TESIS DOCTORAL

EL DERECHO AL OLVIDO DIGITAL DEL PASADO PENAL

DOCTORANDA

INMACULADA JIMÉNEZ-CASTELLANOS BALLESTEROS

DIRECTOR

MANUEL CARRASCO DURÁN

ÍNDICE

Capítulo segundo

EL DERECHO AL OLVIDO DIGITAL

Capítulo tercero

EL DERECHO AL OLVIDO DIGITAL DEL PASADO PENAL

ABREVIATURAS

AA .....Actualidad Administrativa

AA.VV.....Varios Autores

ADPEP .....Anuario de Derecho Público Estudios Políticos.

AEPD .....Agencia Española de Protección de datos

art./s .....artículo/s

art. cit .....artículo citado

ATC .....Auto del Tribunal Constitucional

BOCG.....Boletín Oficial de las Cortes Generales

BOE.....Boletín Oficial del Estado

CDFUE.....Carta de los Derechos Fundamentales de la Unión Europea

CE .....Constitución Española

CEDH .....Convenio Europeo de Derechos Humanos.

CENDOJ.....Centro de Documentación Judicial del CGPJ

CEPC .....Centro de Estudios Políticos y Constitucionales

Cfr .....Confróntese

CGPJ.....Consejo General del Poder Judicial

(coord.).....coordinador

CP .....Código Penal

(dir./s) .....director/es

DA .....Revista de Documentación Administrativa

DOUE.....Diario Oficial de la Unión Europea

DSCG.....Diario de Sesiones de las Cortes Generales

ECRIS .....Sistema de información Europeo de Antecedentes Penales

(ed./s) .....editor/es

ERODAC.....Sistema de comparación de huellas dactilares

EUROJUST .....Unidad Europea de Cooperación Judicial

EUROPOL.....Oficina Europea de Policía

FBBVA .....Fundación Banco Bilbao Vizcaya

FJ .....Fundamento Jurídico

IDP .....Revista de Internet, Derecho y Política

LOPD .....Ley Orgánica de Protección de Datos

LORTAD.....Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos

Núm.....Número

OCDE.....Organización para la Cooperación y el Desarrollo Económico

op. cit.....obra citada

pág./s .....página/s

PUV.....Publicaciones de la Universidad de Valencia

RCEC .....Revista del Centro de Estudios Constitucionales

REDC .....Revista Española de Derecho Constitucional

ReDCE .....Revista de Derecho Constitucional Europeo

REDF .....Revista Europea de Derechos Fundamentales

RGPD.....Reglamento General de Protección de datos

RJC .....Revista Jurídica de Catalunya

SIA .....Sistema de información aduanera

SIV .....Sistema de información de visados

ss.....siguientes

STC .....Sentencia del Tribunal Constitucional

STS .....Sentencia del Tribunal Supremo

TC .....Tribunal Constitucional

TEDH .....Tribunal Europeo de Derechos Humanos

TFUE.....Tratado de Funcionamiento de la Unión Europea

TJUE .....Tribunal de Justicia de la Unión Europea

TIC .....Tecnologías de la información y de la comunicación

TUE.....Tratado de la Unión Europea

UE .....Unión Europea

UNED .....Universidad Nacional de Educación a Distancia

vid.....véase

INTRODUCCIÓN

La sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 constituye el punto de partida, el *leading case,* a partir del cual comienza a utilizarse de forma generalizada la expresión derecho al olvido digital. La repercusión mediática y práctica de esta resolución, de gran impacto social por la conocida multinacional demandada, fue indudable en el ámbito de Internet. De hecho, los medios de comunicación se hacían eco de la decisión poniendo el acento en la creación, a su juicio, de un instrumento demasiado poderoso en la medida en que podía potencialmente lesionar la libertad de expresión y el derecho del público a la información. No obstante, la sentencia no sentó una construcción general del derecho al olvido digital sino que vino a dar respuesta, por la vía de la interpretación de la Directiva 95/46/ CE a la luz de la Carta de los Derechos Fundamentales de la Unión Europea, a las cuestiones prejudiciales que la Audiencia Nacional planteó ante el Tribunal de Justicia de la Unión Europea. En cualquier caso el problema de fondo sobrepasaba el debate en torno a la existencia o no del denominado derecho al olvido digital.

Para su comprensión integral hay que tener en cuenta los cambios que ha supuesto la revolución tecnológica. En la sociedad digital en la que vivimos es innegable el valor alcanzado por los datos personales. Las nuevas tecnologías de la información ofrecen formas y canales de comunicación que exigen desvelar a cada instante aspectos de nuestra vida, unos personales y otros más íntimos. Estos datos aparentemente inocuos se convierten en

identidades digitales que facilitan un rápido conocimiento de contactos, preferencias, direcciones IP o hábitos del usuario.

Paralelamente, las características de Internet como espacio de comunicación libre, abierto y público, que facilita el anonimato y que aparentemente no deja rastro, nos han estimulado a ser menos prudentes con nuestra privacidad. La deformación de la noción de lo público, lo privado y lo íntimo es una realidad, sobre todo, para los nativos digitales. El hecho de que lo que publicamos se expandirá con el carácter viral de la red no parece preocuparnos.

Por consiguiente, nuevas amenazas para los derechos fundamentales han ido apareciendo en el espacio de Internet. Surgen realidades hasta hace unos años desconocidas a las que el derecho debe dar respuesta. Estamos en un terreno lleno de riesgos cuando hablamos del conflicto entre derechos y tecnología. Todo lo que significa intentar someter la tecnología al derecho es un asunto complejo, como lo ilustra la propia realidad que nos envuelve. Internet amplifica y facilita de un modo sin precedentes la difusión de la información. Tanto la propagación como el acceso a los contenidos en la red no tienen límites. Nuestros datos personales están disponibles a escala global, al instante y almacenados *sine die*. El fenómeno digital ha sobrepasado las barreras del espacio y del tiempo y se ha caracterizado por la inmediatez y la omnipresencia.

La actividad de los motores de búsqueda, con sus innumerables ventajas, representa una de estas amenazas. Cada acto o faceta de nuestra vida puede ser rastreado por alguien con una simple búsqueda por nuestro

nombre y apellidos. El resultado es la creación de un perfil de nuestra personalidad que puede ser utilizado para los fines más diversos. Este retrato, en ocasiones descontextualizado, puede mostrar aspectos eventualmente lesivos para la intimidad, la reputación o el libre desarrollo de nuestro proyecto vital, que desearíamos que cayeran en el olvido.

Es en este contexto donde hay que situar la sentencia del Tribunal de Justicia de la Unión Europea. Esta resolución vino precedida por otra dictada el 8 de abril del mismo año y por el mismo Tribunal en la que declaraba inválida la Directiva sobre retención de datos, poniendo de relieve la extraordinaria importancia del derecho a la protección de datos frente a la actuación de los poderes públicos. Siguiendo esta línea, la sentencia de 13 de mayo de 2014 se pronunció en análogo sentido, a propósito del impacto que en el tratamiento de la información generaban los motores de búsqueda en Internet frente al que llevan a cabo las páginas webs. No obstante, las implicaciones de esta sentencia fueron mucho más allá porque abordó aspectos tan conflictivos como la aplicabilidad de la legislación europea de protección de datos a los servicios de Internet que tienen sede en otros países fundamentalmente en Estados Unidos, y a la responsabilidad de los establecimientos de esas empresas en el territorio nacional. Lo decisivo de esta resolución es la afirmación inequívoca de la prevalencia del derecho fundamental a la protección de datos sobre los intereses económicos de las empresas de Internet mediante la asignación de responsabilidad a los gestores de los motores de búsqueda en el tratamiento de los datos.

