicadas, lo cual se debe eludir a no ser que tuvieran relevancia en la información.

Como ejemplo de mención explícita de protección de datos en un código deontológico de los medios de comunicación se cita la web del denominado en alemán *Deutscher Presserat* (traducible como Consejo o Asociación de la prensa) <http://www.presserat.de> En esta página se explica en uno de sus vínculos las obligaciones de la prensa y los medios respecto a la ley alemana de protección de datos personales (*Bundesdatenschutzgesetz* (BDSG) El contenido sería similar a lo que se podría comentar con la propia ley española, lo que se realizó en otros epígrafes. Es significativo para una evolución positiva de la protección de datos en los medios de comunicación.

<http://www.presserat.de/redaktionsdatenschutz/redaktionsdatenschutz-was-ist-das/>

deontológicos) del periodismo como norma autorregulada, con especial incidencia en el secreto profesional, concepto que conectaría la actividad periodística con la protección de datos personales, en ausencia de norma específica para solventar la colisión de derechos, sin olvidar la cuestión de la incidencia de las empresas en esta cuestión⁶⁶⁴.

El periodista se encontraría ante escenarios dinámicos de diversa naturaleza, por lo que la doctrina se inclinaría a favor de la norma autorregulada, la cual se *“encuentra en el espacio existente entre la realidad y el deber ser o el ideal de ejercicio de una libertad que está en función de los medios técnicos y de su distinto alcance.”* Los medios técnicos y su velocidad en el movimiento de la información condicionarían el ejercicio de la labor periodística a la mencionada revisión. Más deseable jurídicamente sería una normativa autorregulada en la que también participaran las empresas de comunicación informativa o de contenidos diversos (mencionados) emitidas por medios de comunicación. Sería completamente visible la diferencia de intereses de las grandes empresas de comunicación, los intereses sociales de los ciudadanos que reciben la información, y los trabajadores-periodistas que son intermediarios de los contenidos. Estos últimos se encuentran en una situación desventajosa en muchas ocasiones, pues deben ponderar y *compatibilizar la finalidad económica de la empresa de comunicación con el respeto a los DDFF*, además de respetar los derechos individuales y los intereses empresariales o de los trabajadores.

⁶⁶⁴ Véase a este respecto la idea de MORETÓN TOQUERO, M., "El secreto profesional del periodista y la empresa de comunicación: ¿Un conflicto de lealtades?", *Revista Jurídica de Castilla y León*, nº 4, 2004. La autora consideró que las normas autorreguladas del estatuto profesional de los periodistas, con su doble carácter de norma jurídica (convenios colectivos) y norma ética (Códigos deontológicos) conforman una forma de estatuto profesional del periodista. Véase también LÓPEZ RICHART, J., "Difamación en la web 2.0 y responsabilidad civil de los prestadores de servicios de alojamiento", *Derecho privado y Constitución*, nº 26, 2012, pág. 143-201. El autor mantiene una postura contraria a la autorregulación basada en los resultados obtenidos. En otra postura doctrinal, CARBAJO NÚÑEZ, M., "La protección de la intimidad en los códigos deontológicos del periodismo europeo", *Antoniano*, nº 4, 2004, pág. 715-745.

Por estos motivos, se piensa que una empresa de comunicación no debería tener el mismo tratamiento jurídico de cualquier otro tipo de empresa, sino que su normalización se mantendría siempre transparente y en revisión constante. La utilidad de una norma autorregulada en el periodismo dotaría de calidad y eficacia a su sistema y si fuera de dimensiones globales, el mundo realzaría sin lugar a dudas un avance significativo debido a los flujos transparentes de información. Pero en la realidad actual ni tan siquiera se llegó a un acuerdo en cuanto a la denominación de internet como fuente periodística.

Otro asunto también a señalar sería la publicación en el año 2016 de una edición actualizada del denominado *Código de Derecho Audiovisual*, una extensa presentación de diferentes normativas en cuanto a medios audiovisuales que operarían en España, entre cuyos textos se especifican diferentes formas de autorregulación para aspectos de tratamiento en los medios, como por ejemplo se menciona en la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual, la normativa autorregulada para la emisión de contenidos publicitarios, para establecer la gradación de la calificación de contenidos para la infancia, o como simple derecho del prestador de servicios de comunicación audiovisual para normalizar su actividad y sus relaciones con terceros, aspecto sumamente importante, pues no se trataría de una obligación o deber de las empresas hacia los ciudadanos, sino de un derecho a su disposición. En el caso del derecho a la protección de datos personales, se encontraría recogido en esta normativa, en diversas formas y diferentes artículos, lo cual se presentaría como un progreso importante, pues aun no existiendo un texto claro sobre el tratamiento por parte de las empresas audiovisuales del derecho fundamental a la protección de datos, sí se menciona en diferentes normas que conforman el Código de derecho audiovisual, junto con otros DDFF, en especial el derecho a la intimidad o los derechos de los menores y personas con especial consideración por su posible vulnerabilidad, remitiéndose a la normativa de la LOPD y su Reglamento (por ejemplo, en la Ley 9/2014, de 9 de mayo, General de Comunicaciones). Podría conseguirse en un futuro próximo una norma autorregulada en materia de protección de datos personales específicamente en el sector de la información y, como ya se apuntó en otros epígrafes, conseguir una

mejor función social del derecho a la libertad de expresión e información sin violar sistemáticamente otros DDFF. No se olvidaría en este análisis la influencia comentada de Autocontrol, como entidad controladora de la actividad publicitaria, fuente de ingresos de los medios informativos y de comunicación social, que podrían a su vez generar un movimiento importante en la consideración de los DDFF por las empresas y profesionales, como se comentó en el epígrafe destinado a esta asociación, vertiéndose su influencia más allá de la publicidad.

GAVARA de CARA insistió en el carácter de voluntariedad en cuanto a la normativa de autorregulación para la adopción de unas normas de conducta que serían seguidas por las partes intervinientes, la creación de un sistema de aplicación e interpretación de esas normas, junto con la generación de un órgano para el ejercicio de esas funciones y medias que garantizaran el cumplimiento de las mismas. Es lo que el autor denominó *autorregulación en sentido puro*. En otra vertiente, si la norma autorregulada se controlase por una entidad pública (gubernamental) en su cumplimiento, se dudaría por el autor de su naturaleza, pues las sanciones administrativas constituirían una especie de *autorregulación institucionalizada*, lo cual pudiera ser jurídicamente cuestionable. En cualquier caso, las empresas de contenidos audiovisuales se resistirían a cualquier intervención de las instituciones públicas en el control de los formatos, alegando, como se comentó, censura previa y vulneración de los derechos constitucionales que asisten a los medios de libertad de expresión e información⁶⁶⁵.

⁶⁶⁵ GAVARA DE CARA, J., *La autorregulación de los medios de comunicación como sistema de control*, Madrid, 2013. El texto del autor es extenso pero muy preciso. Expuso dos modelos de gestión de los medios, uno liberal, en el que predominaría la voluntad empresarial y profesional de gestión de contenidos (entretener, informar, controlar al gobierno, un modelo de EEUU) y otro modelo que denominó *de responsabilidad social*, que conjugarían los intereses de mercado en las empresas con los intereses sociales, la formación de los ciudadanos y la participación democrática. Es el modelo que consideraría la norma europea y, por ende, la española, o al menos eso se pretendería. Destacan las propuestas que realiza en las páginas 34 y ss. “Desde un punto jurídico no es tan importante saber qué sistema de regulación y adaptación se va a utilizar (si es una regulación directa por el legislador, una co-regulación o una autorregulación pura o en sentido estricto), sino cómo que se plantearán mecanismos posteriores de control y garantía para que las medidas concretas puedan adaptarse y desarrollarse.” (...) “En el

3.3.4 Autorregulación para los sectores relacionados con la salud,

El sector de medicina privada inscribió un Código tipo de protección de datos para las organizaciones adheridas ante la AEPD, la cual lo aprobó junto con otros Códigos tipo de organizaciones con ámbito sanitario, como odontología o recursos asistenciales. Se toma como referencia el código que cuenta con mayor número de empresas adheridas y que además tiene una extensión geográfica a nivel nacional. La sensibilidad del sector de la salud hacia el derecho a la protección de datos personales quedó patente en el epígrafe correspondiente. No siendo el derecho a la salud un derecho considerado por la CE como fundamental, tiene un desarrollo tan extenso a lo largo de estos años y una consideración social sumamente importante, a lo que se añade, desde la perspectiva de la protección de datos personales, una fuerte concienciación de los profesionales del sector de la salud, que por su propio ejercicio se encontrarían vinculados al secreto profesional más estricto, promovido por su código ético de colegiados. El código tipo inscrito en la AEPD por las asociaciones del sector privado en el ámbito de la salud (con la denominación en el Código tipo de *Asociaciones promotoras representantes del sector sanitario privado*) afirmó que el texto surgió para *satisfacer una necesidad social, para tratar de adecuar el marco normativo a las necesidades del sector sanitario privado y para atestiguar el alto compromiso de los adheridos con el*

mercado multimedia con el alcance global de las comunicaciones no es posible utilizar los mecanismos tradicionales de regulación nacional confiando a una autoridad de carácter puramente administrativo la adopción de las medidas necesarias de control de los medios audiovisuales. Entre otras razones porque la comunicación y los derechos y libertades que le corresponden son una materia de alta sensibilidad política y social que afecta al ejercicio de derechos fundamentales vitales para la democracia y que aconseja, por tanto, que la aplicación de cualquier medida restrictiva se realice a través de instrumentos independientes del poder público, a la que responde la introducción de dichos mecanismos de la autorregulación.” Aun siendo sumamente interesantes las ideas del autor, no se analizan más profundamente pues no tienen concreción en el derecho fundamental a la protección de datos personales. Se apuntan en cuanto a la doctrina del autor en relación con el sector de las comunicaciones audiovisuales.

cumplimiento de la Ley Orgánica de Protección de Datos. Además, serían empresas conscientes de que en un centro sanitario privado destacaría la importancia del criterio asistencial, por el que *el paciente trasciende la posición de mero cliente o receptor de servicios para establecer con el Centro o empresa sanitaria, un diálogo en el que se establecen unos flujos de información dinámicos y multilaterales, que involucren a terceros, como son las aseguradoras, otros Centros sanitarios, médicos colaboradores y la misma comunidad o sociedad.* El cumplimiento en estas empresas de la obligación de protección de datos personales se transforma en medidas de seguridad sumamente onerosas y complejas, sin lugar a dudas. Además de la norma autorregulada, el código conforma también recomendaciones prácticas y modelos adaptados a las necesidades del sector privado de la salud. Otras empresas pueden adherirse gratuitamente, pero la adhesión no significa que se cumpliera con ello la normativa de protección de datos, sino que simplemente la norma autorregulada *guía* en su cumplimiento al nuevo adherido, además de encontrarse revisada por la AEPD. Existiría también un sistema de resolución pacífica de reclamaciones y denuncias de pacientes y otros colectivos evitando en lo posible la concurrencia de denuncias ante la AEPD, mediante un Comité Directivo, formado por representantes y expertos del sector. También en este sector sanitario intervendría e influiría la asociación Autocontrol, en cuanto a publicidad de medicamentos y centros médicos, terapias y otras manifestaciones empresariales que tiene como ámbito la salud de los ciudadanos.

3.4. La Autoridad de control de protección de datos y la norma autorregulada.

En la doctrina se extendería la línea de análisis sobre las Autoridades de Control dentro de los sistemas jurídicos con la conclusión de que no existe un concepto único para su delimitación dentro del sistema normativo español, por lo que es muy incierto tan siquiera pensar en una definición y concepción mundial.

Una vez que se afirma tan situación, definir qué es una Autoridad de control se convertiría en una búsqueda digna de otro trabajo académico más amplio, saltando el límite de este presente, delimitado al derecho fundamental a la protección de datos personales. Sin embargo, se hace necesario partir de una base conceptual, por lo cual se tomó la determinación de adoptar alguna de las definiciones de Autoridad de control vigentes en la doctrina, centradas en la figura de la Autoridad de control de protección de datos en España, que es la AEPD hasta este momento, vinculando su existencia a la posibilidad de la gestión autorregulada para la eficacia del derecho fundamental a la protección de datos personales.

La AEPD sería lo que se conoce con la denominación de Autoridad u Organismo independiente, que son una serie de entes de las AAPP que funcionan dentro de la Administración correspondiente, pero con autonomía de *carácter reforzado*, que no podría consistir en un quebranto de los vínculos que unirían la Autoridad independiente con el control del Parlamento, del Gobierno de la nación ni implican una ruptura con el sistema de control de los Tribunales. Existiría unanimidad doctrinal al considerar que las Autoridades independientes gozan de una *autonomía cualificada*, con un carácter de neutralidad frente al Gobierno para desarrollan una serie de funciones; por esa razón, las Autoridades independientes actuarían *libres de influencias políticas*, sin control administrativo ordinario, sus miembros son nombrados y cesados sin intervención gubernamental. También se encontrarían inscritas dentro de la denominación de *Administración instrumental* o *Administración descentralizada*, la cual respondería al principio de la descentralización funcional. Estos entes administrativos se crearían por razones de eficacia. Los diferentes sistemas jurídicos de que determinados tipos de funciones y servicios serían mejor atendidos desde organizaciones independientes de las AAPP. Una parte de la doctrina apuntaría a una diferencia entre Autoridades independientes y entes instrumentales, marcando que las Autoridades independientes no mantendrían ninguna relación de instrumentalidad con un ente denominado *matriz*, y en todo lo demás coincidirían ambas figuras administrativas. La doctrina se refugiaría en las diferentes competencias y funciones de las denominadas Autoridades u Organismos independientes para no acordar una definición (o definiciones) que los califi-

quen adecuadamente. Una breve introducción histórica indicaría que las Autoridades independientes serían en España un fenómeno jurídico relativamente reciente, pues se produjeron en los inicios de los años ochenta del pasado siglo XX. Con anterioridad la doctrina consideraría antecedentes de estas organizaciones a las Reales Academias, las Conferencia Hidrográficas o los Tribunales Económicos-Administrativos⁶⁶⁶.

La AEPD se conformaría en consonancia con el mandato implícito en el artículo 18.4 CE, junto con la doctrina del TC que otorgó rango de derecho fundamental al derecho a la autodeterminación informativa o derecho a la protección de datos personales, a través de la STC 292/2000, de 30 de noviembre (FJ 9) (tantas veces ya aludida por su importancia) en la que el TC explicitó que “al dar cumplimiento al mandato contenido en el artículo 18.4 CE, el legislador, sin excluir en modo alguno el recurso último a los órganos jurisdiccionales (...) no ha querido sin embargo que la protección de datos personales frente al uso de la informática se lleve a cabo exclusivamente en la vía judicial, esto, es, cuando ya se ha producido una lesión al derecho fundamental. Por el contrario, ha querido que dicha protección se lleve a cabo mediante el ejercicio por la AEPD, con carácter básicamente preventivo, de las funciones de control de los ficheros (...) y en su caso, a través de las reclamaciones de los afectados. En el FJ 13 el TC constató que “la creación de dicho ente (AEPD) y de las funciones atribuidas al mismo permiten garantizar el ejercicio por los ciudadanos del haz de facultades que integran el contenido del derecho fundamental a la protección de datos.”

La LOPD, a su vez, dedicó en su normativa diversos artículos a la AEPD, los más relevantes en el Título VI. Se estableció una Autoridad independiente de las AAPP, en primer lugar, porque sería necesaria una especialización tanto jurídica como técnica para tutelar el derecho fundamental a la protección de datos personales, capacidades que el poder judicial supuestamente no tenía en su conjunto; y, en segundo lugar, porque las AAPP serían también sujetos sometidos al control de la AEPD. Aquí se advertiría una diferencia de trato entre responsables de ficheros privados y responsables de ficheros públicos en cuanto al régimen sancionador (Título VII LOPD). Cuando se

⁶⁶⁶ Véase a este respecto el extenso análisis de SALVADOR MARTÍNEZ, M., *Autoridades Independientes*, Barcelona, 2002. que para este trabajo solamente se toman sus menciones hacia la AEPD.

tratase de ficheros públicos, la potestad sancionadora se considera como *compartida y limitada*, pues la AEPD iniciaría el correspondiente procedimiento sancionador que procediese, pero se transformaría en un procedimiento disciplinario, quedando al margen de su ámbito de actuación; sin embargo, cuando se tratase de ficheros privados la competencia de la AEPD es total y exclusiva, agotándose la vía administrativa con su decisión en forma de Resolución.

La AEPD se definió como una *autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos*. En sus funciones, *garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos, especialmente en cuanto a los derechos de información, acceso, rectificación, oposición y cancelación de datos*. En cuanto a su naturaleza jurídica, la AEPD es *un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se relaciona con el Gobierno a través del Ministerio de Justicia*⁶⁶⁷.

⁶⁶⁷ Son las definiciones que la propia AEPD publica en http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/index-ides-idphp.php Su marco normativo lo componen por una parte su normativa específica y por otra en las siguientes disposiciones que le son aplicables: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Título VI con rango de ley ordinaria); Real Decreto 1720/2007, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos; Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. El régimen jurídico aplicable es el Derecho Administrativo tanto en el ejercicio de sus competencias como en su régimen patrimonial y de contratación. Para el ejercicio de competencias, se rige por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (BOE 02.10.2015); para el Régimen patrimonial, resulta aplicable la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas (Disposición Adicional 5ª). Y para la contratación está sujeta al Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público (artículo 3). La AEPD cuenta con recursos humanos que provienen del Cuerpo de Funcionarios de las AAPP y personal laboral contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo.

En el año 2013 la AEPD publicó la Carta de servicios de la AEPD⁶⁶⁸. Es una relación informativa para los Órganos, Organismos y Entes Públicos y otras Entidades de la Administración General del Estado, dirigida a los ciudadanos y usuarios, sobre los servicios que tienen encomendados la AEPD, sobre los derechos que les asisten en relación con aquellos y sobre los compromisos de calidad en su prestación. La AEPD se organizó sobre una Dirección, que recaía en una persona física, el Consejo Consultivo, la Secretaría General y la Subdirección General de Inspección de datos, como cargos más relevantes⁶⁶⁹.

La intervención en un determinado sector de actividad con la pretensión de asegurar la correcta regulación y la garantía de un derecho fundamental se podría interpretar

El presupuesto se denomina como *presupuesto integrado*, con la debida independencia, en los Presupuestos Generales del Estado, aunque la AEPD está sometida a los preceptos de la Ley 47/2003, de 26 de noviembre, General Presupuestaria que le sean de aplicación. Mantiene, también, un control externo ejercido por el Tribunal Cuentas y el interno por la Intervención General del Estado (IGAE).

⁶⁶⁸

Véase

en

<http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/CartaServicioSAEPD.pdf> El origen de este documento estuvo vinculado a conseguir la mejora de los servicios públicos atendiendo a las demandas de los ciudadanos. En base a estas consideraciones se dictó el Real Decreto 951/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

⁶⁶⁹ En este momento de 2017, la Directora es Dña. Mar España Martí ostenta la representación de la Agencia y sus actos se consideran como actos propios de la Agencia. Sus resoluciones ponen fin a la vía administrativa y son recurribles ante la Sala de lo Contencioso de la Audiencia Nacional. Es nombrada por el Gobierno mediante Real Decreto de entre quienes componen el Consejo Consultivo y a propuesta del Ministro de Justicia. Tiene la consideración de alto cargo con rango de Subsecretario. Su mandato es de cuatro años. La Directora puede cesar por expiración del mandato, renuncia, fallecimiento o separación acordada por el Gobierno en caso de: incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por un delito doloso. La Directora no puede recibir instrucciones de ningún poder o autoridad y actúa con pleno sometimiento al Derecho. Ejerce sus funciones con dedicación exclusiva, plena independencia y total objetividad. Más información si se considera de interés en http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/el-director-ides-idphp.php

como una forma de protección ante los cambios sociales y económicos, producidos por el avance de la tecnología. A través de la autorregulación se trataría de promover la participación de la ciudadanía, de las empresas y de cualquier parte afectada para que sean ellos mismos los que realizasen una potestad normativa y una potestad disciplinaria. Si se dirige hacia una mayor eficacia de la regulación, la convergencia de la Autoridad de control y la autorregulación sería otro paso más para avanzar en el sentido de la protección de datos personales como derecho fundamental. En países europeos como Alemania, las Autoridades de control (también denominadas como instituciones autónomas) están compuestas por ciudadanos y se crearon precisamente como defensa de los DDFF frente al Estado o frente al Gobierno. No se realizó una doctrina unánime sobre si serían una forma de administración del Estado o una forma de administración o de regulación de la sociedad. Por esa razón, las críticas se basarían en que no se clarifica la posición de las Autoridades de control en una institución autorregulada dentro de la división de poderes tradicional y del principio del Estado de Derecho, pues se pensaría por parte de la doctrina que se privatizarían algunas áreas del Derecho público y se eliminarían partes del Derecho Administrativo en general, hablándose de un *Derecho público especial*. Lo que también se podría considerar objeto de análisis serían las formas de la AEPD en cuanto a su gestión, que algunos autores consideran de intromisión en las actividades de la sociedad (se recuerda al autor BOIX PALOP), la indeterminación o incluso contradicción de las Resoluciones de la AEPD y otras cuestiones a tener en cuenta si realmente, a través de la nueva normativa del RGPD, se tuviese un deseo de avance normalizador hacia el derecho fundamental para la protección de los datos personales. La norma europea reiteraría la importancia de las Autoridades de control en todo el desarrollo del RGPD, afirmando que cada Autoridad de control debe ser competente, en el territorio de su Estado miembro, para ejercer los poderes y desempeñar las funciones que se le confieran de conformidad con el RGPD (Considerando 122) marcando su carácter público pero también de su independencia en conformidad con la normativa europea, la cual le dedicó el Capítulo VI, artículos 51 a 59 RGPD, junto con otros que formularían la cooperación entre las Autoridades de control de los diferentes Estados miembros y la figura del

Comité Europeo de Protección de Datos. Como se dijo en otro espacio de este análisis, todo ello sería compatible con la autorregulación en lo que se denomina dentro del RGPD como Código de conducta.

3.5. Anexo orientativo: la visión de la protección de datos en las certificaciones de seguridad.

Según la visión aportada por las normas ISO, las tecnologías de la información son consideradas como críticas para el funcionamiento de la economía mundial, por lo que la sociedad demanda seguridad, calidad y fiabilidad a las empresas, en especial a los sectores más influyentes, como serían la industria, las tecnologías de la información y las comunicaciones, el transporte, la salud, las finanzas, junto con las importantísimas actividades empresariales de innovación y desarrollo, base sustancial del avance económico y social. Para la implementación de una gestión de seguridad armonizada con la actividad empresarial, las normas sobre seguridad se encontrarían firmemente relacionadas con la gestión de los servicios, de la seguridad de la información, de los riesgos corporativos y la seguridad de la continuidad en la actividad de la empresa (su negocio) frente a situaciones críticas que pongan en riesgo el correcto funcionamiento de la empresa u organización. En el escenario actual, las empresas demandan y consideran necesarios criterios de seguridad en los procesos y servicios que sean equiparables internacionalmente, cumpliendo la legalidad respecto a la privacidad de los datos (se entiende que también cumplirían la normativa europea de protección de datos personales). Con todo ello, la intención sería aportar a la sociedad transparencia, fiabilidad y seguridad en los servicios y en la innovación tecnológica constante, previniendo los incidentes que afecten a la continuidad del negocio, a través de un continuo avance que se muestra como indiscutible, cuyo punto de apoyo más importante es la formación y competencia de los trabajadores que interactúan en el entorno empresarial responsable. Se genera, además, una consolidada perspectiva de futuro, que se acompaña a través de normas reguladas por los Estados, como, en el

caso de España, las normas del Esquema Nacional de Seguridad, el Plan Nacional de Infraestructuras Críticas, las normas sobre protección de datos personales, el cumplimiento de la LSSI o de la LRAP.

La información en cualquier soporte y de cualquier tipología debe ser protegida siempre desde su creación, almacenamiento, procesamiento, distribución y, por último, su destrucción. Esta afirmación no admite la menor duda. El *ciclo de vida de la información* es muy importante para determinar la seguridad de una organización. La protección de la información se realizó siempre a lo largo de la Historia de la Humanidad en diferentes soportes y por muy diversos procesos. Pero será en el siglo XX cuando adquiera mayor relevancia.

Otro concepto a definir para establecer una gestión de seguridad es la definición de los sistemas de información asociados, los cuales se consideran que son las instalaciones actuales de hardware, software, redes de comunicaciones, procesos de gestión de información automatizados, permisos de accesos, administración del sistema, entre otros muchos que se proyectan cada día como novedosos, como puede ser actualmente el mencionado internet de las cosas o IoT. Estos sistemas deben ser fiables, robustos tanto ante imprevistos físicos como lógicos, para responder en situaciones no deseadas o problemáticas. Además, deben ser gestionados dentro del proceso del negocio y formar parte de los riesgos corporativos.

Por todo ello, las normas ISO aportan la siguiente definición de seguridad de la información como *preservación de la confidencialidad, integridad y disponibilidad inmediata y continua de la información; otras cualidades tales como autenticidad, no repudio, responsabilidad y fiabilidad pueden incluirse*.

Los conceptos y definiciones empleados por las normas ISO también son de interés. Por ejemplo, el concepto de amenaza, definido como *evento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales*; el concepto de riesgo, definido como *probabilidad de que una amenaza se materialice generando incertidumbre en la consecución de los objetivos definidos*. Otro concepto interesante es el de control, como *práctica, procedimiento o mecanismo*

que modifica el nivel de riesgo. El contexto, en el ámbito de la seguridad, se define como *entorno interno y externo en los cuales la organización busca alcanzar sus objetivos*. Quizá otra definición atractiva para los juristas sería la de sistema de información como *aplicaciones, servicios y activos tecnológicos y otros componentes de soporte*. Todas las definiciones se encuentran en continua conceptualización, por la actualización que supone nuevas integraciones, producto de las novedades tecnológicas.

Para las normas ISO 27000, las normas con mayor representatividad son las ISO/IEC 27001:2013., denominadas como Requisitos de los Sistemas de Gestión de Seguridad de la Información y las normas ISO/IEC 27002:2013., denominadas como de buenas prácticas para la Gestión de Seguridad de la Información. Ambas se exponen en este anexo someramente.

La norma ISO/IEC 27001:2013 es un procedimiento de Gestión de Seguridad de la Información con Certificación de los sistemas que dan soporte a los procesos del negocio, minimizando los riesgos y asegurando su continuidad frente a imprevistos o desastres. Es una norma *preventiva* basada en la valoración y tratamiento sistemático de los riesgos en materia de seguridad de la información. Asume los principios de ISO 31000. Así mismo, es integrable con otras normas ISO. Se caracteriza por preservar, al menos la confidencialidad, la integridad y la disponibilidad de los datos. Propone un catálogo mínimo de controles, detallados en ISO 27002.

El contenido de la norma ISO 27001 se podría resumir en un listado de requisitos (o Controles), que se determinan por constar de tareas a cumplimentar y definir, como son la política, la organización y los recursos humanos en relación a la seguridad; el control de accesos, la criptografía o encriptación de información; la seguridad física y ambiental de los recursos, tanto humanos como automatizados o también, la seguridad en las operaciones y en las comunicaciones. También se tendrían en cuenta la adquisición, desarrollo y mantenimiento de sistemas automatizados, punto de análisis con máxima relevancia en cuestiones de seguridad. Otra cuestión a tener en cuenta sería la relación con los diferentes proveedores de la empresa u organización, los cuales deben cumplir las normativas del cliente certificado o estar a su vez certificados en seguridad de datos. La gestión de los incidentes y de la continuidad del negocio o

actividad son también aspectos relevantes. Todo ello será controlado regularmente en su cumplimiento por la organización en general.

La norma ISO 27001 se complementa con la norma ISO 27002, la cual define las directrices necesarias para dar soporte a la interpretación e implementación en los sistemas de información de los controles definidos en la norma ISO/IEC 27001 sirviendo como una forma de *manual* de dicha norma. Por ejemplo, define qué se requiere en términos de seguridad de la información, pero no define cómo se ha de cumplir esos requisitos. La norma es tecnológicamente neutral. Por otro lado, especifica un conjunto detallado de controles y buenas prácticas para gestionar la seguridad de la información. Su correcta implantación garantiza un nivel de seguridad adecuado a las circunstancias de la organización manteniendo la confidencialidad, integridad y disponibilidad de los activos y datos.

Para la normativa ISO, el principio de proporcionalidad tiene una lectura económica, pues *la inversión tiene que ser proporcional al riesgo*. Las necesidades se determinan por un análisis de riesgos pormenorizado para cada caso en concreto. El análisis de riesgo determina dos cuestiones sumamente importantes: por un lado, el impacto económico de un fallo en la seguridad; por otro lado, la probabilidad realista de que ocurra el mencionado riesgo y en qué medida afecta a los sistemas. El riesgo se define en las normas ISO como *la probabilidad de que se materialice una amenaza determinada sobre un activo generando un impacto en el mismo*. Se resume en una simple ecuación como

$$\text{RIESGO} = \text{Probabilidad} * \text{Impacto}$$

El riesgo se diferencia a su vez en intrínseco, como la posibilidad de que se produzca un impacto determinado, y en efectivo o residual, como riesgo que permanece tras la aplicación de salvaguardas o medidas de seguridad. La seguridad absoluta no existe, como ya se comentó en este trabajo. Las empresas y organizaciones estarían interesadas no sólo en el cumplimiento de parámetros de eficacia y efectividad, sino en llegar también a la eficiencia.

Partes relevantes de la organización para la generación de un sistema de seguridad serían, además de los responsables del análisis del riesgo, cuestión en la que intervienen especialmente los responsables de sistemas automatizados, los responsables de dirección, el consejo de administración, el departamento jurídico, el departamento de recursos humanos, entre otros. Dentro de otro entorno, en un ámbito estatal o supraestatal, se encontrarían los diferentes colectivos u organizaciones afectadas por la seguridad de la información y de los datos, como son clientes y proveedores, socios o partners de negocios, proveedores de seguridad en general, consultores y asociaciones profesionales, órganos legislativos y de gobierno, junto con organizaciones internacionales o sectoriales que pudieran estar involucradas en la gestión de la organización.

Como un limitado resumen se mencionan en este anexo las fases de un proceso de implantación de seguridad. Lo primero es determinar las necesidades del cliente, a través del conocimiento de su entorno, principalmente. Con esos datos, se propondría una solución realista y adecuada, además de fijar un alcance de objetivos futuros de gestión. Para ello se necesita identificar los procesos clave o estratégicos del negocio o actividad, desarrollar un análisis de riesgo, determinar los niveles de actuación y seleccionar los objetivos y controles. Una vez terminada esta fase, es muy importante concretar cómo se va a implantar cada control de la norma ISO, por lo que se elabora una declaración de aplicabilidad. La implementación de la norma se llevaría a término por medio de controles físicos, técnicos y organizativos, los cuales se auditarían y revisarían por la entidad certificadora, y si fuera necesario, se desarrollarían funciones correctivas.

Lógicamente que las entidades certificadoras en normas ISO extienden los beneficios de su certificación, es el objeto de su actividad económica. Aun así, existen afirmaciones que se manifiestan como ciertas por el largo tiempo en que las normas ISO están presentes en la economía. Algunos de esos beneficios se basan en la realización de políticas y procedimientos reconocidos internacionalmente, acordes con criterios, estructuras y metodologías generalmente aceptados. Aporta a las organizaciones una protección de seguridad y privacidad que generan una buena dirección de empresas y un compromiso con la seguridad de todos los niveles de la organización. Además, pro-

porciona una diferenciación certificada en el mercado, con una notable influencia positiva en la imagen de la empresa, demostrando credibilidad, confianza y satisfacción ante las partes más interesadas, como son los socios, los clientes y los ciudadanos en general. Quizá el aspecto más importante sea la disminución patente de riesgos, demostrándose a su vez, una cuidada y acertada gestión. Todo ello contribuyó en los pasados años al bienestar general de nuestra cultura occidental y con ello, a la extensión de muchos valores importantes a multitud de aspectos, tanto económicos como sociales.

Las críticas al sistema ISO existen. Desde su coste hasta su posible adquisición sin implantación de los sistemas, simplemente por el pago de su precio, como una especie de requisito económico para poder operar dentro de un ámbito determinado. Ese análisis no corresponde a este trabajo. Sí se afirma con rotundidad la grata experiencia profesional que significa colaborar con empresas que realmente aplican la normativa ISO. Se agradece, por último, a los responsables de *Bureau Veritas* toda la atención personal recibida para la redacción de este texto, con el aporte de información que no puede ser referente académico, pero sí forma parte de este anexo como base para su redacción.

CONCLUSIONES Y PROPUESTAS.

PRIMERA. Los derechos fundamentales y el desarrollo de las sociedades se encuentran íntimamente ligados. No se puede entender el significado de los avances sociales sin atender a los diferentes derechos que se fueron reconociendo a lo largo de la historia. En este sentido, el derecho fundamental a la protección de datos personales se configuró como un avance social e individual a lo largo del siglo XX y principios del siglo XXI. Se trata de un derecho fundamental de desarrollo universal, pues partiendo de las necesidades del comercio entre diversos Estados (como en el caso de la UE) y los diversos avances de las tecnologías de la comunicación y de la información, fue desarrollándose a través de pronunciamientos jurisprudenciales un derecho individual a la protección de datos que, a su vez, contribuye a la protección efectiva de otros derechos fundamentales. El proceso de reconocimiento del derecho a la protección de datos se produjo mediante su desglose de otros derechos fundamentales como el derecho a la intimidad personal y familiar o el derecho a la privacidad en el contexto del derecho anglosajón.