El fenómeno de la descontextualización de la información en Internet, que convierte cualquier dato en una realidad permanente cuando ya no se corresponde con la misma, justifica la reivindicación del reconocimiento de un derecho al olvido digital en lo relacionado con el pasado penal de una persona. Si el paso del tiempo provocaba que una condena penal o el indulto de un sujeto plenamente rehabilitado fuera olvidado, la tecnología lo ha devuelto a la actualidad de manera permanente, con el consiguiente riesgo de estigmatización social.

Al margen de la discusión sobre si el derecho al olvido digital es un derecho de naturaleza autónoma, una concreción de los derechos a la intimidad y al honor o una manifestación del derecho fundamental a la protección de datos, la pregunta sería hasta qué punto es exigible que determinadas informaciones lícitas sobre el pasado penal de una persona sin relevancia pública actual pueden ser sustraídas al acceso de los usuarios de Internet. La respuesta desde el punto de vista del derecho fundamental a la protección de datos la ha dado la jurisprudencia española sobre la base de la sentencia del caso *Google.*

A la vista de lo expuesto, el presente trabajo pretende analizar el derecho al olvido digital desde la perspectiva del derecho fundamental a la protección de datos personales tras un amplio repaso a este novedoso derecho fundamental como categoría autónoma, sus relaciones con el derecho fundamental a la intimidad personal y familiar, los principios y facultades que conforman su contenido esencial y la particularidad de su protección por una autoridad de control independiente. Su régimen jurídico se halla actualmente

pendiente de la entrada en vigor del Reglamento General de Protección de datos, así como de la tramitación en la Cortes Generales del proyecto de ley Orgánica de Protección de datos Personales.

Seguidamente, el trabajo se detiene en el estudio de los derechos relacionados con el principio de calidad de los datos, fundamento último del derecho al olvido digital. A tales efectos, el tradicional derecho de cancelación de datos personales ha sido sustituido en la normativa europea por el término supresión, con una especial referencia al derecho al olvido. Para indagar en este derecho hacemos un somero repaso a sus orígenes, en los que el elemento temporal es pieza clave, de tal manera que el problema se da, con respecto a acontecimientos que fueron públicos en el pasado, cuando el transcurrir del tiempo ha hecho que vuelvan a formar parte de la vida privada. A todo esto se une que el almacenamiento permanente de las informaciones en Internet ha desembocado en la necesidad del reconocimiento de una facultad de control de los datos personales que circulan por la red. De ahí el enfoque del derecho al olvido digital desde la perspectiva del derecho fundamental a la protección de datos.

El tercer capítulo abordará los conflictos entre el derecho al olvido digital del pasado penal y las libertades informativas, así como entre este derecho y el principio de transparencia. Frente a las voces alarmistas que sostenían que el derecho al olvido digital permitía la construcción del pasado a medida y que sentaba las bases de la censura de la libertad de información, la jurisprudencia del Tribunal Supremo ha venido a implementar la sentencia del caso *Google*, trazando las líneas esenciales para la construcción jurídica de este derecho.

En resumen vamos a acercarnos tímidamente a una realidad en plena ebullición que no tardará en plantearnos muchos más interrogantes. La elaboración del trabajo ha venido supeditada por dos condicionantes: por una parte, la falta de jurisprudencia del Tribunal Constitucional sobre esta materia, y por otro lado, el carácter novedoso del tema, que ha provocado la reforma de la normativa vigente para adaptarla a los constantes cambios del mundo digital. De hecho, asumimos el riesgo de que por la evolución tanto de la técnica como de la conciencia social, algunas afirmaciones que se hacen queden dentro de algún tiempo obsoletas. No obstante, hemos procurado hacer un estudio lo más riguroso posible sobre el derecho fundamental a la protección de datos para dejar constancia de la creciente importancia que va a tener para la protección de la vida privada en la sociedad tecnológica que nos ha tocado vivir.

Capítulo primero

EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

1. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS COMO DERECHO AUTÓNOMO. 2. LA RELACIÓN DE LOS DERECHOS FUNDAMENTALES A LA PROTECCIÓN DE DATOS Y A LA INTIMIDAD PERSONAL Y FAMILIAR. 3. LA DELIMITACIÓN DEL CONTENIDO ESENCIAL DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES. 3.1. Principios. 3.1.1. Transparencia y derecho a la información. 3.1.2. Consentimiento. 3.1.3. Calidad de los datos. 3.1.4. Seguridad de los datos. 3.2. De los derechos ARCO a los derechos ARSLPO. 3.3. La autoridad de control independiente. 3.4. Límites**. 4. EL RÉGIMEN JURÍDICO DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES.**

1. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS COMO DERECHO AUTÓNOMO.

La afirmación del carácter iusfundamental del derecho a la protección de datos en el ordenamiento jurídico español es relativamente reciente. La Constitución española no reconoce este derecho de manera explícita, ni lo incluye en el catálogo de derechos fundamentales que representa su Título I.

Los derechos de la personalidad se encuentran ubicados en el artículo 18 de nuestra Carta Magna. El honor, la intimidad y la propia imagen están garantizados en el párrafo primero. Los tradicionales derechos a la inviolabilidad del domicilio y al secreto de las comunicaciones, por su parte, en los apartados segundo y tercero. El emplazamiento de todos ellos en la Sección primera del Capítulo II, del Título I de nuestra norma suprema les confiere la condición de derechos fundamentales con la máxima relevancia constitucional, pues disponen de un conjunto de garantías jurisdiccionales exclusivas, como la protección a través de los procedimientos preferentes y sumarios y a través del recurso de amparo ante el Tribunal Constitucional -en adelante TC-, además de la reserva de Ley Orgánica y el procedimiento de revisión constitucional.

Si bien es cierto que el artículo 18 incluyó en el párrafo cuarto la referencia a la limitación del uso de la informática como garantía de otros derechos fundamentales, la falta de precisión del texto constitucional propició, en un primer momento, una interpretación ambigua sobre la existencia autónoma del derecho a la protección de datos. Algunos de los derechos

incluidos en este precepto eran considerados, en cierta manera, como concreciones o manifestaciones del derecho a la intimidad (derecho a la propia imagen o a la inviolabilidad del domicilio)[1]. En este sentido no estuvo claro, en un principio, si el artículo 18.4 CE recogía un derecho nuevo e independiente del derecho a la intimidad, o simplemente una repetición o matización innecesaria del párrafo primero[2]. Desde esta última perspectiva, el derecho a la intimidad, sus mecanismos jurídicos de tutela y su ámbito de protección resultaban suficiente garantía para el individuo en el desarrollo de su vida privada[3].