SEGUNDA. La UE ha alcanzado acuerdos de mínimos e irregulares en cuanto a su eficacia en materia de protección de datos. Ahora bien, especialmente durante los últimos años, se observa una clara tendencia a la convergencia de los diferentes sistemas jurídicos de los Estados miembros, esto es, a la homogeneización de normativas, no solamente en protección de datos, sino también en otras materias con incidencia en el tratamiento de datos personales. De hecho, son escasas las actividades tanto económico-privadas como puramente administrativas-públicas que quedan excluidas de la regulación comunitaria. La normativa europea tiene una clara *vis expansiva* en las relaciones con terceros Estados, pues todas las sociedades se encuentran interrelacionadas por el comercio u otros intercambios culturales, científicos, ocio, etc.

TERCERA. La ausencia de una regulación trasnacional sobre Internet, en el entendimiento de que se trata de la mejor forma de asegurar la libertad, facilita la vulneración del derecho a la protección de datos y de otros derechos fundamentales por parte de particulares (individuos o empresas). Por tanto, se hace necesario revisar la

función del Estado como garante de los derechos fundamentales. Obviamente, la aludida función se debe realizar en coordinación con otros Estados, Entidades supranacionales u organizaciones internacionales. En este sentido, desde hace muchos años, la UE abogó por un sistema de autorregulación controlado por las Autoridades correspondientes y dotado de sistemas para el cumplimiento efectivo de la norma sobre protección de datos.

Las empresas de tecnología también deberían ser más conscientes de su responsabilidad en cuanto al respeto de los DDFF. Deben generar productos respetuosos con la normativa sobre protección de datos, con los principios de privacidad por defecto y desde el diseño (*privacy by desing*), junto con sistemas de gestión transparentes en sus políticas de privacidad.

El equilibrio entre la actividad económica, su control administrativo y los DDFF, no solamente se debe aplicar al derecho fundamental a la protección de datos personales, sino también el conjunto de Derechos, al conjunto del sistema jurídico, del que los DDFF son su máximo exponente, su inspiración y su base legal.

CUARTA. Las actividades antijurídicas que se ejecutan a través de las nuevas tecnologías de la comunicación no difieren en sus resultados de las mismas conductas realizadas por medios más convencionales o conocidos dentro del sistema jurídico. El método para la vulneración de un derecho no debe implicar en todos los casos un nuevo derecho o un nuevo hecho antijurídico. Por ejemplo, la difamación o la intromisión en la intimidad no resultan diferentes si se realizan mediante un dibujo o una cámara web. El asunto reside actualmente en la divulgación de hechos mediante las tecnologías de la comunicación y en las dimensiones que pudieran conseguir con la exposición amplia y continuada de situaciones, que no son predecibles cuando los datos se encuentran dentro de una red de comunicaciones sin control por parte del perjudicado por el tratamiento de su información personal. Desde la diferencia entre intromisión y vulneración, llegando a aspectos claramente delictivos, son necesarias nuevas herramientas técnicas a disposición de los ciudadanos, con suficiente pedagogía en su utili-

zación, para que la autodeterminación informativa sea una realidad. Lo razonable desde la perspectiva mantenida en el presente estudio es la concienciación de las empresas y los particulares sobre la necesidad de utilizar la identidad electrónica verificada en todo tipo de actuaciones realizadas en la red. Uno de esos instrumentos puede ser el DNle o identidad electrónica verificada, cuyo desconocimiento conduce a su escasa utilización.

QUINTA. El nuevo RGPD, que entrará en vigor en mayo de 2018, se presentó como una norma muy extensa que trata de proporcionar una regulación del derecho fundamental a la protección de datos personales común para toda la UE. También tiene la finalidad de mantener un mercado único y garantizar el flujo de información entre los diferentes operadores en el territorio de los Estados miembros. El cumplimiento efectivo de la norma descansa en un sistema de sanciones administrativas.

A pesar del enorme esfuerzo realizado en cuanto a la delimitación de los puestos de aplicación del nuevo reglamento comunitario, lo cierto es no se resuelve totalmente la cuestión del tratamiento de datos desconocidos o con terceros países. El RGPD se aplicará a todas las organizaciones dentro del territorio de la UE y a todas las organizaciones externas que realicen operaciones mercantiles o comerciales con la UE, lo cual significa que muchas organizaciones y terceros Estados deben cumplir el RGPD. En consecuencia, muchas empresas perderán el interés en establecer relaciones comerciales con terceras empresas que cumplan con la normativa europea sobre protección de datos personales. En un futuro, más o menos próximo, se comprobará si realmente el RGPD es eficaz en las relaciones comerciales.

La norma europea no distingue entre nacionales de los diferentes Estados miembros ni sobre su ubicación. Si los responsables o encargados del tratamiento de datos personales de ciudadanos europeos no se encontrarán dentro del territorio de la UE, deberán designar un representante que resida en alguno de los Estados miembros.

El RGPD amplía la definición de *dato personal*. Además de lo que pudiera ser toda información sobre una persona física identificada o identificable (lo que el RGPD denomina *interesado*), se define como persona identificable a toda persona cuya identi-

dad pueda determinarse, directa o indirectamente, mediante identificadores electrónicos o en línea, números de teléfono, datos de localización, datos de la identidad física, fisiológica, genética, psíquica, económica, cultural o social. Se trata de un listado abierto, lo cual permite considerar como dato personal a cualquier información que se pudiera utilizar para la identificación del titular en un futuro. Se recuerda en este punto lo expuesto respecto a las últimas tecnologías de tratamiento de grandes bases de datos, que teóricamente podrían identificar a una persona con datos no personales después de un tratamiento de otros datos relativos a su entorno (consumo, páginas web visitadas, ocio, trabajo, intereses, relaciones, geolocalización, entre otros factores).

SEXTA. El principio de transparencia es un eje fundamental para el tratamiento de datos personales con fines limitados y consecuencias de mínimo alcance para los titulares. Otros aspectos, como la confidencialidad, la integridad, la seguridad de los datos frente a pérdidas, destrucciones o daños, intencionados o no, son considerados de interés para la adaptación de procesos en las organizaciones vinculadas a los tratamientos de datos personales, que serían una mayoría.

SÉPTIMA. Salvo en los casos de requerimientos legales o de urgencia, el consentimiento del titular resulta determinante para la norma europea de protección de datos. El consentimiento debe ser claro e inequívoco, no considerándose así el silencio o consentimiento tácito, el obtenido mediante casillas previamente marcadas o mediante cláusulas abiertas. El RGPD explicita que el consentimiento debe otorgarse para cada una de las actividades de tratamiento de datos personales, sin cláusulas o formulas ambiguas, de forma escrita o similar (grabación de audio y/o video, por ejemplo); en cualquier caso, siempre debe poder ser probado, por lo que la documentación del consentimiento se presenta como un elemento crucial, pues además el consentimiento se debería revocar o retirar de forma sencilla y eficaz. El RGPD requiere que el responsable del tratamiento proporcione un método de revocación del consentimiento tan sencillo como el proceso para su obtención.

OCTAVA. Una novedad del RGPD también reseñable consiste en la exigencia de un registro de las actividades de tratamiento. En ausencia de la obligación de inscripción

de ficheros ante la Autoridad de control (AEPD, en el caso de España), el RGPD obliga a las organizaciones y empresas al mantenimiento de un conjunto de informaciones o registro sobre qué tipo de datos se tratan por el responsable o el encargado del tratamiento, dónde se tratan y por qué razón (artículo 30 RGPD). Los Registros estarán a disposición de la Autoridad de control si se solicitan.

También se debe realizar una *evaluación de impacto o de riesgo* para los derechos de los titulares en el tratamiento de datos que se desarrolle, quedando pendiente la determinación por la Autoridad de control de cuáles son las situaciones en que tales evaluaciones son obligatorias. En estos dos puntos se está a lo que se denominó como *protección de datos desde el diseño y por defecto* (artículo 25 RGPD). El RGPD no especifica ninguna de estas obligaciones, ni cómo debe implementarse el grado de seguridad, o el tipo de tratamiento y medios adecuados, los formularios para recabar el consentimiento, entre otros factores a tener en cuenta por cualquier organización empresarial. Deberán ser las propias organizaciones a través de sus responsables (personas con apoderamientos o simplemente los propietarios de la empresa) quienes deberán probar ante la Autoridad de control que cumplen la normativa europea, teniendo en cuenta la seguridad de los datos desde el diseño de sus sistemas de gestión de información personal y por defecto.

NOVENA. La figura novedosa del Delegado de protección de datos (DPO) será necesaria si los datos son tratados por una Autoridad, organización u organismo público, salvo los Tribunales en su función judicial; también si las actividades del responsable o encargado del tratamiento de los datos personales se realiza por medio de una gestión masiva de datos; y por último, en el caso de que las actividades del responsable o encargado del tratamiento se desarrollasen con el tratamiento masivo de datos especialmente protegidos o de datos relativos a infracciones y condenas de ámbito penal. Se podría suponer que cualquier organización empresarial necesitaría un DPO para solventar los asuntos que se presentaran en el desarrollo de la actividad, pero también con la intención de prever cualquier tipología de riesgo en cuanto a seguridad de datos. Al objeto de cumplir con las obligaciones del RGPD, es probable y recomendable que grupos de pequeñas organizaciones mancomunen los servicios de un DPO co-

mo, por ejemplo, en el caso de pequeñas clínicas médicas u odontológicas, despachos de abogados que no se compongan de un número importante de socios o empleados, empresas de limpieza y mantenimiento de instalaciones estratégicas o de seguridad, etc. El tratamiento de categorías especiales de datos personales (art. 9 RGPD, datos concernientes al origen étnico o racial, ideología política o sindical, datos genéticos, datos biométricos que identificaran a una persona unívocamente, datos relativos a la salud, a la vida sexual o a la orientación sexual) se encuentra seriamente limitado o prohibido (como ya sucede en la vigente LOPD) sin consentimiento del titular de los datos, o bien se podrían tratar por razones de urgencia ineludible y también por mandato legal o judicial. Al respecto, el DPD aportará a las organizaciones empresariales los conocimientos y la seguridad necesarias para el cumplimiento efectivo del derecho fundamental a la protección de datos personales, con un papel decisivo para que se protejan los derechos de los ciudadanos desde la gestión, antes de la vulneración, siendo además un enlace profesional con las Autoridades de control, las AAPP y la sociedad en su conjunto. Sus funciones se centrarían en asegurar que el responsable o el encargado del tratamiento de datos personales cumplieran las normas sobre protección de datos, asesorar a los responsables de la empresa, en especial a los responsables de personal y recursos humanos, supervisar las evaluaciones de impacto y de riesgo, realizar cuantos informes fueran necesarios, entre otras posibles funciones. Para desarrollar todas estas competencias resulta evidente la necesidad de una cualificación profesional específica, que debería ser incluso certificada, cuestión que hasta el momento actual no se ha abordado en España.

DÉCIMA. El RGPD introduce la obligación de poner en conocimiento de las Autoridades de control y de los titulares de datos cualquier violación de seguridad de los datos personales, obligación que anteriormente no se consideraba necesaria. Posiblemente se dieron frecuentes violaciones en la seguridad de diversas empresas que no se pusieron en conocimiento de las Autoridades de control ni de los titulares de los datos. Con la nueva norma, se deberán notificar las violaciones de seguridad en el plazo máximo de 72 horas desde su conocimiento, siendo posible un periodo mayor sólo en el caso de que exista una circunstancia que no lo haga viable. Se hace necesario un pro-

cedimiento adecuado para la descripción de las medidas de seguridad y de contingencia que se generarán para abordar esa situación, con la descripción de los posibles riesgos y efectos secundarios. En caso de constituir una determinada violación de la seguridad un riesgo para los DDFF de los titulares de los datos personales, el responsable del tratamiento deberá ponerse en contacto inmediato con ellos. Por prevención frente a estas posibles violaciones de seguridad, el RGPD incide frecuentemente en la necesidad de seudonimización, anonimización o cifrado de datos. Otra excelente herramienta para proteger los datos personales es la denominada copia de restauración, la cual permite reintegrar la información si sufriera merma o violación. Todo ello supone minimizar también el riesgo y el impacto de acciones ilícitas o desafortunadas. Se trata de la *implementación de un sistema holístico de seguridad de la información* en la gestión de las organizaciones, que incluye la protección de datos personales y la gestión de datos en general. Los costes de las medidas y sistemas de seguridad se verían compensados en el tiempo con mejoras perceptibles en la eficacia, eficiencia e incluso efectividad dentro de las empresas. Lejos de suponer un coste para cumplir un derecho fundamental, supondrían un aliciente de progreso y mejora del posicionamiento en el mercado y las relaciones con proveedores y clientes.

UNDÉCIMA. En referencia a las transferencias internacionales de datos (TID) para considerarlas lícitas se establece la obligación del cumplimiento de la normativa expresada en el Capítulo V RGPD. La normativa está diseñada para garantizar, en la medida de lo posible, la protección de los DDFF de los ciudadanos y residentes en la UE, en especial para garantizar el derecho a la protección de datos personales. Las TID requieren garantías específicas para su tutela efectiva. Se trata de conseguir que las TID sólo se puedan realizar entre Estados u organizaciones que tengan implementadas similares medidas de seguridad y protección para los datos personales. En este sentido, la redacción e incorporación de normas corporativas vinculantes o BCR será una herramienta muy estimable para conseguir mayor protección en las actividades empresariales que impliquen TID, que en este momento podrían considerarse como mayoritarias, a través de los sistemas de almacenamiento en nube o *cloud*. Los modelos de BCR deben ser aprobados por las Autoridades de control de protección de datos

personales que resulten competentes en cada Estado miembro. Resultará conveniente que los modelos para definir las BCR sean comunes a todo el EEE para evitar distorsiones de los diferentes sistemas jurídicos de los Estados miembros. Junto con las BCR se prevé la implementación de sistemas de autorregulación o normas de conducta para las relaciones internacionales, así como las diversas certificaciones en protección de datos por la UE o por entidades independientes.

DUODÉCIMA. Como primera iniciativa para el cumplimiento del RGPD se considera necesaria e imprescindible la auditoría profesional de protección de datos personales. En una auditoría de protección de datos personales se establece, en primer lugar, la tipología de datos que son objeto del tratamiento, cómo son tratados (automatizada o no automatizadamente), quién tiene acceso a los mismos, desde dónde, cómo y la finalidad del mismo, también cómo son almacenados, dónde y por quién. Se conoce si existen duplicados o copias de los datos personales dentro y fuera de la organización, distinguiendo esta finalidad de almacenamiento de la finalidad propia del tratamiento. En un segundo término se examina la finalidad para su recabación, al igual que la recabación del obligado consentimiento de los titulares de los datos personales, entre otras cuestiones que cualquier auditoría de datos aborda en un primer estadio para cada caso concreto. Dentro de las auditorías sobre protección de datos destaca el análisis de las *evaluaciones de impacto*, relativas a la protección de datos personales. Su determinación es muy importante para diseñar un sistema de prevención y tratamiento de futuro. Todo ello sin olvidar la obligación de documentar el cumplimiento de la normativa, en cuyo punto más destacable se situaría las pruebas de consentimiento de los titulares de datos personales para el tratamiento y finalidad expresamente informados, al igual que se debería probar con documentación suficiente que se implementaron todas las medidas de seguridad necesarias para mitigar cualquier posible riesgo o consecuencia de la una violación en la seguridad, o al menos, medidas que minimizaran las probabilidades y las consecuencias. Si se subcontrataran servicios de tratamiento de datos, se deberán solicitar las garantías necesarias por el responsable del tratamiento. La seguridad se basa en el control de accesos a la información, tanto acceso físico como acceso lógico. En este punto, convergen las discipli-

nas jurídicas y de tecnología, tanto de comunicaciones como informática, además de la importantísima gestión y administración de la empresa en general.

DECIMOTERCERA. La observancia de la normativa sobre protección de datos personales se encomienda al Comité Europeo de Protección de datos. El Comité se compone de un representante de cada Estado Miembro y su Autoridad de control. Se pudiera esperar mejoras en las posibles orientaciones de las Autoridades de control de cada Estado miembro para el cumplimiento del derecho fundamental a la protección de datos, como pudieran ser las indicaciones específicas para los formularios de recabación del consentimiento informado, la cumplimentación de documentación sobre las medidas de seguridad implementadas, impactos de riesgos y violaciones de la protección de datos, certificaciones *a priori* de las organizaciones y sus medidas de seguridad, al mismo tiempo que se autorizan las TID, como ejemplos. De esta forma, se fomenta el cumplimiento de la normativa sin recurrir a las cuantiosas multas, que no siempre serían la solución, sin olvidar que una sanción se impone después de un incidente dañoso, mientras que el espíritu de un derecho de protección sería actuar *antes de los hechos* mediante la prevención.

DECIMOCUARTA. El tratamiento de datos personales en materia religiosa necesita una actualización importante. Una posibilidad sería la gestión conjunta de la Iglesia Católica (IC) y el Estado español de los Libros con datos personales que mantiene históricamente y en la actualidad la IC, en forma de un archivo histórico debidamente organizado. Otra propuesta sería la absoluta modernización de la gestión y tratamiento de datos personales por los representantes de la IC para actos convalidados entre el Derecho Civil y el Canónico, como es el matrimonio. En este caso, la gestión electrónica de las AAPP es evidente que se debe ampliar a este acto y la gestión de la IC. Para otros actos documentados, como la impartición de Sacramentos (bautismo, comunión), también sería deseable (cuando no obligado) un cumplimiento de la normativa del RGPD, en vigor dentro de pocos meses para toda la UE, con un control territorial de cada Estado miembro y de colaboración conjunta. Se tienen en este estudio serias dudas sobre la procedencia de tratamiento de datos personales por organizaciones denominadas religiosas o de cualquier tipo de creencias que no respeten los DDFF ni

los más básicos DDHH. En estos casos, no sólo se debe controlar el cumplimiento de las normas sobre protección de datos, también se debería por parte del Estado establecer la pertinencia y legalidad de tales actividades, siendo el primer paso la prohibición de tratamientos de datos personales para este tipo de asociaciones de creencias o comunidades religiosas.

DECIMOQUINTA. Se considera imprescindible promover incentivos y ayudas públicas para las pequeñas y medianas empresas, trabajadores autónomos y profesionales de pequeños medios económicos (en general PYMES). Se trata de una medida posible y acorde al mandato del artículo 9.2 CE, pues facilitaría la efectividad del derecho a la protección de datos. Para ellos sería muy conveniente que el Estado realizara formularios acordes a su actividad aprobados por la Autoridad de control y ponerlos a su disposición, también sería apropiado que tuvieran acceso a un DPO compartido por el gremio o profesión, además de sistemas de almacenamiento en remoto o en *nube* certificados por un coste asequible o de forma gratuita mantenidos por el Estado. Se promovería la seguridad en las PYMES, sin que el coste del cumplimiento de las obligaciones sobre protección de datos supusiera una merma de sus ingresos. Así también, el Estado mantendría la posibilidad de garantizar el derecho de los ciudadanos afectados por el tratamiento de datos de las PYMES. Al igual que el cumplimiento de otras obligaciones con las AAPP, se tendrían a disposición de quien lo solicitara, Certificados y documentación de que la empresa tiene sus datos depositados en los servidores protegidos que el Estado pusiera a disposición de estos profesionales, como ocurre, por ejemplo, en el cumplimiento de las obligaciones con la Hacienda Pública o la Seguridad Social, las cuales actúan a través de medios electrónicos. Esta misma idea se puede aplicar para las grandes corporaciones, si lo consideran conveniente, con un coste determinado, pues se presupone a las empresas de ciertos niveles económicos los suficientes recursos como para no necesitar de ayudas estatales, más bien podrían proveer entre los profesionales con los que desarrollan su actividad un sistema conjunto de seguridad de datos personales para gestionar voluntariamente su protección, acción que también debería ser reconocida por el Estado, por medio de Certificados que avalarán esta buena práctica.

DECIMOSEXTA. El ejercicio del derecho de supresión (*derecho al olvido*) requiere, por una parte, del compromiso de las empresas de buscadores, que son las obligadas a no indexar datos de personas identificables, y, por otra parte, la provisión de accesos efectivos a organismos estatales para supresión de datos personales, evitando la discriminación que supondría para determinados ciudadanos sin recursos económicos no poder atender los honorarios de empresas dedicadas a la supresión de datos. Sería imposible de comprender que los sistemas de publicidad del Estado sí respetaran la protección de datos personales en Sentencias y Boletines oficiales, pero las empresas privadas gozaran de total impunidad. Todo ello respetando el derecho a la libertad de expresión e información, diferenciando entre lo que significa la relevancia pública de la información en un momento determinado, frente al acceso a las hemerotecas digitales, cuya información se refiere a hechos pasados, y, por tanto, sólo significativa desde la perspectiva de la investigación periodística, histórica, etc. Sobre la cuestión, téngase en cuenta que los hechos pasados cuya difusión se reitera en el tiempo dan la sensación de hecho continuado. En el caso de delitos pueden imposibilitar la reinserción de las personas. La indexación de información y la difusión continuada de los hechos por los medios de comunicación y los buscadores restringen la reinserción social efectiva de los ciudadanos.

DECIMOSÉPTIMA. En cuanto a los casos de colisión del derecho a la libertad de expresión e información y el derecho a la protección de datos, se considera que la reciente STEDH, caso *Paulina Rubio*, sintetiza claramente los mandatos dirigidos a los poderes públicos para la protección de la vida privada y, por tanto, de los datos personales publicados y divulgados, imponiendo al Gobierno nacional la obligación (deberes positivos) de proteger los derechos de las personas de relevancia pública (en el caso concreto, una celebridad). Se determina qué información jamás puede ser objeto de una tertulia televisada, de comentarios en las redes sociales o de cualquier otro tratamiento de datos (léase información en formato de texto o en formato audiovisual). Por lógica, aspectos tan íntimos como la situación de salud de un personaje público, una intervención de interrupción de embarazo o cualquier otro contenido sensible, convierten esos contenidos en objeto de protección de datos, pero también de pro-

tección respecto al derecho a la intimidad personal y eventualmente del derecho al honor. La definición de lo que se considera información relevante es difícil sin llegar en algunos casos a la censura, pero lo que sí se puede saber, sin lugar a dudas, es lo que no constituye información relevante.

DECIMOCTAVA. Finalmente se considera necesario reformar el artículo 18.4 CE al objeto de adaptarlo a la realidad social. Dada su transcendencia supranacional, el derecho fundamental a la protección de datos debería reformularse en su delimitación dentro de las líneas maestras que se han ido forjando en el ámbito de la Unión Europea y del Convenio Europeo de Derechos Humanos.

Los Derechos Fundamentales y las normas de protección de datos personales.
Práctica empresarial y ciudadana.

Dña. María Montserrat Velasco Nájera

Dirigida por: Dr. D. Antonio Magdaleno Alegría, Profesor de la Universidad de Cantabria.

Página 564 | 606

BIBLIOGRAFÍA

- ABA CATOIRA, ANA, *La limitación de los Derechos en la Jurisprudencia del Tribunal Constitucional español*, Tirant Lo Blanch, Valencia, 1999.
- ABELLÁN GARCÍA, JOSÉ; MARTINEZ GÓMEZ, LUIS, *El Pensamiento español de Séneca a Zubiri*, UNED, Madrid, 1977.
- ABELLÁN GARCÍA SÁNCHEZ, FERNANDO, "Los análisis genéticos dentro de la Ley de Investigación Biomédica", *Revista de la Escuela de Medicina Legal*, junio, 2009.
- ABERASTURI GORRIÑO, UNAI, "La cesión de datos de salud fuera del ámbito sanitario", *Revista vasca de Administración Pública*, nº 91, 2011, pág.17-101.
- ABRIL, PATRICIA, "La intimidad europea frente a la privacidad americana", *Indret: Revista para el Análisis del Derecho*, nº 1, 2014.
- ADSUARA VARELA, BORJA , "Algunas consideraciones previas sobre el comercio electrónico", *Información Comercial Española, ICE: Revista de economía*, nº 813, 2004, pág.15-26.
- ALAMILLO DOMINGO, IGNACIO, "La identidad electrónica en la red." *Derecho y redes sociales*, Civitas, Madrid, 2010.
- ALBADALEJO, MANUEL, *Derecho Civil I*, Edisofer, S.L., Madrid, 2002.
- ALEGRE ÁVILA, JUAN MANUEL., "Interceptación de comunicaciones electrónicas y rango normativo", *Protección de datos y proceso penal*, Madrid, 2011.
- ALEXY, ROBERT, *Teoría de los derechos fundamentales (Theorie der Grundrechte, 1986)*, Centro de Estudios Constitucionales, Madrid, 1993,
- "Los derechos fundamentales y el principio de proporcionalidad", *Revista Española de Derecho Constitucional*, nº 91, 2011, pág.11-29.
- ALMUZARA ALMAIDA , CRISTINA, *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, Madrid, 2005.

- ALONSO RIMO, ALBERTO, "La publicidad de los antecedentes penales como estrategia de prevención del delito.", *Revista General de Derecho Penal*, nº 17, 2012.
- ÁLVAREZ CIVANTOS, ÓSCAR J., *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Comares, Granada, 2008.
- ÁLVAREZ GARCÍA, FRANCISCO JAVIER, "El acceso por parte de las Fuerzas y Cuerpos de Seguridad del Estado a ficheros de datos personales", *Protección de datos y proceso penal*, Madrid, 2010, pág. 53-88.
- ÁLVAREZ GONZÁLEZ, SUSANA, *Derechos Fundamentales y protección de datos genéticos*, Dykinson, Madrid, 2008.
- "La protección de los datos genéticos de carácter personal", *Derechos Humanos y protección de datos personales en el siglo XXI*, Punto Rojo Libros, 2013.
- ÁLVAREZ RIGAUDIAS, CECILIA, "El poder del usuario digital", *Hacia un nuevo Derecho Europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015.
- "Las Transferencias Internacionales de datos personales y el nivel equiparable o adecuado de protección".
- <http://www.uria.com/documentos/publicaciones/1467/documento/art1.pdf?id=2064>,
- "Comentario a los artículos 33 y 34 LOPD. Las Transferencias Internacionales de datos personales". *Comentario a la Ley de Protección de Datos de Carácter Personal*, Aranzadi, , 2010,
- APARICIO SALOM , JAVIER, "El tercero al que se le comunican los datos. Un tercer género entre quienes tratan datos.", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 34, 2014.
- "Comentario al artículo 4. Principios de la LOPD. La Calidad de datos.", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Madrid, 2010.
- ARCE JANÁRIZ, ALBERTO, "El Derecho a la intimidad; de Samuel D. Warren y Louis Brandeis", *Revista Española de Derecho constitucional*, nº 47, 1996.

- ARENAS RAMIRO, MÓNICA, "La protección de datos personales en los países de la Unión Europea", *Revista jurídica de Castilla y León.*, nº 16, 2008.
- "Reforzando el ejercicio del derecho a la protección de datos personales: viejas y nuevas facultades", *Hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015.
- ÁRIAS MÁIZ, VICENTE, "Comentario al artículo 6 LOPD. Una Excepción no contemplada en el artículo 6 LOPD: El uso de datos personales por medios de comunicación." *Comentario a la Ley Orgánica de Protección de Datos de Carácter Persona*, Aranzadi, Madrid, 2010.
- ARIAS POU, MARÍA, *Manual Práctico de Comercio Electrónico*, La Ley, Madrid, 2006.
- ARISTÓTELES, *Política*, S.L.U. Espasa Libros, Madrid, 2006.
- ARROYO JIMÉNEZ, LUIS, "Participación electrónica y elaboración de normas administrativas en España y en los Estados Unidos de América", *Centro de estudios europeos Luis Ortega Álvarez. Universidad de Castilla-La Mancha.*, nº 1, 2016.
- BASTIDA FREIJEDO, FRANCISCO J.; VILLAYERDE MENÉNDEZ, IGNACIO; REQUEJO RODRÍGUEZ, PALOMA; PRESNO LINERA, MIGUEL ÁNGEL; ALDÁEZ CORRAL, BENITO; FERNANDEZ SARASOLA, IGNACIO, *Teoría General de los derechos fundamentales en la Constitución Española de 1978*, Tecnos, Madrid, 2012,
- BASTIDA FREIJEDO, FRANCISCO JOSÉ, "El fundamento de los derechos fundamentales", *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja REDUR*, nº 3, 2005.
- BEHLING, THORSTEN; ABEL, RALF BERND, *Praxishandbuch Datenschutz im Unternehmen*, De Gruyter, Berlin, 2014.
- BEJAR MERINO, HELENA, *El ámbito íntimo. Privacidad, individualismo y modernidad*, Alianza Editorial, Madrid, 1990.
- BELTRÁN AGUIRRE, JUAN LUIS, "Tratamiento de datos de salud en la prestación de servicios sociales", *DS Derecho y Salud*, nº 1, 2009.

- "La protección de los datos personales relacionados con la salud", *Ponencia del Defensor del Pueblo de Navarra*. 2012.
- BELTRÁN PARDO, MARTA; SEVILLANA JAÉN, FERNANDO, *Cloudcomputing, tecnología y negocio*. Paraninfo, Madrid, 2013.
- BERROCAL LANZAROT, ANA ISABEL, "La protección de datos relativos a la salud y la historia clínica", *Revista de la Escuela de Medicina Legal*, nº 18, 2011, pág.11-44.
- BINDI, ELENA, "Test de proporcionalidad en el *age of balancing*", *UNED Revista de Derecho Político*, nº 96, 2016, pág.291-330.
- BLASI CASAGRAN, CRISTINA, *La protección de los Derechos Fundamentales en el Tratado de Lisboa*, Instituto Universitario de Estudios Europeos, Barcelona, 2010.
- BÖCKENFÖRDE, THOMAS, "Auf dem Weg zur elektronischen Privatsphäre", *JZ Juristen Zeitung*, nº 19, 2008, pág. 925-939.
- BODENSCHATZ, NADINE, *Der europäische Datenschutzstandard*, Peter Lang. Internationaler Verlag der Wissenschaften, Frankfurt am Main, 2010.
- BOIX PALOP, ANDRÉS , "¿Una red donde todos somos menores de edad?", *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías* , Universidad de Valencia, 2010.
- "Transparencia, participación y procedimiento de elaboración de disposiciones reglamentarias para un modelo de open government", *El paradigma del gobierno abierto: retos y oportunidades de la participación, transparencia y colaboración*, Universidad Complutense, 2015.
- "El equilibrio entre los derechos del artículo 18 de la Constitución, el "derecho al olvido" y las libertades informativas tras la Sentencia Google." *Revista General de Derecho Administrativo*, nº 38, 2015.
- "De McDonald's a Google. La ley ante la tercera revolución productiva", *Teoría y derecho: revista de pensamiento jurídico*, nº 1, 2007, pág.124-147.

- "La construcción de los límites a la libertad de expresión en las redes sociales", *Revista de Estudios Políticos.*, nº 173, 2016
- "Las leyes de convalidación en el ordenamiento constitucional", *Revista española de derecho constitucional*, nº 73, 2005, pág.157-186.
- "Libertad de expresión y pluralismo en la red", *Revista española de derecho constitucional*, nº 65, 2002, pág.133-182.
- BOIX PALOP, ANDRÉS ; LÓPEZ GARCÍA, GUILLERMO; "Derecho y cuarto poder en la era digital", *Revista de estudios políticos*, 2005.
- BOZA CHIRINO, JOSÉ , "La Responsabilidad Social de las Empresas y la Cultura de la Certificación", *Atlantic Review of Economics: Revista Atlántica de Economía*, nº 1, 2011.
- BRÖHMER, JÜRGEN, *Transparenz als Verfassungsprinzip*, Mohr Siebeck, Tübingen, 2004.
- BRUNO, GASTÓN, "Cloud computing en la industria financiera", *Ciencia y tecnología*, nº 13, 2013, pág.69-82.
- BULL, HANS PETER , *Informationelle Selbstbestimmung - Vision oder Illusion? : Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit* , Mohr Siebeck, Tübingen , 2011.
- BUSTAMANTE DONAS, JAVIER, "Ética en la nube: Dilemas éticos y políticos en el modelo de computación en la nube (*Cloud Computing*)", *Argumentos de razón técnica: Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología*, nº 16, 2013, pág.37-54.
- BUSTOS GISBERT, RAFAEL, "El concepto de libertad de información a partir de su distinción de la libertad de expresión. ", *Revista de Estudios Políticos*, 1994, pág.261-290.
- CÁMARA VILLAR, GREGORIO, "La garantía de los Derechos Fundamentales afectados por la Convención de Prüm", *Revista de Derecho Constitucional Europeo*, nº 7, 2007, pág.97-118.