Lo cierto es que la irrupción de la informática y, sobre todo, Internet y las nuevas tecnologías en el tratamiento de la información, pusieron de manifiesto nuevos peligros y amenazas, que no pueden equipararse a los riesgos que para los derechos de la persona derivaban del uso convencional de los datos personales[4]. Mediante la utilización de las técnicas informáticas y de la transmisión de datos entre ordenadores, con su capacidad de proceso, se puede ejercer un control social y, sin que la persona llegue a percatarse, interferir en su vida privada[5]. Surge, por tanto, la necesidad de reforzar las garantías personales frente a la incidencia de la informática, que ha eliminado las barreras del tiempo y el espacio, y, sobre todo, frente a quienes aspiran al

---

[1] PARDO FALCÓN, J.: "Los derechos del artículo 18 de la Constitución en la Jurisprudencia del Tribunal Constitucional", núm. 34, 1992, pág. 174.
[2] VILLAVERDE MENÉNDEZ, I.: "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993", *REDC*, núm. 41, 1994, págs. 187 y ss.
[3] HERRANZ ORTIZ, A. I.: *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, 1998, pág. 93.
[4] *Ibidem,* pág. 75.
[5] En este sentido DAVARA RODRÍGUEZ, M. A.: *Manual de Derecho Informático*, Aranzadi, Cizur Menor (Navarra), 2015, pág. 51.

control de la sociedad[6]. Fenómenos como la recopilación masiva de información, la conexión de datos que en sí mismos son inocuos, pero que permiten construir perfiles de nuestra personalidad, y, en general, el tratamiento automatizado de los datos personales, exigen mecanismos jurídicos de defensa nuevos y más reforzados que los que se derivan del derecho a la intimidad. Cuando se trata del conflicto entre los derechos de la personalidad y la informática, conviene articular una defensa o protección unitaria y no condicionada por el bien objeto de agresión[7].

Los avances tecnológicos, unidos al fortalecimiento del derecho fundamental a la protección de datos en el ámbito comparado, donde se irán poniendo las bases de un reconocimiento de este derecho cada vez más homogéneo, contribuyeron a dejar constancia de la necesidad de su tutela en el ordenamiento jurídico español. La doctrina científica dio el primer paso[8]. Sin embargo, su consagración definitiva fue el resultado de la evolución de la jurisprudencia del Tribunal Constitucional.

---

[6] Como señala Fernández Esteban, "el desarrollo tecnológico de los sistemas de comunicación, la informática y las modernas técnicas de captación y grabación del sonido y la imagen hacen que cada día sea más difícil conservar intacto el ámbito de la propia vida privada, que no hace muchos años se salvaguardaba solo con la protección del domicilio y la correspondencia… En la comunicación electrónica las fronteras entre lo público y lo privado tienden a difuminarse. Es cierto que la sociedad de masas permite el anonimato, pero la tecnología allana la vida privada… Internet introduce una evidente amenaza para la protección de la vida privada ya que es posible la difusión de elementos relativos a la imagen y vida particular de los individuos a través de la Red". *Vid.* FERNÁNDEZ ESTEBAN, M. L.: "El impacto de las nuevas tecnologías e Internet en los derechos del artículo 18 de la Constitución", *Anuario de la Facultad de Derecho, Universidad de Extremadura*, núm. 17, 1999, págs. 526-528. En este sentido también se pronuncia, CONTRERAS NAVIDAD, S.: La *protección del honor, la intimidad y la propia imagen en Internet,* Aranzadi, Cizur Menor (Navarra), 2012, págs. 16-17.

[7] HERRANZ ORTIZ, A.: *op. cit.,* págs. 124 y 125.

[8] WESTIN, A.: *Privacy and Freedom*, Atheneum, New York, 1967; FROSSINI, V.: *Cibernética diritto e societá*, Edizioni di Comunita, Milano, 1968; PÉREZ LUÑO, A. E.: *Cibernética, Informática y Derecho. Un análisis metodológico*, Publicaciones del Real Colegio de España, Bolonia, 1976; LUCAS MURILLO DE LA CUEVA, P.: *El derecho a la autodeterminación informativa. La protección de los datos personales frente al uso de la informática*, Tecnos, Madrid, 1990.

Hoy por hoy, podemos afirmar que nos encontramos ante un derecho fundamental autónomo, de creación jurisprudencial y señalado por la relevancia de los bienes que ampara. Asimismo, nos hallamos ante un derecho fundamental de configuración legal, si bien atípico, porque la incorporación de España a las Comunidades Europeas y la asunción por parte de estas de la competencia en materia de protección de datos condicionaron la labor del legislador orgánico español a la hora de llevar a cabo la tarea de desarrollar su contenido esencial. La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos -LORTAD-, fue sustituida por la Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal -LOPD- para trasponer la Directiva 95/46/CE sobre la materia.

En la actualidad, esta norma europea ha sido derogada por el Reglamento General de Protección de Datos (UE) 2016/679 -en adelante RGPD-[9]. A pesar de ser el Reglamento un instrumento normativo de aplicación directa, la amplitud de su contenido y la remisión en muchos aspectos al Derecho de los Estados miembros va a obligar al legislador nacional a llevar a cabo un desarrollo que adapte a su contenido gran parte de la regulación vigente.

Por consiguiente, el régimen jurídico del derecho a la protección de datos personales va a estar presidido por dos fuentes normativas de procedencia dispar, aspecto absolutamente novedoso en el marco de los

[9] DOUE núm. 119, de 4 de mayo de 2016.

derechos fundamentales: el reglamento comunitario que empieza a aplicarse el 25 mayo de 2018 y la LOPD, que sigue vigente[10].

Respecto a su ámbito de aplicación, el Reglamento regula solo aquellos sectores que sean competencia del derecho de la Unión Europea –en adelante UE-. Resulta un ámbito muy extenso porque incluye todas las actividades económicas, pero que, al mismo tiempo, deja un amplio margen de desarrollo a los Estados. En este espacio regirá el Reglamento, y también la LOPD, o la norma que en el futuro la sustituya, en lo que sea compatible con aquel. Respecto a los tratamientos de datos sobre las materias que no sean objeto de las competencias de la UE, que quedan excluidas del ámbito de aplicación del Reglamento[11], operará la LOPD, o la norma que previsiblemente la sustituya en el futuro.

La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. Con estas palabras, recogidas en el considerando 6, refleja el citado Reglamento la conciencia europea de la trascendencia del problema: "La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades.

---

[10] Proyecto de Ley Orgánica de Protección de Datos de 24 de noviembre de 2017, BOCG, núm. 13.1. Disponible en Internet: http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A /BOCG-12-A-13-1.PDF

[11] Artículo 2.2 RGPD: "El presente Reglamento no se aplica al tratamiento de datos personales: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas; d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención".

Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales".