- CANALES GIL, ÁLVARO, "Comentario al artículo 5 LOPD. Derecho de información en la recogida de datos.", *Comentario a la Ley Orgánica de Protección de Datos Personales*, Aranzadi, Madrid, 2010.
- CAÑÓN DE FRANCIA, JOAQUÍN , "Repercusión económica de la certificación medioambiental ISO 14001", *Cuadernos de gestión*, nº 1, 2006, pág.45-62.
- CARBAJO NÚÑEZ, MARTÍN , "La protección de la intimidad en los códigos deontológicos del periodismo europeo", *Antoniano*, nº 4, 2004, pág. 715-745.
- CARMONA SALGADO, CONCEPCIÓN, *Libertad de expresión e información y sus límites*, Editorial de Derecho Reunidas, S.A., Madrid, 1991.
- CARRILLO, MARC, *El derecho a no ser molestado*, Aranzadi, Madrid, 2014.
- "El uso de internet en la empresa", *Iuslabor*, nº 1, 2016.
- CARRILLO SALCEDO, JUAN ANTONIO, *Soberanía de los Estados y Derechos Humanos en Derecho internacional contemporáneo*, Tecnos, Madrid, 2001.
- CARRIZOSA PRIETO, ESTHER;, "Las facultades de vigilancia y control en el centro de trabajo y su incidencia sobre el derecho a la intimidad de los trabajadores", *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*, Tirant lo Blanch, Valencia, 2014.
- CASTELLANOS RUIZ, ESPERANZA , "Las normas de Derecho Internacional Privado sobre consumidores en la Ley 34/2002 de Servicios de la Sociedad de la información y de comercio electrónico.", *Cuadernos de derecho transnacional*, nº 2, 2009, pág.134-159.
- CASTILLO, LAURA, "Nuevo Reglamento General de Protección de Datos de la Unión Europea", *Red Seguridad. Revista especializada en seguridad informática, protección de datos y comunicaciones*, nº 73, 2016, pág.1-80.
- CHAMORRO MERA, ANTONIO; MIRANDA GONZÁLEZ, FRANCISCO JAVIER; RUBIO LACOB, SERGIO; "Clarificando el concepto de certificación. El caso español", *Boletín económico de ICE, Información Comercial Española*, nº 2825, 2004, pág.1001-1016.

CIANCIARDO, JUAN, *El conflictivismo en los Derechos Fundamentales*, Ediciones Universidad de Navarra, S.A. (EUNSA), Barañáin , 2000.

CORDERO CUTILLAS, ICIAR, "Redefiniendo los derechos de la personalidad en el siglo XXI", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, 2014.

COTINO HUESO, LORENZO, "Datos Personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público. Comentario al artículo 3.", *Comentario a la Ley de Protección de Datos de Carácter Personal*, Aranzadi, Madrid, 2010.

—"El Reglamento de la Iniciativa Ciudadana Europea de 2011", *Revista de derecho político*, nº 81, 2011, pág.323-378.

—"Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías.", Universidad de Valencia, Valencia, 2010.

—"Algunas cuestiones clave de protección de datos en la nube. Hacia una "regulación nebulosa"", *Revista catalana de dret públic*, nº 51, 2015, pág.86-103.

—"El conflicto entre las libertades de expresión e información en internet y el derecho a la protección de datos. El derecho al olvido y sus retos: "un falso derecho, a juzgar por un falso tribunal", *Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia*, Madrid, 2014.

COTINO HUESO, LORENZO; SAHUQUILLO OROZCO, JOSÉ LUIS; CORREDOIRA ALFONSO, LORETO; *El paradigma del Gobierno Abierto*, Universidad Complutense de Madrid, Madrid, 2015.

CRESPO FRANCO, TONY , "Las empresas españolas con certificación de calidad ISO 9000", *La gestión de la diversidad : XIII Congreso Nacional, IX Congreso Hispano-Francés, Logroño (La Rioja), 16, 17 y 18 de junio, 1999* , nº , 1999, pág.965-974.

CUENCA GÓMEZ, PATRICIA, "La incidencia del derecho internacional de los derechos humanos en el derecho interno: la interpretación del artículo 10.2 de la Constitución Española.", *Revista de Estudios Jurídicos. Versión electrónica.* , nº 12, 2012, pág.1-24.

- DARNACULLETA I GARDELLA, MERCÈ, *Derecho administrativo y autorregulación: la autorregulación regulada*, Universidad de Girona, Girona, 2002.
- DAVARA RODRÍGUEZ, MIGUEL ÁNGEL, "El concepto de fichero en la normativa sobre protección de datos. Comentario al artículo 3.", *Comentario a la Ley de Protección de Datos de Carácter Personal*, Aranzadi, 2010.
- "El Reglamento Europeo sobre protección de datos", *El Consultor de los Ayuntamientos*, nº 11, 2016.
- "Acerca de la seguridad en el tratamiento de la información y la protección de datos", *El Consultor de los Ayuntamientos*, nº 9, 2016.
- "Los drones y la privacidad", *El Consultor de los Ayuntamientos*, nº 15, 2015.
- "Firma electrónica y autoridades de certificación. El notario electrónico", *El acceso a los documentos municipales*, Archivos municipales y gestión de documentación. Madrid, 2002.
- "Validez y eficacia jurídica de los documentos generados por medios informáticos o telemáticos: la autenticación de intervinientes y contenidos." *Revista Calalana d'Arxivística*, nº 14, 1999, pág.13-34.
- "El humanismo tecnológico", *Datospersonales.org, Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº 1, 2003, pág.1-4.
- DE DOMINGO, TOMÁS, *¿Conflictos entre derechos fundamentales?*, Centro de Estudios políticos y constitucionales, Madrid, 2001.
- DE LA CUESTA RUTE, JOSÉ MARÍA , "La autorregulación como regulación jurídica", *Ponencia presentada al I Congreso Internacional Códigos de Conducta. Mercado, Publicidad y Mercados Financieros*, nº , 2008.
- DE LA SERNA BILBAO, MARÍA, "Fuentes Accesibles al público. Comentario al artículo 3. ", *Comentario a la Ley de Protección de Datos de Carácter personal*, Aranzadi, Madrid, 2010.

- DE LA TORRE OLID, FRANCISCO; CONDE COLMENAREJO, PILAR; "Consideraciones críticas en torno a la autogestión y preservación de la intimidad en un escenario de riesgo", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, 2014.
- DE MIGUEL MOLINA, MARÍA; OLTRA GUTIERREZ, JUAN VICENTE; "La autorregulación europea de las redes sociales: análisis de las políticas de uso de la imagen de menores en España", *Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías*, Universidad de Valencia, Valencia, 2010.
- DECKER, FRANK; HÖRETH, MARCUS, *Die Verfassung Europas. Perspektiven des Integrationsprojekt*. VS Verlag für Sozialwissenschaften, Wiesbaden, 2009.
- DEL CASTILLO VÁZQUEZ, ISABEL CECILIA, *Protección de datos: Cuestiones constitucionales y administrativas: el derecho a saber y la obligación de callar*, Civitas, Madrid, 2007.
- "Transparencia, acceso a la documentación Administrativa y protección de datos de carácter personal.", *Revista Foro Nueva Época. Servicio de publicaciones de la Universidad Complutense de Madrid*, nº , 2007, pág.231-254.
- "Artículo 2.2.b) Ficheros sometidos a la normativa sobre protección de materias clasificadas", *Comentario a la ley de protección de datos de carácter personal*, Aranzadi, Madrid, 2009.
- DEL PESO NAVARRO, EMILIO, *Ley de Protección de Datos, la nueva ley LORTAD*, Díaz de Santos, Madrid, 2000.
- DI MARTINO, ALESSANDRA, "Datenschutz im Europäischen Recht", *Walter Hallstein-Institut für Europäisches Verfassungsrecht*, 2004.
- DÍAZ, VANESSA, "Derecho a la información en el sector salud y protección de datos personales", *Derecho comparado de la información*, nº 12, 2008, pág.111-132.
- DÍAZ BUCK, ANID VANESSA , "La autorregulación en redes sociales como forma de garantizar los derechos de intimidad, privacidad y protección de datos personales", *Derecom*, nº 13, 2013.

- DÍAZ REVORIO, FRANCISCO JAVIER;, "Comentario al artículo 5 LOPD. Derecho de la Información en la recogida de datos. Una perspectiva constitucional", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Madrid, 2010.
- DÍEZ PICAZO, LUIS, *Constitucionalismo de la Unión Europea*, Civitas, Madrid, 2002.
- Sistema de Derechos Fundamentales*, Aranzadi, Madrid, 2003.
- DIX, ALEXANDER, "Datenschutz und transatlantische Freihandelszone ", *Karlsruher Dialog zum Informationsrecht / Zentrum für Angewandte Rechtswissenschaft (ZAR), Karlsruher Institut für Technologie (KIT)*, 2016.
- DOMINGO DE, TOMÁS, *¿Conflictos entre Derechos Fundamentales?*, Centro de Estudios Constitucionales, Madrid, 2001.
- DOMÍNGUEZ MEJÍAS, IGNACIO, "Hacia la memoria selectiva en Internet. Honor, intimidad y propia imagen en la era digital a partir de la jurisprudencia española.", *Revista Iberoamericana de Ciencia, Tecnología y Sociedad - CTS*, nº 11, 2016.
- DORSCHER, JOACHIM, *Praxishandbuch Big Data. Wirtschaft - Recht - Technik.*, Springer Fachmedien, Wiesbaden, 2015.
- ERCOLANI, GIUSEPPE, "Análisis del potencial del Cloud Computing para las PYMES", *Cuadernos de Gestión de información*, nº 2, 2012.
- ERMIDA URIARTE, ÓSCAR; GIANIBELLI, GUILLERMO; ÁLVARO ORSATTI; *Responsabilidad social empresarial: perspectivas jurídicas para estrategias sindicales*, Friedrich-Ebert-Stiftung, Pluna-Uruguay, 2010.
- ESCALERA ALMENDROS, CARLOS ; PASCUAL FAURA, MARCELO; "La normalización y certificación como ventaja competitiva para la empresa española", *Boletín económico de ICE, Información Comercial Española*, nº 2820, 2004, pág.1001-1012.
- ESCANCIANO GARCÍA-MIRANDA, CARMEN , "Certificación ISO 9000 en España. Dificultades versus satisfacción empresarial", *Dirección y organización: Revista de dirección, organización y administración de empresas*, nº 27, 2002, pág.148-156.

FARRIOLS i SOLÀ, ANTONI, *La protección de datos de carácter personal en los centros de trabajo*, Cinca, Madrid, 2006.

FAYOS GARDÓ, ANTONIO, *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, Madrid, 2014.

—"Los derechos a la intimidad y a la propia imagen: Un análisis de la jurisprudencia española, británica y del Tribunal Europeo de Derechos Humanos. 25º Aniversario de la LO 1/1982", *Indret. Revista para el Análisis del Derecho*, nº 4, 2007.

FERNÁNDEZ BARRERO, MARÍA ÁNGELES; GUIRADO BORREGO, VÍCTOR; *Comunicación y desarrollo en la era digital. Congreso AE-IC 3, 4 y 5 de febrero de 2010*, Madrid, 2010.

FERNANDEZ LÓPEZ, JUAN MANUEL, "Comentario al artículo 6. Principio de Consentimiento", *Comentario a la Ley Organica de Protección de Datos de Carácter Personal.*, Aranzadi, Madrid, 2010.

FERNÁNDEZ SÁNCHEZ, ESTEBAN; VÁZQUEZ ORDÁS, CAMILO JOSÉ; ESCANCIANO GARCÍA-MIRANDA, CARMEN; "Influencia de la certificación ISO 9000 en el avance de la empresa española hacia la calidad total", *Cuadernos de economía y dirección de la empresa*, nº 14, 2003, pág.99-114.

FRAILE ORTIZ, MARÍA, "La protección constitucional de la intimidad frente a los medios de comunicación.", *Teoría y realidad constitucional*, nº 18, 2006, pág.557-562.

FRANZIUS, CLAUDIO, "Das Recht auf informationelle Selbstbestimmung", *Zeitschrift für das Juristische Studium*, nº 61, 2015.

GALÁN MÚÑOZ, ALONSO; ARRIBAS LEÓN, MÓNICA; CARRIZOSA PRIETO, ESTHER; CARUSO FONTÁN, VVIANA; HOLGADO GONZÁLEZ, MARÍA; LUCENA CID, ISABEL; TOSCANO GIL, FRANCISCO, *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y la comunicación*, Tirant Lo Blanch, Valencia, 2014.

GARCÍA DEL POYO, RAFAEL, "Cloud Computing. Aspectos jurídicos clave para la contratación de estos servicios", *Revista Española de Relaciones Internacionales*, nº 4, 2012, pág.48-91.

GARCÍA FIGUEROA, ALFONSO, *Principios y positivismo jurídico : el no positivismo principalista en las teorías de Ronald Dworkin y Robert Alexy*, Centro de Estudios políticos y constitucionales, Madrid, 1998.

GARCÍA MONTORO, LOURDES , "El sueño de la resolución online de conflictos de consumo, cerca de convertirse en una realidad", *Publicaciones jurídicas. Universidad de Castilla-La Mancha. CESCO. Centro de estudios de consumo*, nº 1, 2016.

GARCÍA SAN JOSÉ, DANIEL I., *Los derechos y libertades fundamentales en la sociedad europea del siglo XXI*, Secretariado de Publicaciones. Universidad de Sevilla, 2001.

GARCÍA SAN MIGUEL, LUIS, *Estudios sobre el derecho a la intimidad*, Tecnos, Madrid, 1992.

GARRIGA DOMINGUEZ, ANA, *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2004 y segunda versión de 2009.

—*La protección de datos personales en el Derecho español*, Dykinson, Madrid, 1999.

—*Nuevos retos para la protección de datos personales*, Dykinson, Madrid, 2015.

—"La protección de los datos personales en internet: problemas actuales", *Derechos Humanos y protección de datos personales*, Punto Rojo Libros, 2013.

—"Una nueva exigencia de la libertad: La protección de los datos personales "sensibles" Revista jurídica de la Universidad de Santiago de Compostela, nº 2, 2000, pág. 39-48.

—*Fundamentos éticos y jurídicos de las TIC's*, Aranzadi, Navarra, 2012.

GARRIGA DOMINGUEZ, ANA; ÁLVAREZ GONZÁLEZ, SUSANA, "Historia clínica y protección de datos personales: recomendaciones y propuestas en torno al uso de la información.", *El Tiempo de los Derechos*, noviembre, 2010.

GAVARA DE CARA, JUAN CARLOS, *La autorregulación de los medios de comunicación como sistema de control*, Bosch, Madrid, 2013.

—*Las autoridades independientes de control de los medios de comunicación audiovisual*, Bosch, Barcelona, 2013.

- GAVARA DE CARA, JUAN CARLOS; DE MIGUEL BÁRCENA, JOSU, *La autorregulación como mecanismo de autocontrol de los medios de comunicación: intervención pública y regulación interna*, Bosch, Madrid, 2013.
- GEORG F., SCHRÖDER, *Datenschutzrecht für die Praxis*, dtv Beck Rechtsberater, München, 2016.
- GIL GONZÁLEZ, ELENA, *Big Data, privacidad y protección de datos*, AEPD Agencia Española de Protección de datos, Madrid, 2016.
- GOLA, PETER; JASPER, ANDREAS, *Das Bundesdatenschutzgesetz im Überblick*, Datakontext, Heidelberg, 2011.
- GÓMEZ DE LIAÑO, IGANACIO, *La mentira social. Imágenes, mitos y conducta*, Tecnos, Madrid, 1989.
- GÓMEZ PIQUERAS, CRISTINA, "Disociación/anonimización de los datos de salud", *DS Derecho y Salud*, nº 1, pág.43-56.
- GÓMEZ SÁNCHEZ, YOLANDA, "La protección de datos genéticos. El derecho a la autodeterminación informativa.", *Revista Derecho y Salud*, 2008.
- GÓMEZ-REINO Y CARNOTA, ENRIQUE, "La Carta de los Derechos Fundamentales de la Unión Europea", *Dereito: Revista xuridica da Universidade de Santiago de Compostela*, nº 1, 2013.
- GONZÁLEZ ÁLVAREZ, MARTA; FERNÁNDEZ FERNÁNDEZ, JOSÉ LUIS, "Discapacidad, empresa y legitimidad", *XXIII Congreso EBEN España*, nº 1, 2015.
- GONZÁLEZ BEILFUSS, MARKUS, *El Principio de Proporcionalidad en la Jurisprudencia del Tribunal Constitucional*, Aranzadi, Cizur Menor, 2003.
- GONZÁLEZ CIFUENTES, CAROLINA, *El derecho a la intimidad de los altos cargos*, Universidad de Salamanca, Salamanca, 2011.
- GONZÁLEZ FUSTER, GLORIA, "Comentarios a la Sentencia del Tribunal Europeo de Derechos Humanos 30562/04 Y 30566/04, vida privada y los límites al tratamiento de

datos biométricos de personas no condenadas.", *Revista de Derecho Comunitario Europeo*, nº 33, , pág.619-633.