Partiendo de estas consideraciones, vamos a profundizar en la construcción del derecho fundamental a la protección de datos como categoría autónoma. Encontramos la primera aproximación al origen de este derecho en el reconocimiento de la dignidad humana como fundamento de los derechos, tanto a nivel nacional como internacional. La Declaración Universal de Derechos Humanos, adoptada y proclamada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948, en su Preámbulo, establece que "la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana". Y, posteriormente, en su artículo I, declara que "todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente". La invocación de la dignidad humana muestra la conciencia del valor alcanzado por el individuo.

Asimismo, nuestra Carta Magna abre el título I, "De los derechos y deberes fundamentales", con la consagración de la dignidad humana como fundamento del orden político y de la paz social. Es en este espacio donde podemos encuadrar el derecho fundamental a la protección de datos. No cabe duda de que este derecho tiene su razón de ser en las potenciales agresiones

a la dignidad humana que suponen las nuevas tecnologías, lo cual contribuye a confirmar su condición de derecho fundamental, dada la excepcional relevancia de los valores personales implicados.

La importancia que nuestra Constitución confiere a los tratados y los acuerdos internacionales ratificados por España para la interpretación de los derechos fundamentales, como se desprende del párrafo segundo del artículo 10 CE, nos permite perfilar aún más el alcance de la cobertura de este derecho fundamental. Como puede constatarse, la Declaración Universal no contiene referencia alguna a la protección de datos personales. Sin embargo, esta exigencia puede ser deducida de otras previsiones más genéricas de la propia Declaración. Así, conforme a su artículo 12, “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”. A la vista de este pronunciamiento, resulta innegable que el derecho a la autodeterminación informativa se construye tomando como fundamento el concepto de vida privada.

Del mismo modo, el otro gran pilar internacional de la interpretación de los derechos fundamentales, el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, de 4 de noviembre de 1950 -en adelante CEDH- consagró la protección de la vida privada en su artículo 8: “1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una

sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."

Este precepto y la interpretación teleológica del mismo a la luz de la realidad social actual llevada a cabo por el Tribunal Europeo de Derechos Humanos –en adelante TEDH- serán los ejes esenciales en la elaboración de la doctrina sobre el derecho fundamental a la protección de datos, que queda inescindiblemente vinculado al respeto a la vida privada y familiar[12]. En este sentido, muchos de los Estados firmantes del CEDH no reconocían expresamente en sus Constituciones un derecho fundamental a la protección de datos, de ahí que la jurisprudencia del Tribunal Europeo de Derechos Humanos[13] haya ejercido una función decisiva: la de mínimo común denominador europeo para su tutela.

En la misma línea, y desde un punto de vista cronológico, el Pacto Internacional de los Derechos Civiles y Políticos, firmado en Nueva York el 19 de diciembre de 1966, seguirá idéntica orientación[14]. Un año después, se crea

---

[12] A partir del caso Leander contra Suecia (STEDH de 26 de marzo de 1987) se plantea ante el Tribunal Europeo de Derechos Humanos que la recogida de datos personales relativos a la vida privada de un individuo por parte de una autoridad pública, su utilización y la negativa a conceder la facultad de refutarlos podía suponer una vulneración del derecho al respeto de la vida privada y familiar del individuo.

[13] En este sentido, el Tribunal Constitucional, al tratar los límites del derecho fundamental a la protección de datos en la STC 292/2000, FJ 9, hizo referencia expresa a las SSTEDH de 26 de marzo de 1987, caso Leander contra Suecia*;* de 25 de febrero de 1997, caso Z contra Finlandia; de 25 de febrero de 1993, caso Funke contra Francia; de 26 de marzo de 1985, caso X e Y contra Países Bajos, y de 7 de julio de 1989, caso Gaskin contra Reino Unido.

[14] Artículo 17: "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques" y también el artículo 11 de la Convención Americana de Derechos Humanos, de 22 de noviembre de 1969.

una comisión consultiva de expertos en el seno del Consejo de Europa. El resultado de su trabajo fue la Resolución 68/509/CE sobre "los derechos humanos y los nuevos logros científicos y técnicos". Este documento deja entrever la necesidad de instituir mecanismos de protección de los derechos de las personas, especialmente de su esfera interna, frente al poder de la informática.

La potencial incidencia de las tecnologías de la información y la comunicación -TIC- en la privacidad de las personas empieza a preocupar a los poderes públicos a lo largo de la primera mitad de la década de los setenta del siglo pasado. Las infinitas posibilidades de actuación que ofrecen tales tecnologías respecto al tratamiento de la información personal ponen sobre aviso a los legisladores, que buscan respuestas jurídicas a la amenaza que representará para los individuos un descontrolado avance en el campo del tratamiento de datos[15]. De este modo, se aprobaron a ambos lados del Atlántico distintas normas para paliar los riesgos derivados de los avances producidos en este campo[16]. Así, se aprobó la Ley de protección de datos *Datenschutz,* de 7 de octubre de 1970, del *Land* de Hesse*,* con el objetivo de asegurar la confidencialidad en el manejo de los datos de los particulares exclusivamente en ficheros públicos. Esta norma crea la figura del Comisario Parlamentario de Protección de Datos, con funciones similares a las de un *Ombudsman*. Por su parte, en los Estados Unidos se promulgó el 31 de diciembre de 1974 la *Privacy Act,* referida también a los ficheros de los organismos públicos, en cuya Exposición de Motivos se afirma: "El Congreso

[15] En este sentido HERRANZ ORTIZ, A. I.: *op. cit*., pág. 75.
[16] *Vid.* FROSSINI, V.: "Bancos de datos tutela de la persona", *REP*, núm. 30, 1982, págs. 27-31.

estima que la privacidad de un individuo es afectada directamente por la captación, conservación, uso y difusión de información personal por entes y órganos federales [...]"[17].

No obstante, la primera ley de carácter nacional que extiende su ámbito de aplicación a la totalidad de los tratamientos de datos de los sectores público y privado será la *Data Lag* sueca de 11 de mayo de 1973, que desarrolla por primera vez los principios que inspirarán la protección de datos (principios de finalidad y adecuación al fin, de seguridad, de secreto profesional, de duración limitada de la conservación de datos, principios de exactitud y actualización) y reconoce derechos básicos en la materia (derecho de información, acceso, rectificación y cancelación)[18]. En el período comprendido entre 1977 y 1979, la República Federal de Alemania, Francia, Dinamarca, Austria y Luxemburgo aprobarán leyes nacionales de protección de datos de carácter personal siguiendo las premisas marcadas por la legislación sueca[19].

Un avance más en esta materia lo representan aquellos Estados donde el derecho a la protección de datos comienza a alcanzar reconocimiento constitucional, para singularizarse frente al derecho a la intimidad. La

---

[17] Resalta Téllez Aguilera que el artículo 2 de esta Ley, después de reconocer la posible injerencia que el uso de la informática puede tener en la vida privada, consagra la protección de la intimidad de los ciudadanos como derecho fundamental de la persona tutelado por la Constitución. Sin embargo, esta importante declaración de principios se ve enturbiada a lo largo del propio texto legal, y mucho más por el propio sistema legislativo norteamericano, que ha propiciado un importante conjunto de leyes sectoriales de protección de datos. *Vid.* TÉLLEZ AGUILERA, A.: *La protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores,* Edisofer, Madrid, 2002, pág. 23.