GONZÁLEZ GRANDA, PIEDAD , "Protección judicial de consumidores y usuarios en el ámbito del comercio electrónico", *Indret: Revista para el Análisis del Derecho*, nº 4, 2007.

GONZÁLEZ MORENO, BEATRIZ;, "Comentario del artículo 7 LOPD. La Ley Orgánica de protección de datos y los Libros de Bautismo.", *Comentario a la Ley Orgánica de Protección de Datos Personales*, Aranzadi, Madrid, 2009.

GONZÁLEZ -TABLAS SASTRE, RAFAEL, "El Derecho y las Nuevas Tecnologías", nº 6-7, 2000-2001.

—"La revolución social de las redes sociales en internet", *Nuevas tecnologías y Derechos Humanos*, Tirant lo Blanch, Valencia, 2014.

GUASCH PORTAS, VICENTE, "Cloud Computing, turismo y protección de datos", *Revista de análisis turístico*, nº 17, 2014, pág.61-68.

GUERRERO PICÓ, MARÍA DEL CARMEN, *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal*, Thomson Civitas, Navarra, 2006.

HÄBERLE, PETER, *La Garantía del contenido esencial de los Derechos Fundamentales*, Dykinson, Madrid, 2003.

HABERMAS, JÜRGEN, *Factividad y validez*, Trotta, Madrid, 1998.

HEREDERO HIGUERAS, MANUEL, *La Directiva comunitaria de Protección de los Datos de Carácter Personal*, Aranzadi, Madrid, 1997.

—"Informática y Libertad: la respuesta de los juristas a un problema de nuestro tiempo"

<http://revistasonline.inap.es/index.php?journal=DA&page=article&op=view&path%5B%5D=4175&path%5B%5D=4229>

,

—"La sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población de 1983"

<http://revistasonline.inap.es/index.php?journal=DA&page=article&op=view&path%5B%5D=4687&path%5B%5D=4741>

—"La protección de datos de salud informatizados en la Ley Orgánica 5/1992 de 29 de octubre", *DS Derecho y Salud*, nº 1, 1994, pág.17-30.

HERNÁNDEZ LÓPEZ, JOSÉ MIGUEL, *El Derecho a la Protección de Datos Personales en la Doctrina del Tribunal Constitucional*, Aranzadi, Cizur Menor, 2013.

HERRÁN ORTIZ, ANA ISABEL, *El derecho a la protección de datos personales en la sociedad de la información*, Universidad de Deusto. Cuadernos Deusto de Derechos Humanos, Bilbao, 2003.

—*El derecho a la intimidad en la nueva ley orgánica de protección de datos personales.*, Dykinson, Madrid, 2002.

—"Nuevos tiempos para la protección de datos persojnales y su repercusión en los despachos de abogados. Breves notas al esperado Reglamento Europeo de Protección de datos. ", *Revista de Derecho, Empresa y Sociedad (REDS)*, nº 4, 2014.

HOBBS, THOMAS, *Leviatan*, Losada, Madrid, 2003.

HOCHREITER, MONIKA, *Die heimliche Überwachung internationale Telekommunikation*, Herbert UTZ Verlag GmbH , München, 2001.

HOLGADO GONZÁLEZ, MARÍA, "La protección constitucional de la intimidad de los trabajadores frente al uso de las nuevas tecnologías de la comunicación", *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*, Tirant lo Blanch, Valencia, 2014.

JIMENA QUESADA, LUIS , "La técnica legislativa y otros aspectos constitucionales relativos a la Ley de servicios de la sociedad de la información y de comercio electrónico", *Revista de Derecho*, nº 2, 2002.

JIMÉNEZ DE PARGA, MANUEL, *El Derecho Constitucional a la protección de la salud*, Comunidad de Madrid, 2004.

KÖHLER, PETER , *Ein einheitliches Datenschutzkonzept in der EU?: Die neue EU-Datenschutzverordnung* , GRIN Verlag GmbH , München, 2016.

KRANIG, THOMAS; EIFERT, MARTIN;"Selbstregulierung und wettbewerbsrechtliche Elemente im Datenschutz der Zukunft"

https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Datenschutz/ergebnisse_panel_3_de.pdf?__blob=publicationFile,

LEÓN BASTOS, CAROLINA, *La interpretación de los derechos fundamentales según los tratados internacionales sobre derechos humanos*, Editorial Reus, Madrid, 2010.

LINARES GUTIERREZ, ANTONIO, "El chantaje de los ficheros de morosos", *Dereito: Revista xuridica da Universidade de Santiago de Compostela*, nº 1, 2014, pág.113-126.

LINDER, ANDREAS, *EU-Datenschutz-Grundverordnung*, BoD GmbH, Norderstedt, 2016.

LOCKE, JOHN, *Segundo ensayo sobre el gobierno civil*, Losada, Madrid, 2003.

LÓPEZ AGUILAR, JUAN FERNANDO, "*Data protection package* y parlamento europeo", *Hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015.

LÓPEZ DEL MORAL ECHEVARRÍA, JOSÉ LUIS;, "Comentario al artículo 13 LOPD; Impugnación de valoraciones", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Madrid, 2010.

LÓPEZ JIMÉNEZ, DAVID, "La solución idónea frente a la elevada desprotección de la privacidad en Internet", *Revista Telos (Cuadernos de Comunicación e innovación)*, nº 1, 2014.

—"La protección de datos de carácter personal en el ámbito de las redes sociales electrónicas. El valor de la autoregulación", *Anuario de la Facultad de Derecho*, nº 2, 2009, pág.237-278.

—"Los códigos tipo como instrumento para la protección de la privacidad en el ámbito digital", *Estudios constitucionales: Revista del Centro de Estudios Constitucionales*, nº 2, 2013, pág. 575-614.

—"La autorregulación de las TIC por parte de las empresas de economía social: D'Confianza como modelo de referencia.", *Revista Internacional del Mundo Económico y del Derecho*, nº VII, 2014, pág. 1-28.

LÓPEZ PINA, ANTONIO;, "La utonomía privada y los derechos fundamentales. Los intereses generales, mandato constitucional", *Teoría y realidad consitucional*, nº 20, 2007, pág.145-173.

LÓPEZ RICHART, JULIÁN , "Difamación en la web 2.0 y responsabilidad civil de los prestadores de servicios de alojamiento", *Derecho privado y Constitución*, nº 26, 2012, pág.143-201.

LÓPEZ-MUÑIZ GOÑI, MIGUEL, "La ley de regulación del tratamiento automatizado de los datos de carácter personal", nº 6-7, 1994.

—*Informática Jurídica Documental*, Díaz de Santos, Madrid, 1984.

LORENZO RODRÍGUEZ-ARMAS, MAGDALENA, *Análisis del contenido esencial de los Derechos Fundamentales enunciados en el art. 53.1 de la Constitución Española*, Editorial Comares, Granada, 1996.

LOSANO, MARIO G., *Curso de Informática Jurídica*, Tecnos, Madrid, 1987.

LUCENA CID, ISABEL VÍCTORIA;, "El concepto de la intimidad en los nuevos contextos tecnológicos", *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*, Tirant lo Blanch, Valencia, 2014.

LLÁCER MATACÁS, M., "La autodeterminación informativa en la sociedad de la vigilancia: *ubiquitous computing*", *Protección de datos personales en la sociedad de la información y la vigilancia*, Madrid, 2011, pág. 61 y ss.

LLANEZA, PALOMA, "Aspectos legales: *periodismo, ciudadanos y la ley*", *Periodismo ciudadano*. Evolución positiva de la comunicación, Fundación Telefónica, Ariel. 2011.

MAGDALENO ALEGRÍA, ANTONIO, *Los límites de las libertades de expresión e información en el Estado social y democrático de Derecho*, Congreso de los Diputados, Madrid, 2006.

- "Libertad de expresión y partidos políticos en la jurisprudencia del Tribunal Europeo de los Derechos Humanos.", *Anuario de la Facultad de Derecho de la Universidad de La Coruña*, nº 11, 2007, pág.431-450.
- "Libertad de expresión, terrorismo y límites de los Derechos Fundamentales.", *Revista de Derecho Político*, nº 69, 2008, pág.181-222.
- MAIER, NATALIE , *Die Datenweitergabe im Rahmen des Cloud Computings unter besonderer Betrachtung von Unterauftragsverhältnissen*, Kassel Univ. Press, Kassel, 2014.
- MAQUIAVELO, NICOLÁS, *Discursos sobre la primera época de Tito Livio*, Losada, Madrid, 2005.
- MARTÍN RETORTILLO BAQUER, LORENZO, "Comentario al artículo 35 LGT", *Comentarios a la Ley General de Comunicaciones; Ley 32/2003 de 3 de noviembre*, Thomson-Civitas, Madrid, 2004.
- MARTÍNEZ MARTÍNEZ, RICARD, *Tecnologías de la Información, Policía y Constitución*, Tirant lo Blanch, Barcelona, 2001.
- "Una aproximación crítica a la autodeterminación informativa, Civitas, Madrid, 2004.
- "El Derecho Fundamental a la Protección de Datos: Perspectivas", nº 5, 2007.
- "El Reglamento de protección de datos de la Unión Europea: un reto colectivo", *Revista SIC: Ciberseguridad, seguridad de la información y privacidad*, 2016, pág.90-92.
- "El rol de los profesionales de la privacidad", *Hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015.
- MARTÍNEZ MARTÍNEZ, SILVIA, "El derecho a la intimidad en el periodismo participativo: consideraciones desde el ámbito de la ética y la regulación deontológica de la información", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, Madrid, 2014.

- MARTÍNEZ OTERO, JUAN MARÍA, "El derecho al olvido en Internet", *Revista de Derecho Político*, nº 93, 2015, pág.103-142.
- MEDINA GUERRERO, MANUEL, *La protección constitucional de la intimidad frente a los medios de comunicación*, Tirant lo Blanch, Valencia, 2005.
- La vinculación negativa del legislador a los derechos fundamentales*, McGraw-Hill, Madrid, 1996.
- "Escritos sobre Derechos Fundamentales", *Revista Española de Derecho Constitucional*, nº 41, 1994.
- MEGÍAS QUIRÓS, JOSÉ JUSTO;, "Comentario al artículo 2.2.a) LOPD", *Comentario a la Ley Orgánica de Protección de datos de carácter personal*, Thomson-Civitas, Madrid, 2009.
- MEGÍAS TEROL, JAVIER, "Privacy by design, construcción de redes sociales garantes de la privacidad", *Derecho y redes sociales*, Civitas, Madrid, 2010.
- MESSÍA DE LA CERDA BALLESTEROS, FRANCISCO JOSÉ, "El consentimiento y el derecho a la protección de datos de carácter personal", *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas. Los derechos fundamentales y las nuevas tecnologías*, nº 1, 2005.
- MIERES MIERES, LUIS JAVIER, "El derecho al olvido digital", *Fundación Alternativas*, 2014.
- MINERO ALEJANDRE, GEMMA, "A vueltas con el "derecho al olvido". Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital.", *Revista jurídica Universidad Autónoma de Madrid*, 2014, pág.129-155.
- MINISTERIO DE JUSTICIA, , *Resoluciones del Comité de Ministros del Consejo de Europa*, Ministerio de Justicia, Madrid, 2014.
- MINISTERIO DEL INTERIOR. COMISIÓN TÉCNICA DE APOYO A LA IMPLANTACIÓN DEL DNI ELECTRÓNICO, "DNI electrónico. Guía de referencia Básica.", *Grupo de trabajo de divulgación y comunicación. Policía Nacional*, nº 1, 2016.

MIRALLES LÓPEZ, RAMÓN, *Capacidad efectiva del ejercicio y tutela de los derechos LOPD en las redes sociales*, Servicio de publicaciones de la Universidad de Valencia, Madrid, 2011.

—"Seguridad de la información y protección de datos personales. ", *Comentario a la Ley de Protección de Datos Personales*, 2010.

MIRANDA GONZÁLEZ, FRANCISCO JAVIER; RUBIO LACOBIA, SERGIO; CHAMORRO MERA, ANTONIO;, *Introducción a la gestión de la calidad*, Delta, Madrid, 2007.

MONTESQUIEU, CHARLES LOUIS DE SECONDAT, BARÓN DE, *Del espíritu de las Leyes*, Alianza Editorial, Madrid, 2012.

MORENO MUÑOZ, MIGUEL, "La tensión entre privacidad y seguridad en el desarrollo de internet", *Dilemata*, nº 15, 2014, pág.181-193.

MORETÓN TOQUERO, MARÍA ARÁNZAZU, "El secreto profesional del periodista y la empresa de comunicación: ¿Un conflicto de lealtades?", *Revista Jurídica de Castilla y León*, nº 4, 2004.

MURILLO DE LA CUEVA, PABLO LUCAS, *Derecho a la Autodeterminación informativa*, Autor-Editor, Madrid, 2009.

—"La construcción del derecho a la Autodeterminación informativa", *Revista de Estudios Políticos*, nº 104, 1999, pág.35-60.

—"Perspectivas del derecho a la autodeterminación informativa", *Revista de Internet. Derecho y Política*, nº 5, 2007, pág.18-33.

—"La protección de los datos de carácter personal en el horizonte del 2010", *Anuario de la Facultad de Derecho*, nº 2, 2009, pág.131-142.

—"La Constitución y el derecho a la autodeterminación informativa", *Cuadernos de Derecho Público*, nº 19-20, 2003, pág.27-44.

—"El derecho fundamental a la protección de los datos relativos a la salud.", *Agencia Catalana de Protección de Datos. Servicio de publicaciones*, nº 1, 2005.

—"El Objeto de la Ley Orgánica de Protección de Datos de Carácter Personal", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Madrid, 2010.

MÜTHLEIN, THOMAS, *Datenschutz-Grundverordnung DS-GVO (General Data Protection Regulation)*, Datakontext, Frechen, 2016.

NIETO MARÍN, ADÁN; MAROTO CALATAYUD, MANUEL; "Redes Sociales en internet y data mining en la prospección de comportamientos delictivos", *Derecho y redes sociales*, Civitas, Madrid, 2010.

NORTON, PETER, *Introducción a la Computación*, McGraw-Hill Interamericana Editores, S.A., México, 2006.

NUÑEZ MARTINEZ, MARÍA ACRACIA; "El Tribunal Constitucional y las Libertades del artículo 20 de la Constitución Española."

[http://revistas.uned.es/index.php/RDUNED/article/viewFile/10954/10482,](http://revistas.uned.es/index.php/RDUNED/article/viewFile/10954/10482)

O'CALLAGHAN MUÑOZ, XAVIER, *Libertad de expresión y sus límites. Honor, intimidad e imagen*, Editorial de derecho Reunidas, S.A., Madrid, 1991.

OLIVER-LALANA, A. DANIEL, "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Madrid, 2013.

ORTEGA GIMÉNEZ, ALFONSO, *La (des) protección del titular del derecho a la protección de datos derivada de una transferencia ilícita*, Agencia Española de Protección de Datos, Madrid, 2014.

—*Transferencias internacionales de Datos de Carácter personal Ilícitas*, Aranzadi, Pamplona, 2016.

ORTEGA Y GASSET, JOSÉ, *El Espectador*, Edaf, Madrid, 2007,

—*La Rebelión de las masas*, Espasa, Madrid, 2009.

ORTÍ VALLEJO, ANTONIO, *Derecho a la intimidad e informática*, Comares, Madrid, 1994.

—"El nuevo derecho fundamental (y de la personalidad) a la libertad informática. A propósito de la STC 254/1993, de 20 de julio." *Derecho Privado y Constitución*, nº 2, 1994, pág.305-332.

ÓRTIZ LÓPEZ, PAULA, "Redes sociales: funcionamiento y tratamiento de información personal", *Derecho y redes sociales*, Civitas, 2010.

OTADUY, JORGE;, "Iglesia Católica y Ley Española de Protección de Datos: Falsos conflictos."

file:///D:/Downloads/95-08.OtaduyEst.pdf,

—"La Iglesia Católica ante la Ley Española de Protección de Datos",

file:///D:/Downloads/ICn90(529-555).pdf,

PALOMAR OLMEDA, ALBERTO, "Confidencialidad y protección de datos en la Ley de Salud Sexual", *DS Derecho y Salud*, nº 2, 2010.

PARDO FALCÓN, JAVIER, "Los Derechos del artículo 18 de la Constitución Española en la jurisprudencia del Tribunal Constitucional", nº 34, 1992, pág.141-180.

PATRICIA ROJAS, ÁNGELA, "La responsabilidad de las PSSI y la libertad de expresión.", *Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías*, Servicio de publicaciones de la Universidad de Valencia, 2010.

PAUNER CHULVI, CRISTINA, "La actividad periodística en los ordenamientos nacionales y europeos sobre protección de datos", *Hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015.

—"Implicaciones del futuro Reglamento europeo sobre protección de datos en la libertad de información", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, , Madrid, 2014.

PECES-BARBA, GREGORIO, "Critica a Prieto Sanchis en su obra "Principios y normas". Problemas de razonamientos jurídicos." Madrid, 1992.

PEDRAZ PENALVA, E., *Protección de datos y proceso penal*, Madrid, 2010.

PELAYO OLMEDO, JOSÉ DANIEL, "La adscripción religiosa como dato especialmente protegido. El caso del registro butismal en España."

<http://revistas.uned.es/index.php/derechopolitico/article/view/15740/13691>,

PERALTA ORTEGA, JUAN CARLOS, "El derecho de autodeterminación informativa como derecho de la personalidad o derecho fundamental" *Cuadernos de estudios empresariales*, Universidad Complutense, Madrid, 1995.

PERELLÓ DOMÉNECH, ISABEL, "El principio de proporcionalidad y la jurisprudencia constitucional", *Jueces para la democracia*, nº 28, 1997.

—"Notas sobre el concepto de razonabilidad y su uso en la jurisprudencia constitucional", *Jueces para la democracia*, nº 46, 2003.

PÉREZ LUÑO, ANTONIO, *Los Derechos Fundamentales*, Tecnos, Madrid, 2004.

—"Internet y los Derechos Humanos", *Anuario de Derechos Humanos Nueva Época*, Universidad Complutense de Madrid, nº 12, 2011.

—*Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 2010.

—"Sobre el arte legislativo del birlibirloque. La LOPRODA y la tutela de la libertad informática en España", *Anuario de Filosofía del Derecho*, nº 18, 2001, págs. 321-326.

—"La tutela de la libertad informática en la sociedad globalizada", *Isegoría: Revista de filosofía moral y política*, nº 22, 2000, págs. 59-68.

—"Del Habeas Corpus al Habeas Data", *Informática y Derecho*, 1992.

—*Nuevas Tecnologías y Derechos Humanos*, Tirant lo Blanch, Valencia, 2014.

—"La protección de los datos personales de carácter sanitario", *Derechos Humanos y protección de datos personales en el siglo XXI*, Punto Rojo Libros, Madrid, 2013.

—"Ciudadanía y definiciones", *DOXA Cuadernos de filosofía del derecho*, 2002, págs. 177-211.

—"Comentario al Artículo 6 LOPD. El consentimiento de los menores." *Comentario a la Ley Orgánica de Protección de Datos*, Aranzadi, Madrid, 2010.

- "Impactos sociales y jurídicos de Internet", *Revista Española de ciencia, tecnología y sociedad, y filosofía de la tecnología*, nº 1, 1998, pág. 33-48.
- "La peculiaridad normativa de los principios generales del Derecho", *Persona y Derecho. Revista de la fundamentación de las instituciones y de Derechos Humanos*, nº 42, 2000, pág. 131-160.
- "La Seguridad Jurídica: Una garantía del Derecho y la Justicia", *BFD Boletín de la Facultad de Derecho de la UNED*, nº 15, 2000, pág. 25-38.
- "Las nuevas tecnologías y la garantía procesal de las libertades", *RDUNED Revista de Derecho UNED*, 2012, pág. 1007-1020.
- "Principios Generales del Derecho. ¿Un mito Jurídico?", *Revista de estudios políticos*, nº 98, 1997, pág. 9-24.
- PÉREZ-LUÑO ROBLEDO, ENRIQUE, "Las nuevas tecnologías y la garantía procesal de las Libertades", *Revista de Derecho UNED*, nº 11, 2012.
- PÉREZ MARTÍNEZ, JORGE; FRÍAS BARROSO, ZORAIDA, *Las reglas del juego en el ecosistema digital. Level Playing Field*, Fundación Telefónica, Madrid, 2016.
- "El derecho a la privacidad. Debate a ambos lados del Atlántico.", *Telos. Cuadernos de comunicación e innovación*, 2014, pág. 44-47.
- PIÑAR MAÑAS, JOSÉ LUIS, *Transparencia, acceso a la información y protección de datos*, Reus, Madrid, 2014.
- "Códigos de conducta y espacio digital. Especial referencia a la protección de datos", *Códigos de conducta y actividad económica: una perspectiva jurídica*, Marcial Pons Ediciones Jurídicas y Sociales, Madrid, 2012.
- "Concepto de dato personal. Comentario al Artículo 3.", *Comentario a la Ley de Protección de Datos de Carácter Personal*, Aranzadi, Madrid, 2010.
- PRIETO SANCHIS, LUIS, *Apuntes de Teoría del Derecho*, Trotta, Madrid, 2014.
- "Neoconstitucionalismo y ponderación judicial", *Anuario de la Facultad de Derecho de la Universidad Autónoma de Madrid*, nº 5, 2001.

- El constitucionalismo de los derechos: ensayos de filosofía jurídica*, Trotta, Madrid, 2013.
 - Justicia constitucional y derechos fundamentales*, Trotta, Madrid, 2003.
 - "Identificación y justificación del Derecho", Universidad de Castilla - LaMancha, nº 25, 2008-2009.
 - "Principia iuris", una teoría del derecho no (neo)constitucionalista para el estado constitucional", *DOXA, Repertorio Constitucional de la Universidad de Alicante*, nº 31, pág. 325-356, Alicante, 2008.
 - "Iusnaturalismo, positivismo y control de ley. Los presupuestos históricos, ideológicos y doctrinales de jurisdicción constitucional", *Fundamentos, cuadernos monográficos de Teoría del Estado público e Historia Constitucional*, nº 4, 2006, pág. 27-101
 - "Observaciones sobre las antinomias y el criterio de ponderación", Cuadernos sobre Derecho Público, nº 11, 2000, pág. 9-30.
 - "Tribunal Constitucional y positivismo jurídico", *Doxa: Cuadernos de filosofía del derecho*, nº 23, 2000, pág. 161-196.
 - "El constitucionalismo de principios, ¿entre el positivismo y el iusnaturalismo? (A propósito de "El Derecho dúctil" de Gustavo Zagrebelsky)", *Anuario de Filosofía del Derecho*, nº 13-14, 1996-1997, pág. 125-158.
 - "Diez argumentos sobre los principios", *Jueces para la Democracia*, nº 26, 1996, pág. 41-49.
 - "Sobre la separación entre Derecho y Moral y otras cuestiones relativas a los principios", *Anuario de Filosofía del Derecho*, nº 10, 1993, pág. 545-554.
- PUYOL MONTERO, JAVIER, "Comentario al artículo 19 LOPD. Derecho de indemnización", *Comentario a la Ley Orgánica de Protección de datos Personales*, Aranzadi, Madrid, 2010.

RAAB, JOHANNES, *Die Harmonisierung des einfachgesetzlichen Datenschutzes: von der umsetzungsdefizitären Datenschutzrichtlinie 95/46/EG zur Datenschutz-Grundverordnung*, LIT, Berlin und Münster, 2015.

RALLO LOMBARTE, ARTEMI, *El derecho al olvido en internet. Google versus España*, Centro de Estudios Constitucionales, Madrid, 2014.

—"El derecho al olvido y su protección a partir de la protección de datos", *Telos. Cuadernos de comunicación e innovación. Fundación Telefónica.*, nº 85, 2010, pág.104-108.

RALLO LOMBARTE, ARTEMI; GARCÍA MAHAMUT, ROSARIO; *Hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015.

RALLO LOMBARTE, ARTEMI; MARTÍNEZ MARTÍNEZ, RICARD, *Derecho y Redes Sociales*, Civitas Aranzadi, Navarra, 2010.

RALUCA STROIE, IULIANA , "Alternativas a la resolución de conflictos en materia de consumo: la Directiva 2013/11/UE del parlamento europeo y del consejo y el reglamento (UE) 524/2013 del Parlamento europeo y del Consejo, de 21 de mayo de 2013", *Publicaciones jurídicas. Universidad de Castilla-La Mancha. CESCO. Centro de Estudios de consumo.*, nº 1, 2013.

RAMOS FERNÁNDEZ, FERNANDO , "Autorregulación, mediación y consulta previa, la nueva frontera de la ética publicitaria", *Zer: Revista de estudios de comunicación, Komunikazio ikasketen aldizkaria*, nº 11, 2001.

REAL ACADEMIA ESPAÑOLA, *Diccionario de la Real Academia Española*, España, 2012.

REBOLLO DELGADO, LUCRECIO, *Vida privada y protección de datos en la Unión Europea*, DYKINSON, Madrid, 2008.

—*El Derecho Fundamental a la Intimidad*, Dykinson, Madrid, 2000; 2ª Edición 2005.

—*Derechos Fundamentales y Protección de Datos*, Dykinson, Madrid, 2004.

REBOLLO DELGADO, LUCRECIO; SERRANO PÉREZ, Mª MERCEDES; *Introducción a la protección de datos*, Dykinson, Madrid, 2008.

REVUELTA PÉREZ, INMACULADA, "Incidencia de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico en el servicio universal de telecomunicaciones. La inclusión del acceso a internet", *Revista de Derecho*, nº 2, 2003.

RIASCOS GÓMEZ, LIBARDO ORLANDO, *El Derecho a la intimidad, la visión iusinformática y el delito de los datos personales*, Universidad de Lleida, 2007.

RIBAGORDA GARNACHO, ARTURO, "La protección de datos personales y la seguridad de la información. ", *Revista Jurídica de Castilla y León.* , nº 16, 2008, pág.373-400.

RÍOS MARTÍN, JULIÁN CARLOS, "Los ficheros de internos de especial seguimiento"

<http://www.derechopenitenciario.com/comun/fichero.asp?id=995>,

RODOTÁ, STEFANO, "Las lecciones de wikileaks: nueva transparencia y nueva distribución del poder", *Transparencia, acceso a la información y protección de datos*, Barcelona, 2015.

—"Democracia y protección de datos."

https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/DemocraciaMadrid_mayo_05.pdf,

RODRÍGUEZ, JOSÉ, "La autodeterminación informativa como barrera a la libertad de información y al ejercicio profesional del periodismo", *Anàlis. Quaderns de comunicació i cultura*, nº 42, 2011, pág.79-94.

RODRÍGUEZ GÓMEZ, EDUARDO FCO., "El Tribunal Constitucional y el conflicto entre la libertad de información y los derechos al honor, la intimidad y la propia imagen.", *Estudios sobre el mensaje periodístico*, nº 20, 2014, pág.1209-1224.

ROMEO CASABONA, CARLOS MARÍA, "Persona identificada o identificable, el afectado o interesado y el procedimiento de disociación en la protección de datos de carácter personal. Comentario al artículo 3.", *Comentario a la Ley de Protección de Datos de Carácter Personal*, Aranzadi, Madrid, 2010.

ROSSNAGEL, ALEXANDER, "Selbstregulierung im Datenschutz", *Medien, Ordnung und Innovation*, Springer Verlag Berlin Heidelberg, 2006.

ROURA, SANTIAGO, "La lucha por los Derechos Fundamentales y el federalismo en los Estados Unidos. ", *Anuario da Facultade de Dereito da Coruña*, nº 4, 2000, pág.435-448.

RUIZ CARRILLO, ANTONIO, *Los datos de carácter personal*, Bosch, Barcelona, 1999,

RÚIZ MIGUEL, CARLOS, *La configuración Constitucional del Derecho a la Intimidad*, Tecnos, Madrid, 1995.

—"El Derecho a la Protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea. Análisis Crítico.", *Revista de Derecho Comunitario Europeo*, nº 14, 2003, pág. 7-43.

—"Los Derechos Fundamentales en la Unión Europea renovada", *Revista del Ministerio de Trabajo e Inmigración*, nº 92, 2011, pág. 33-52.

SABATER FERNÁNDEZ, MARÍA CARMEN, "Comunicación. El debate en torno a la autorregulación y la cancelación de datos personales en internet.", *Revista Iberoamericana para la Investigación y el Desarrollo Educativo: RIDE*, nº 1, 2010, pág. 151-168.

SÁENZ DE SANTAMARÍA, PAZ ANDRÉS, "La Carta de los Derechos Fundamentales de la Unión Europea en la práctica española", *Revista de derecho de la Unión Europea*, nº 15, 2008, pág. 233-255.

SÁIZ ARNAIZ, ALEJANDRO, *La apertura constitucional al derecho internacional y europeo de los derechos humanos. El artículo 10.2 de la Constitución Española.*, Consejo General del Poder Judicial, Madrid, 1999.

SALDAÑA, NIEVES, "El Derecho a la Privacidad en los Estados Unidos: Aproximación diacrónica a los intereses constitucionales en juego", *Teoría y realidad Constitucional*, nº 28, 2011, pág. 279-312.

—"The Right to Privacy" La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el Centenario legado de Warren y Brandeis", *UNED Revista de Derecho Político*, nº 85, 2012.

- SALVADOR AYESTARÁN, IGNACIO , "La firma digital. Una tecnología para la intercomunicación en la sociedad-red", *Revista española de documentación científica*, nº 1, 2001.
- SALVADOR MARTÍNEZ, MARÍA, *Autoridades Independientes*, Ariel, Barcelona, 2002.
- SÁNCHEZ BRAVO, ÁLVARO A., *La protección del derecho a la libertad informática en la Unión Europea*, Universidad de Sevilla. Secretariado de Publicaciones, 1998.
- "Nuevo marco europeo de protección de datos personales", *Derechos Humanos y protección de datos personales en el siglo XXI*, Punto Rojo Libros, 2013.
- SÁNCHEZ GONZÁLEZ, SANTIAGO, "De la imponderable ponderación y otras artes del Tribunal Constitucional", *Teoría y Realidad Constitucional*, nº 12/13, 2003, pág. 351-382.
- SANCHO VILLA, DIANA, "Protección de datos personales y transferencia Internacional. Cuestiones de ley aplicable.", *Revista jurídica de Castilla y León*, nº 16, 2008, pág. 401-446.
- "Developing Search Engine Law: It Is Not Just about the Right to Be Forgotten.", *Legal Issues of Economic Integration*, nº 4, 2015, pág. 357-382
- "Artículo 2.1 Ámbito de aplicación territorial.", *Comentario a la Ley de protección de datos de carácter personal*, Aranzadi, 2010.
- SANTAOLALLA LÓPEZ, FERNANDO, *Derecho Parlamentario Español*, Espasa Calpe, Madrid, 1990,
- SARRIÓN ESTEVE, JOAQUÍN , "Tras la larga sombra de Google Spain", *Universidad de Valencia*, nº 1, 2015.
- SCHILD, HANS-HERMANN; RONELLENFITSCH , MICHAEL;
Hessisches Datenschutzgesetz. Kommentar. Kommunal- und Schul-Verlag, Wiesbaden, 2009,
- SCHMITT, CARL, *Teoría de la Constitución (Verfassungslehre, 1928)*, Alianza Editorial, Madrid, 2001.

SERRANO ALONSO, EDUARDO, *Derecho de la persona*, La Ley, Madrid, 1992.

SERRANO PÉREZ, MARÍA MERCEDES, "El derecho Fundamental a la protección de datos. Su contenido esencial.", *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, nº 1, 2005, pág. 245-265.

—*El derecho fundamental a la protección de datos. Derecho español y comparado*, Thomson Civitas, Madrid, 2003.

SEVILLA JIMÉNEZ, MARTÍN ; TORREGROSA MARTÍ, TERESA;, *Anales de economía aplicada 2010*, Delta Publicaciones Universitarias; ASEPELT, Madrid, 2010.

STEINMEYER ESPINOSA, ALFREDO, "¿Permite el acceso a la información pública el acceso a datos personales?", *Serie Bibliotecnología y Gestión de Información* , nº 79, 2013.

SUÁREZ RUBIO, SOLEDAD MARÍA, "La protección de la confidencialidad de los datos y documentos sanitarios", *Documentos de trabajo. Seminario permanente de Ciencias Sociales*, nº 10, 2012, pág. 15-38.

TASCÓN LÓPEZ, RODRIGO, "La protección de datos personales de los trabajadores", *Revista Jurídica de Castilla y León*, nº 16, 2008, pág. 447-501.

TASCÓN LÓPEZ, RODRIGO;, "Comentario al Artículo 6. Los Ficheros empresariales sobre trabajadores y los derechos de los mismos en el marco contractual con el empleador.", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Madrid, 2010.

TEJERINA, OFELIA, *Seguridad de Estado y Privacidad*, Reus, Barcelona 2014.

TOCQUEVILLE, ALEXIS DE, *La democracia en América*, Trotta, Madrid, 2010.

TOMÁS MALLÉN, BEATRIZ;, "Privacidad vs. seguridad en el ámbito europeo", *Los derechos a la intimidad y a la privacidad en el siglo XXI*, Dykinson, Madrid, 2014.