[18] *Ibidem*, pág. 29

[19] Ley de Protección de Datos de la República Federal Alemana de 27 de Enero de 1977 (*Bundesdatenshutzgesetz)*. Un año más tarde, en 1978, la Ley de Informática, Ficheros y Libertades francesa (Ley 78-17, de 6 de enero). El 8 de junio de 1978 se aprobaron en Dinamarca las leyes número 293, sobre registros privados y 294, sobre registros públicos. La Ley de Protección de Datos de Austria se aprobó el 18 de octubre de 1978. Por último, el 31 de mayo de 1979, se aprobó en Luxemburgo la Ley sobre utilización de datos en tratamientos informáticos. Para todas, v*id.* TÉLLEZ AGUILERA, A: *op. cit.,* págs. 30-35.

Constitución de Portugal de 2 de abril de 1976 contiene una declaración de derechos fundamentales sin precedentes en el constitucionalismo del viejo continente por su extensión y su carácter abierto. Portugal será el primer Estado europeo que reconozca de forma expresa un derecho a la protección datos personales distinto e incluso anterior a la incorporación del derecho a la intimidad al texto de su Norma Suprema[20]. La razón de su constitucionalización separada reside, desde luego, en los cambios sociales y políticos que desembocaron en la revolución de 25 de abril de 1974, y, de manera inmediata, en la suspensión de un proyecto sobre creación de un Registro, que atribuía un número nacional de identificación a todas las personas físicas y jurídicas[21].

En nuestro país, si bien es cierto que el derecho a la protección de datos no estaba previsto abiertamente en nuestro texto constitucional, no cabe duda de que se hallaba presente en el ánimo de los constituyentes la intención de preservar a las personas frente a los peligros del incipiente desarrollo de las TIC. La conciencia de la entidad del problema era una realidad allá por el año 1978, como se deduce del artículo 18.4 de la CE: "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". Señala Lucas Murillo de la Cueva que "sobre este particular existían ya elementos de juicio suficientes para apreciar que de la utilización de la informática podían derivarse riesgos

[20] El derecho a la reserva de la intimidad de la vida privada no se encontraba consagrado en el texto constitucional de 1976, aunque la doctrina lo consideraba derecho fundamental por la conexión que guardaba con algunos derechos constitucionales reconocidos en la Constitución como la integridad personal o el derecho a la inviolabilidad del domicilio y de la correspondencia, y por su carácter de derecho universal e inmanente, ligado a la dignidad de la persona. Por estos motivos, se incluyó en el texto constitucional con la reforma llevada a cabo en 1997 en el artículo 26. *Vid.* ARENAS RAMIRO, M.: El *derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, 2006, págs. 415 y ss.

[21] La Ley 2/73, de 10 de febrero, por la que se creaba un Registro Nacional de Identificación, que iba a desarrollarse por Decreto Ley 555/73, de 26 de octubre.

graves para las personas que requerían establecer de forma expresa el principio de la protección frente a tales peligros, no solo de los reconocidos en el artículo 18.1, sino de todos los derechos que les corresponden"[22].

No obstante, la redacción de la norma española no fue muy afortunada, si la comparamos con otros preceptos, como el artículo 35 de la Constitución portuguesa. Según lo dispuesto en el precepto luso, en su redacción original:

"1. Todos los ciudadanos tienen derecho a conocer los datos que les conciernen que constan en registros mecanográficos y el fin al que son destinados, pudiendo exigir su rectificación y actualización. 2. La informática no puede ser utilizada para el tratamiento de datos relativos a convicciones políticas, creencias religiosas o vida privada, salvo cuando se trate de un procesamiento de datos personales no identificables con fines estadísticos. 3. Está prohibida la atribución de un numero nacional único a los ciudadanos"[23].

---

[22] LUCAS MURILLO DE LA CUEVA, P.: "La Constitución y el derecho a la autodeterminación informativa", *Cuadernos de Derecho Público*, núm. 19-20, 2003, pág. 29.

[23] El artículo 35 de la Constitución Portuguesa ha sido modificado en varias ocasiones. En su redacción actual dispone:"1.Todo ciudadano tendrá derecho de acceso a todos los registros informáticos que le conciernen, a requerir que sean rectificados y actualizados, y a ser informado de la finalidad a que se destinan las informaciones, de conformidad con lo dispuesto en la ley. 2. La ley definirá el concepto de "dato personal", junto con términos y condiciones aplicables a su tratamiento automatizado, vínculos, transmisiones y uso, y garantizará su protección, en particular por medio de un órgano independiente. 3. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones filosóficas o políticas, afiliaciones a partidos o sindicatos, creencias religiosas, vida privada u orígenes étnicos, salvo con el consentimiento expreso del sujeto, con autorización prevista por la ley y garantías de no discriminación, o con el fin de procesar datos estadísticos que no puedan ser individualmente identificados.4. El acceso de terceros a los datos personales estará prohibido, salvo en casos excepcionales, de conformidad con la ley. 5. Se prohíbe atribuir un número nacional único a los ciudadanos. 6. Se garantiza a todos el libre acceso a la red informática de uso público. La ley determinará tanto las reglas aplicables al flujo de datos a través de las fronteras como las medidas apropiadas para proteger datos personales y otros que justificadamente hayan de ser salvaguardados en interés nacional. 7. Los datos personales contenidos en archivos manuales disfrutarán de la misma protección prevista en los apartados precedentes, de conformidad con lo dispuesto en la ley". http://www.congreso.es/consti/otras/europea/flash.html

Las diferencias entre la Constitución portuguesa y la española en esta materia son evidentes. La redacción del precepto de la primera era ya, por entonces, mucho más precisa que la de nuestro articulo 18.4 y, por tanto, eliminaba las ambigüedades que este plantea. Reconocía las facultades de acceso y rectificación de que goza el titular del derecho como manifestación del poder de control sobre sus datos. Hacía referencia al derecho a ser informado sobre la finalidad de tratamiento y a la trascendencia de los datos sensibles, al mismo tiempo que, de manera más coyuntural, ponía de manifiesto algunos de los problemas que planteaba en ese momento el uso de la informática, como la atribución de un número nacional único al ciudadano. Por el contrario, la fórmula de la norma constitucional española es incompleta, ya que solamente hace referencia al enfoque negativo, limitativo y restrictivo del fenómeno[24]. Al propio tiempo, ha planteado muchas dudas acerca de su interpretación. A pesar de sus insuficiencias, el mero hecho de su existencia ya facilitó en nuestro sistema el reconocimiento del estatus de fundamental del derecho a la protección de datos, pero se perdió la oportunidad de reconocerlo expresamente, pues la influencia de la Norma fundamental portuguesa no fue lo suficientemente fuerte.

Si comparamos el artículo 18.4 CE con el mandato dirigido al legislador en el apartado cuarto del artículo 17 CE, según el cual "la ley regulará un procedimiento de *habeas corpus* para producir la inmediata puesta a disposición judicial de toda persona detenida ilegalmente", tenemos que en

[24] Según Pérez Luño, la propia fórmula del apartado cuarto del artículo 18 no es en modo alguno casual, sino que evidencia la postura defensiva adoptada en el debate constitucional, en el que se puso el énfasis en la dimensión negativa de la libertad informática en detrimento de su significación positiva. *Vid*. PÉREZ LUÑO, A. E.: "Informática y Libertad. Comentario al artículo 18.4 de la Constitución Española", *REP,* núm. 24,1981, pág. 46.

esta ocasión el constituyente recoge expresamente una garantía constitucional específica del derecho fundamental a la libertad personal[25]. Su exigua regulación constitucional expresa, al menos, la finalidad del procedimiento, que es poner fin a una detención ilegal, quedando encomendado su desarrollo a lo que disponga la ley. A primera vista, pues, la delegación legislativa del 18.4 CE constituye también un complemento, es decir, una garantía constitucional de los derechos al honor y a la intimidad personal y familiar, al igual que ocurre con el *habeas corpus*. No obstante, resulta conveniente repasar las distintas fases del *iter* constituyente, para comprender mejor el alcance de esta habilitación al legislador.

El Anteproyecto constitucional de 5 de enero de 1978 se hizo eco de la cuestión en el párrafo cuarto del artículo 18 en estos términos: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos"[26]. Tras su publicación, y concluido el plazo de presentación de enmiendas, el informe de la Ponencia se convirtió en el artículo 17.4: "La ley limitará el uso de la informática de manera que quede a salvo el respeto a la intimidad personal y familiar y el honor de los ciudadanos"[27]. En la sesión de 19 de mayo de 1978 se debatieron las enmiendas a este artículo, y, en particular, a su párrafo cuarto, que podemos resumir en dos posturas:

---

[25] STC 288/2000, FJ 1: "sino prioritariamente una cuestión que afecta al derecho a la libertad personal, en cuanto que la suficiencia o razonabilidad de una resolución judicial relativa a la garantía constitucional del procedimiento de *hábeas corpus*, prevista en el artículo 17.4 CE, forma parte de la propia garantía".

[26] B.O.C. de 5 de enero 1978, núm. 44, pág. 672. Disponible en Internet: http://www.congreso.es/public_oficiales/L0/CONG/BOCG/BOC_044.PDF

[27] B.O.C de 17 de abril de 1978, núm. 82, pág. 1533.

-La supresión o limitación de cualquier referencia a la informática o su restricción solo al ámbito de la intimidad, representada por las enmiendas número 2 al artículo 17, de Carro Martínez, del Grupo Parlamentario de Alianza Popular. Según su argumentación, la protección autónoma del derecho al honor, intimidad personal y familiar y propia imagen era una novedad en el derecho constitucional y su garantía se encontraba ya reconocida en el artículo 20.6 CE. Frente a esta afirmación, Peces Barba vino a poner de manifiesto la inexactitud de tal alegato, pues su inclusión independiente en el texto de la Norma Suprema estaba en la línea más adecuada al derecho constitucional contemporáneo, poniendo como ejemplos el Convenio Europeo de Derechos Humanos (art. 8), la Declaración Universal de Derechos del Hombre (art. 2) y el Pacto de Derechos Civiles y Políticos de 1966 (art. 17)[28]. Esta alusión demuestra la conciencia que había en los debates parlamentarios acerca del Derecho Internacional vigente en materia de derechos humanos.

La enmienda número 716, relativa a la informática, formulada por el diputado Sancho Rof, del Grupo Parlamentario de Unión de Centro Democrático, proponía la eliminación del apartado cuarto del artículo 17 por superfluo, pues, según su parecer, simplemente ampliaba lo que decía el apartado primero a un aspecto muy concreto de la técnica, como es la informática. A pesar del contenido de su discurso, con manifestaciones tales como la de que “se corre el peligro en este momento de que la informática se use en ella -en la Constitución- de forma desmesurada para *aportación de*

[28] DS. Congreso de los Diputados, núm. 70, de 19/05/1978, págs. 2518 y 2519, Comisión de Asuntos Constitucionales y libertades públicas.

datos, etc.", (la cursiva es nuestra) su razonamiento no alcanzó a deslindar la dimensión del problema de la garantía de la intimidad.

-Las posturas expansivas, que pretendían extender la protección a todos los derechos constitucionales. En esta línea, la enmienda del Grupo Mixto número 79 de Gastón Sanz, del Partido Socialista de Aragón, pretende dar una explicación más detallada a la cuestión de la informática, al proponer como texto del precepto el siguiente: "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" (la cursiva es nuestra). A mi juicio, este artículo habría sido mucho más certero y particularmente original, e incluso premonitorio, ya que hacía por primera vez referencia a los datos personales, concretamente a la dimensión positiva que faculta al control de los mismos, así como a sus relaciones con las libertades públicas.

Finalmente, esta enmienda fue retirada y unida a efectos de voto a la enmienda 117 de Minoría Catalana. Esta última pretendía incorporar entre los límites de la informática el que garantizara el pleno ejercicio de los derechos por parte de los ciudadanos, y no solamente los derechos al honor y a la intimidad personal y familiar. Interesante es la visión de su autor, Roca Junyent, que advertía de los problemas que la informática estaba ya planteando en países más desarrollados, como Estados Unidos, por las injerencias en la libertad, es decir "cuando un ciudadano, por ejemplo, deseando constituir una asociación o promocionar una reunión o bien practicar una actividad económica, encuentra, que por razón de una información de la que él no es conocedor y respecto de la cual incluso no puede ni pronunciarse en muchas

ocasiones, se limita de tal manera el ejercicio de sus derechos que se ve colocado en una situación de inferioridad y desigualdad frente a los ciudadanos"[29]. Apoyará esta enmienda el representante del Grupo Socialista de Cataluña, Martín Toval, que recalcó la creciente importancia social de una técnica de intromisión cada vez con más incidencia en el ámbito de los derechos individuales y que, por esto, reclamaba cláusulas de garantía frente al Estado acentuando la dimensión defensiva de esta protección, pues "es una técnica que proporciona una capacidad de control creciente sobre las vidas y circunstancias de los individuos y por el contrario -esto hay que reconocerlo a la vista de la práctica existente en el Derecho comparado- es muy difícil que exista una autentica capacidad de control sobre esa creciente capacidad de control que es el uso de la informática en manos del Ejecutivo". Adhiriéndose a esta postura, Solé Tura, representante del Grupo Parlamentario Comunista, apostilló que "se trata de establecer garantías de control de los controladores"[30].

Efectuadas las votaciones, la enmienda de Minoría Catalana fue aprobada por unanimidad y, con ella, el apartado cuarto del artículo 17, que tomaría la numeración de artículo 18.4: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el

[29] *Ibidem*, pág. 2527.
[30] "El 'controlar a los controladores' es tan solo el punto de partida de una protección que pronto se revelaría imprescindible como consecuencia del acceso a la tecnología no solo del sector económico privado, sino también de los particulares", *vid*. GUERRERO PICÓ, M. C.: *El impacto de Internet en el Derecho Fundamental a la protección de datos de carácter personal*, Aranzadi, Cizur Menor (Navarra), 2006, pág. 186.

pleno ejercicio de sus derechos". Redacción definitiva, al no prosperar la alternativa que propuso el voto particular de Zarazaga Burillo en el Senado[31].