TORRES, JORDI, *Empresas en la nube*, Libros de cabecera, Barcelona, 2011.

TRONCOSO REIGADA, ANTONIO, *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, Valencia, 2010,

- Comentario a la ley de protección de datos de carácter personal*, Aranzadi, Madrid, 2010.
- "Las redes sociales a la luz de la propuesta de Reglamento general de protección de datos personales. Parte Uno.", *IDP Revista de Internet, derecho y política*, nº 15, 2012, pág.61-75.
- "Las redes sociales a la luz de la propuesta del reglamento general de protección de datos personales. Parte dos.", *IDP Revista de Internet, derecho y política.*, nº 16, 2013, pág.1-20.
- "La administración electrónica y la protección de datos personales", *Revista jurídica de Castilla y León*, nº 16, 2008, pág.31-113.
- "Comentario artículo 4 LOPD El principio de Calidad de los datos", *Comentario a la Ley de Protección de Datos de Carácter Personal*, Aranzadi, 2010.
- "Comentario al artículo 11. La comunicación de datos personales. El concepto de cesión.", *Comentario a la Ley de Protección de Datos de Carácter Personal*, Aranzadi, Madrid, 2010.
- TÜRK, ALEX, *La ley francesa de protección de datos de carácter personal*, Agencia Española de Protección de Datos, Santander, 2005.
- <https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/ConferenciaTURK.pdf>
- VELEIRO REBOREDO, BELÉN , "Incidencia de la normativa en las empresas que prestan sus servicios a través de Internet", *Boletín económico de ICE, Información Comercial Española*, nº 2812, 2004, pág.1000-1016.
- VIDAL MARÍN, TOMÁS; "La libertad sindical", *Anuario Parlamento y Constitución*, nº 4, 2000, pág. 201-238.
- VILASAU SOLANA, MÓNICA, "El fin de la situación de transitoriedad: la Ley Orgánica 15/1999, de 13 de diciembre , de protección de datos de carácter personal ya tiene desarrollo reglamentario", *Revista de Intenet, Derecho y Política*, nº 7, 2008.

- "La Directiva 2006/24/CE sobre conservación de datos del Tráfico en las comunicaciones electrónicas: seguridad vs. privacidad", *IDP Revista de Internet, Derecho y Política*, nº 3, 2006.
- "Privacidad, redes sociales y el factor humano", *Derecho y redes sociales*, Civitas, Madrid, 2010.
- VILLAVERDE MENÉNDEZ, IGNACIO, *El legislador de los derechos fundamentales*, Tecnos, Madrid, 2004.
- "Ciberconstitucionalismo. Las TIC y los espacios virtuales de los derechos fundamentales", *Revista Catalana de dret públic*, nº 35, 2007, pág.19-42.
- "La intangibilidad competencial de los derechos fundamentales. Forma de estado y derechos fundamentales.", *Teoría y realidad constitucional*, nº 20, 2007, pág.321-357.
- "La intimidad, ese "terrible derecho" en la era de la confusa publicidad virtual", *Espaço Jurídico*, nº 3, 2013, pág.57-72.
- "El control de constitucionalidad de las reformas constitucionales ¿Un oximorón constitucional? Comentario al ATC 9/2012", *Teoría y realidad constitucional*, nº 30, 2012, pág.483-498.
- "El control previo de constitucionalidad de las normas con rango de ley. Crónica de un escéptico." *Revista catalana de dret públic*, nº 49, 2014, pág.20-40.
- "Actividad informativa y derecho privado", *Derecho privado y Constitución.*, nº 10, 1996, pág.219-258.
- "A propósito de la reciente jurisprudencia del Tribunal Constitucional sobre el empleo de cámaras ocultas", *Derecom*, nº 10, 2012.
- "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo.", *Revista española de derecho constitucional*, nº 14, 1994, pág.187-224.

- "Lo que cuestan los derechos fundamentales. Una revisión de su tutela ante los tribunales constitucionales.", *Fundamentos. Cuadernos monográficos de teoría del estado, derecho público e historia constitucional*, nº 4, 2006, pág.351-384.
- "Comentario al Artículo 6. Derecho de oposición. ", *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Madrid, 2010.
- VON IHERING, RUDOLF, *La Lucha por el Derecho*, Civitas, Madrid, 1985.
- WARREN, SAMUEL; BRANDEIS, LOUIS, *El derecho a la intimidad*, Civitas, Madrid, 1995.
- WESTIN, ALAN, F, *Privacy and Freedom*, The Bodley Head, New York, 1967.
- WESTIN, ALAN; SOLOVE, DANIEL, *Privacy and Freedom*, Ig Pub, New York, 2015.
- ZAMORA JIMÉNEZ, ÁNGEL JOSÉ; "Comentario al artículo 2.2 c) Ficheros establecidos para la investigación del terrorismo y formas graves de delincuencia organizada.", *Comentario a la Ley Orgánica de Protección de Datos de carácter personal.*, Aranzadi, Madrid, 2010.
- ZÁRATE ROJAS, SEBASTIAN, "La problemática entre el derecho al olvido y la libertad de prensa", *Derecom*, nº 13, 2013.

ANEXO A BIBLIOGRAFÍA. SITIOS WEB DE INTERÉS.

ACTAS DE LA PONENCIA CONSTITUCIONAL DE 1977, "congreso.es"

<http://www.congreso.es/constitucion/ficheros/actas/actas.pdf>,

AEPD, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

INFORMES JURÍDICOS.

—"Informe sobre DNI como dato personal 0334/2008",

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2008-0334_La-creaci-oo-n-de-una-base-de-datos-en-la-que-s-oo-lo-aparezca-el-DNI-o-el-NIF-queda-sometida-a-toda-la-normativa-de-Protecci-oo-n-de-Datos.pdf,

—"Informe sobre implicación de la LOPD a la actividad de particulares que comparten fotos de sus hijos por Internet."

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0615_Inaplicaci-oo-n-LOPD-a-actividad-de-particulares-que-comparten-fotos-de-sus-hijos-a-trav-ee-s-de-Internet.pdf,

—"Informe sobre número de teléfono y concepto de dato personal 285/2006. "

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2006-0285_N-uu-mero-de-tel-ee-fono-y-concepto-de-dato-personal.pdf,

—"IP como Dato Personal. Informe 327/2003"

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf,

—"Informe Jurídico. Consentimiento otorgado por menores de edad."

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Consentimiento-otorgado-por-menores-de-edad.pdf,

—"Informe Jurídico 0167/2005 Naturaleza y alcance del Derecho de Acceso."

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/derecho_acceso_rectificacion_cancelacion_oposicion/common/pdfs/2005-0167_Naturaleza-y-alcance-del-derecho-de-acceso.pdf,

—"Informe jurídico 0296/2008 Libros de registro de la Iglesia Católica"

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/derecho_acceso_rectificacion_cancelacion_oposicion/common/pdfs/2008-0296_Derecho-de-cancelacion-de-datos-de-los-libros-de-confirmaciones-y-matrimonios-de-la-iglesia-catolica.p,

—"Informe Jurídico 297375/2011 Protección de datos de trabajadores de la Administración Pública"

http://www.fsc.ccoo.es/comunes/recursos/99922/doc96541_Informe_de_la_Agencia_de_Proteccion_de_Datos_sobre_listados_de_oposiciones.pdf,

—"Informe Jurídico 0575/2008 Fichero con números de teléfono móvil."

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2008-0575_Fichero-con-numeros-de-telefonos-moviles.pdf,

—"Informe Jurídico 0132/2010 Publicación de datos personales en medios de comunicación.",

https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2010-0132_Publicacion-de-datos-personales-en-medios-de-comunicacion.pdf,

—"Informe Jurídico 0279/2009. Concepto de Fichero."

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/naturaleza_publicacion_ficheros/common/pdfs/2009-0279_Concepto-de-fichero.pdf,

ORIENTACIONES Y GUÍAS DE LA AEPD.

—Sección de la página web de la AEPD sobre el Reglamento General de Protección de Datos.

<https://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-id.php>

—"Orientaciones sobre protección de datos en la reutilización de la información del sector público."

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_proteccion_datos_Reutilizacion.pdf,

—"Orientaciones y garantías en los procedimientos de anonimización de datos personales.",

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf,

—"Recomendaciones. Derechos de niños y niñas. Deberes de los padres y madres."

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2008/recomendaciones_menores_2008.pdf,

—"Directrices para la elaboración de contratos entre responsables y encargados del tratamiento",

<https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricescontratos.pdf>

—"Guía para el cumplimiento del deber de informar",

<https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf>

—"Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento. Guía Protección de datos UE ",

https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf

—"Guía para clientes que contrates servicios de Cloud Computing",

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf,

—"Guía para la videovigilancia"

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf,
,

—"Guía del Responsable del Fichero"

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf,

—"Guía de Seguridad de Datos"

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf,

—"Guía La protección de datos en las relaciones laborales"

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales2.pdf,

—"Guía para el ciudadano. El derecho fundamental a la protección de datos."

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO.pdf,

MEMORIAS DE LA AEPD.

—“Memoria 2015”

https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2015/Memoria_AEPD_2015.pdf

—“Memoria 2014”

http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/Memoria_AEPD_2014.pdf,

—“Memoria 2009”

http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2009/AEPD_memoria_2009.pdf,

ALGUNAS DE LAS RESOLUCIONES DE LA AEPD MENCIONADAS.

—“Estándares internacionales sobre protección de datos personales y privacidad. Resolución de Madrid.”

http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf,

—“Resolución E/00561/2004 DNI como dato personal”

http://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2005/common/pdfs/E-00561-2004_Resolucion-de-fecha-20-04-2005_Art-ii-culo-11-LOPD.pdf,

—“Resolución R/02762/2015 ASSEMBLEA NACIONAL CATALANA Y ÒMNium.”

<https://www.agpd.es/portalwebAGPD/resultados-ides-idphp.php>

—“Resolución 00862/2006 Banco de Sabadell”

http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2008/common/pdfs/PS-00002-2008_Resolucion-de-fecha-17-07-2008_Art-ii-culo-5.4-y-5.5-LOPD.pdf,

—“Resolución R/01374/2015 retira de datos personales publicados en Sentencia penal. ”,

http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2015/common/pdfs/TD-00022-2015_Resolucion-de-fecha-01-06-2015_Art-ii-culo-16-LOPD.pdf,

—“Resolución R/01349/2008 Contratación de un servicio de telefonía móvil por una menor.”

http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2008/common/pdfs/PS-00315-2008_Resolucion-de-fecha-11-11-2008_Art-ii-culo-4.3-y-6-LOPD_Recurrida.pdf,

—"Resolución E 04001/2011" artículo 6 LOPD.

http://www.agpd.es/portalwebAGPD/resoluciones/recursos_reposicion/rr_sobre_archivo_de_actuaciones/common/pdfs/REPOSICION-E-04001-2011_Resolucion-de-fecha-13-08-2012_Art-ii-culo-6-LOPD.pdf,

VARIOS AUTORES, "Los Retos de la Seguridad y Privacidad en la atención integral sanitaria y social", *XIII Foro de Seguridad y Protección de Datos en Salud*, nº 116, 2016.

<http://www.seis.es/ForoPD2016/imagen/Programa.pdf>

CNI CENTRO NACIONAL DE INTELIGENCIA, "Normas para la protección de Información clasificada"

https://www.cni.es/comun/recursos/descargas/Normas_de_la_Autoridad_Nacional_para_la_Proteccion_de_la_Informacion_Clasificada.pdf,

—"Protección de la información clasificada"

http://www.cni.es/comun/recursos/descargas/Proteccion_de_la_Informacion_Clasificada.pdf,

COMISIÓN EUROPEA, "Informe de Grupo de Trabajo WP29 4/2007 sobre el concepto de datos personales."

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf,

—"Comunicación de la Comisión al Consejo y al Parlamento Europeo. Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia.", *Comunicados y estudios de la UE.*, nº COM(2010)385, 2010

—"La Unión Europea y los Estados Unidos. Socios Mundiales con responsabilidades mundiales.",

http://eeas.europa.eu/us/docs/infopack_06_es.pdf,

DIARIO DE SESIONES DEL CONGRESO DE LOS DIPUTADOS, 31, "congreso.es",
http://www.congreso.es/public_oficiales/L0/CONG/DS/C_1978_130.PDF,

ECHEBARRÍA, JUAN JOSÉ, "elpais.es"

http://elpais.com/diario/1989/07/23/espana/617148001_850215.html,

ELVIRA PERALES, ASCENSIÓN, "congreso.es"

<http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2>,

GOBIERNO DE ESPAÑA. MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE. OBSERVATORIO TECNOLÓGICO., "Introducción a la seguridad informática. Seguridad de la información."

<http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1>,

—PAE PORTAL ADMINISTRACIÓN ELECTRÓNICA, "MAGERIT v.3 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información."

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vvk2nUvkveUk,

MERINO NORVERTO, MARÍA, "congreso.es"

<http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=10&tipo=2>,

PRIETO GUTIERREZ, JESÚS MARÍA, "mjusticia.gob.es"

<http://www.mjusticia.gob.es/cs/Satellite/1292344076928?blobheader=application%2Fpdf&blobheadername1=Content...>,

SNOWDEN, EDWARD;, "La sociedad abierta avanza"

http://elpais.com/elpais/2015/06/04/opinion/1433436340_438817.html,

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, Sentencia 6 de octubre de 2015. Caso Puerto Seguro.

http://curia.europa.eu/juris/document/document_print.jsf?doclang=ES&text=&pageIndex=1&part=1&mode=req&docid=169195&occ=first&dir=&cid=455702

—Comunicado de prensa Nº 117/15 06 de octubre de 2015 Sentencia en el asunto C-362/14

<http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf>,

ITU INTERNATIONAL TELECOMMUNICATION UNION (UIT EN ESPAÑOL), "itu.int"

<http://www.itu.int/es/about/Pages/default.aspx>,

SENTENCIAS DEL TRIBUNAL CONSTITUCIONAL.

STC 11/1981, de 8 de abril.
STC 18/1981 de 8 de junio.
STC 36/1982, de 16 de junio.
STC 101/1983, de 18 de noviembre.
STC 67/1984, de 7 de junio.
STC 325/1994, de 12 de diciembre.
STC 110/1984, de 26 de diciembre.
STC 53/1985, de 11 de abril.
STC 159/1986, de 12 de diciembre.
STC 254/1988, de 21 de diciembre.
STC 171/1990, de 12 de noviembre.
STC 53/1991, de 14 de febrero.
STC 64/1991, de 22 de marzo.
STC 85/1992, de 8 de junio.
STC 254/1993, de 20 de julio.
STC 372/1993, de 13 de diciembre.
STC 143/1994, de 9 de mayo.
STC 170/ 1994, de 7 de junio.
STC 66/1995, de 8 de mayo.
STC 176/1995, de 11 de diciembre.
STC 11/1998, de 13 de enero.
STC 94/1998, de 4 de mayo.
STC 202/1999, de 8 de noviembre.
STC 292/2000, de 30 de noviembre.

STC 46/2001, de 15 de febrero.

STC 81/2001, de 26 de marzo.

STC 156/2001, de 2 de julio

STC 41/2002, de 25 de febrero.

STC 99/2002, de 6 de mayo.

STC 14/2003, de 30 de enero.

STC 114/2006, de 5 de abril.

STC 236/2007 de 7 noviembre.

STC 29/2013, de 11 de febrero.

STC 35/2016, de 3 de marzo.

STC 38/2016, de 3 de marzo.

STC 39/2016, de 3 de marzo.

SENTENCIAS DEL TRIBUNAL SUPREMO.

STS 1105/1999, de 18 de febrero
STS 482/2006, de 25 de enero de 2006
STS 921/2006, de 26 de septiembre
STS 4646/2008, de 19 de septiembre
STS 2555/2009, de 17 de marzo
STS 4047/2010, de 15 de julio.
STS 4057/2010, de 15 de julio.
STS 4050/2010, de 15 de julio.
STS 1084/2010, de 9 de diciembre
STS 6153/2011, de 3 de octubre de 2011.
STS 1440/2013, de 18 de febrero
STS 1715/2013, de 6 de marzo.
STS 355/2014, de 22 de enero.
STS 2618/2014, de 13 de mayo.
STS 2040/2014, de 21 de mayo.
STS 3896/2014, de 3 de octubre.
STS 672/2014, de 19 de noviembre.
STS 545/2015, de 15 de octubre.
STS 185/2016, de 3 de febrero.
STS 532/2015, de 23 de septiembre.
STS 4020/2016, de 21 de julio
STS 4070/2016 de 7 de julio.
STS 4077/2016 de 12 de julio.
STS 185/2016, de 3 de febrero de 2016.
STS 796/2016, de 1 de marzo de 2016.