A la vista del triunfo de las tesis expansivas, podemos concluir que existía claramente una conciencia acerca de los riesgos de la rápida evolución de la tecnología, y, en particular, de su repercusión sobre el tratamiento de los datos y de la información en los derechos individuales, y no solamente en la intimidad. Esto nos permite inferir que la razón del mandato dirigido al legislador de limitar el uso de la informática iba más allá de la protección del honor y la intimidad a que se refiere el apartado primero del artículo 18. De hecho, esta disposición hace mención expresa a la garantía normativa de otros derechos frente a las nuevas amenazas derivadas del tratamiento automatizado de la información.

Paralelamente, como pusieron de manifiesto los debates parlamentarios, los problemas derivados de la sociedad de la información[32] estaban originando soluciones jurídicas en el Derecho comparado. En la década de los ochenta se van a cimentar los pilares de la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal a nivel internacional. Cronológicamente, es la Organización para la Cooperación y el Desarrollo Económico -OCDE-, en la Recomendación del Consejo relativa a la protección de la privacidad y el flujo transfronterizo de datos de 23 de septiembre de 1980, la primera que toma conciencia de que los países que

[31] DS. Senado núm. 60 de 27 de septiembre de 1978, págs. 2981-2983. Disponible en Internet: http://www.congreso.es/public_oficiales/L0/SEN/DS/S_1978_060.PDF

[32] En su intervención, Martín Toval puso el ejemplo del programa Safari, preparado por el Ministerio del Interior francés. B.O.C. de 19 de mayo de 1978 núm. 70, pág. 2528.

formaban parte de esta organización tenían legislaciones dispares, que dificultaban la seguridad en la circulación internacional de los datos[33].

Por su parte, el Consejo de Europa había aprobado dos Resoluciones en los años 70[34], dirigidas a la protección de datos, pero cuyos principios, por su naturaleza no vinculante para los Estados miembros, no alcanzaron la finalidad pretendida. Esta circunstancia desembocó, años más tarde, en la firma, el 28 de enero de 1981, del Convenio 108, sobre la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. Este texto representa la piedra angular de la tutela del derecho fundamental a la protección de datos, que ya sí resultaba de obligado cumplimiento para los Estados que lo suscribieron. Ratificado por España el 27 de enero de 1984[35], el Convenio no tiene aplicación directa, pero, pese a ello, la jurisprudencia constitucional le ha atribuido valor de instrumento integrador del derecho a la protección de datos[36]. Su artículo primero define el objeto y fin de este documento: "… 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

---

[33] *Vid*, sobre las directrices contenidas en la Recomendación del Consejo de la OCDE de 23 de septiembre de 1980, PUENTE ESCOBAR, A.: "Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal", en PIÑAR MAÑAS, J. L.: *Protección de datos de carácter personal en Iberoamérica*, Tirant lo Blanch, Valencia, 2005, págs. 51-54*. Vid.* DAVARA RODRÍGUEZ, M. A.: *La protección de datos en Europa: principios, derechos y procedimiento*, Universidad Pontificia de Comillas, Madrid, 1998, pág. 32, Sobre esta Recomendación y sobre la Recomendación de la OCDE de 26 de noviembre de 1992, relativa a la seguridad en los sistemas de información, *vid.* TÉLLEZ AGUILERA, A.: *op. cit*., págs. 37-39.

[34] Resolución 73/22, de 26 de septiembre de 1973, sobre la protección de la intimidad frente a los bancos electrónicos de datos en el sector privado, y Resolución 74/29, de 20 de septiembre de 1974, sobre protección de la intimidad frente a los bancos electrónicos de datos en el sector público. Sobre los principios, *vid.* DAVARA RODRÍGUEZ, M. A.: *La protección de datos en Europa*…, págs. 30-31.

[35] BOE núm. 274 de 15 de noviembre de 1985

[36] SSTC 254/1993, 143/1994, 94/1998, 144/1999, 202/1999 y 292/2000.

privada, con respecto al tratamiento automatizado de datos de carácter personal correspondientes a dicha persona". No se utiliza la expresión intimidad, sino que se trata de proteger un valor distinto, más amplio, la vida privada, que rebasa aquel contenido y lo engloba[37].

A pesar de lo expuesto, conviene recordar que el derecho fundamental a la protección de datos no siempre encontró su justificación en la protección a la intimidad o la vida privada. En Alemania, la Ley Fundamental no reconoce expresamente un derecho a la vida privada o a la intimidad. El derecho a la autodeterminación informativa, como lo denomina el Tribunal Constitucional alemán, es un concepto de elaboración jurisprudencial a la luz del derecho al libre desarrollo de la personalidad[38]. De acuerdo con el artículo 2.1 del texto constitucional: "Todos tienen derecho al libre desarrollo de su personalidad, en tanto en cuanto no lesionen los derechos ajenos y no contravengan el orden constitucional establecido o las buenas costumbres". Este es un derecho fundamental de libertad que garantiza todos los ámbitos del individuo necesarios para el desarrollo de su personalidad. Se compone de dos elementos, uno activo y otro pasivo: la libertad general de acción y un derecho general de la personalidad. La primera permite al titular del derecho un hacer o

[37] El Convenio 108 es el primer instrumento internacional que procura disponer una normativa armonizadora para hacer frente al fenómeno del tratamiento automatizado de datos correspondientes a personas naturales con el fin de establecer unas reglas que informaran las diversas legislaciones europeas. En este sentido, los Estados Parte del Convenio se obligaban a adoptar en su derecho interno las medidas necesarias para llevar a efecto la protección de datos. Sobre el Convenio 108 hay mucha bibliografía. Sin ánimo exhaustivo: CONDE ORTIZ, C.: *El derecho a la protección de datos personales: un derecho autónomo sobre la base de los conceptos de intimidad y privacidad*, Dykinson, Madrid, 2005, pág. 50; LUCAS MURILLO DE LA CUEVA, P.: *El derecho a la autodeterminación*…, págs. 140-145; TÉLLEZ AGUILERA, A.: *op. cit.,* págs. 39-47.

[38] En contra DENNINGER que considera que el derecho a la autodeterminación informativa no es un invento del Tribunal Constitucional alemán. *Vid*. DENNINGER, E, "El derecho a la autodeterminación informativa" en PÉREZ LUÑO, A. E.: *Problemas actuales de la documentación y la informática jurídica*, Tecnos, Madrid, 1987, pág. 271.

no hacer general. El derecho general de la personalidad se conecta con la dignidad humana, reconocida como valor fundamental por el artículo 1.1 de la Ley Fundamental de Bonn, al establecer que "la dignidad humana es intangible. Respetarla y protegerla es obligación de todo poder público"[39].

A partir del caso *Elfes,* de 16 de enero de 1957[40], en el que el Tribunal Constitucional alemán se refirió a la libertad de acción del ser humano en sentido amplio, aquel resolverá después varios supuestos en los que a propósito de este derecho al libre desarrollo de la personalidad reconocerá, primero, una esfera privada del sujeto[41] y, después, un derecho a la autodeterminación informativa, que alcanzaría su reconocimiento definitivo en la sentencia sobre la Ley del Censo de población, de 15 de diciembre de 1983. Por tanto, en Alemania, habrá que esperar hasta la década de los 80 para poder considerar a la protección de datos como un derecho fundamental autónomo, en la forma de derecho a la autodeterminación informativa.

El Tribunal Constitucional de la República Federal Alemana definió las características del derecho que nos ocupa, resolviendo una autocuestión de inconstitucionalidad acerca de la Ley Federal del Censo de población, aprobada por el *Bundestag* el 4 de marzo de 1982. La elaboración del censo preveía la revelación de una amplia cantidad de datos personales, lo que planteaba dudas sobre su conformidad con los artículos 1, 2, 5 y 19 de la Ley Fundamental de Bonn, a saber, el derecho al libre desarrollo de la personalidad

---

[39] Vid. ARENAS RAMIRO, M.: *op. cit.*, págs. 383 y siguientes. *Vid.* también PÉREZ LUÑO, A, E.: *Nuevas tecnologías, sociedad y derecho: el impacto de socio-jurídico de las nuevas tecnologías de la información*, Fundesco, Madrid, 1987, págs. 126-129.
[40] BVerfGE 6,32 [Wilhelm Elfes] http://www.kas.de/wf/doc/kas_16817-544-4-30.pdf
[41] BVerfGE 27,1 [Microcenso] de 16 de julio de 1969.

y la dignidad humana, la libertad de expresión y las garantías procesales[42]. El Alto Tribunal reconoció que el fundamento del derecho a la autodeterminación informativa era el derecho al libre desarrollo de la personalidad, garantizado por la Ley Fundamental, concretamente, en el artículo 2.1, en conexión con su artículo 1.1, relativo a la dignidad humana. Según su argumentación, las posibilidades de interferir en la vida de los individuos se han ampliado en una forma hasta ahora desconocida con el procesamiento automático de datos. De esta manera, se puede generar una imagen más o menos completa de la personalidad, sin que el implicado pueda controlar suficientemente su exactitud y la utilización de la misma. Un orden legal en el que los ciudadanos no puedan conocer quiénes, cuándo y en qué circunstancias saben qué sobre ellos sería incompatible con el derecho a la autodeterminación de la información. Esto no solo iría en detrimento de la posibilidad de desarrollo individual, sino también de la sociedad, porque la autodeterminación es una condición elemental de una nación democrática libre. El libre desarrollo de la personalidad presupone en el moderno procesamiento de datos la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales. Por tanto, lo relevante en materia de protección de datos no es la naturaleza íntima o no de los datos personales cuyo registro se pretende, sino que lo decisivo será la utilización y la finalidad o el propósito para el que los mismos

[42] HEREDERO HIGUERAS, M.: "La sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de Población de 1983", *DA,* núm. 198, 1983, pág. 142. Disponible en. Internet :https://revistasonline.inap.es/index.php?journal=DA&page=article&op=view&path%5B%5D=4687

se solicitan, así como los procedimientos de interrelación entre categorías de datos personales[43].

Paralelamente, nuestro Tribunal Constitucional tuvo ocasión de pronunciarse por primera vez sobre el problema de determinar en qué medida afectaban al ámbito de la intimidad constitucionalmente protegida los datos relativos a la situación económica de una persona en el recurso de amparo resuelto por la STC 110/1984, de 26 de noviembre. Sin embargo, a diferencia del Alto Tribunal alemán, no abordó la cuestión controvertida, para centrarse en los límites de los derechos fundamentales. Casi una década más tarde, en el recurso de inconstitucionalidad contra la Ley 2/1991, de 7 de enero, sobre derechos de información de los representantes de los trabajadores en materia de contratación, la STC 142/1993 recuerda cómo en aquella resolución se advirtieron ya los riesgos de la posibilidad de que "en una sociedad tecnológicamente avanzada, a través del estudio sistemático de las actuaciones económicas de un determinado sujeto, pueda llegarse a reconstruir no ya su situación patrimonial sino el desarrollo de su vida íntima en el sentido constitucional del término" (FJ 8).

Sin embargo, habrá que esperar al cambio de milenio para que el mandato dirigido al legislador destinado a limitar los abusos del empleo de las nuevas tecnologías sirva al máximo intérprete de nuestra Carta Magna para encontrar en el artículo 18.4, de manera implícita, un derecho o libertad fundamental en sí mismo, que se ha venido a llamar libertad informática, derecho de autodeterminación informativa o derecho a la protección de datos

[43] HERRANZ ORTIZ, A.: *op. cit.,* pág. 86.

(*habeas data*)[44]. Esta "declaración de independencia", que se apunta en las SSTC 254/1993, 11/1998 y 94/1998, es claramente visible en la STC 292/2000[45]. Si la institución del *habeas corpus* surgió en el Derecho anglosajón como garantía de la libertad personal y de la integridad física, la doctrina habla de un *habeas data* como un conjunto de instrumentos procesales (acceso, rectificación y cancelación) que garantizan que la persona dispone de sus datos personales, y, por tanto, una protección sobre su identidad personal[46]. En este supuesto, se produce un salto cualitativo, pues del carácter instrumental del derecho a la intimidad, la exégesis del precepto lleva al Tribunal Constitucional a delimitar un derecho fundamental de dimensión positiva, que faculta a su titular para poder controlar sus datos personales. Aludir a un tránsito desde el *habeas corpus* al *habeas data* representa aceptar, de forma implícita, que existe una evolución de los derechos y libertades o, si se prefiere,

[44] Entre las Constituciones que reconocen explícitamente el *habeas data* podemos citar sin ánimo exhaustivo, Argentina, artículo 43; Brasil, arts. 5, 71 y 76; Colombia, artículo 15; Ecuador, artículo 66.19; Nicaragua, artículo. 26; México, artículo. 2; Paraguay, artículo 135; República Dominicana, artículo 44. 2; Venezuela, artículo 28; y Angola, artículo 69. En otras Constituciones, tal derecho se deduce del respeto a la vida privada, así en las de Andorra, artículo 14; Chile, artículo. 19; Bolivia, artículo 21; y Rusia, artículo. 24. *Vid*. AA.VV.: *Protección de datos y habeas data: una visión desde Iberoamérica,* AEPD, 2015, Disponible en Internet: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones /common /premios_2015/Proteccion_de_datos_y_habeas_data.pdf. Y Congreso de los Diputados, Portal Constitución, Constituciones del mundo. Disponible en Internet: http://www.congreso.es/consti/otras/mundo/index.htm. *Vid.* FROSINI, T. E.: "Nuevas tecnologías y constitucionalismo", *REP*, núm. 124, 2004, págs. 134-136.

[45] En este sentido, CIDONCHA MARTÍN, A.: "Garantía institucional, dimensión institucional y derecho fundamental: balance jurisprudencial", *Teoría y Realidad Constitucional*, núm. 23, 2009, pág. 155.

[46] A propósito de la doctrina italiana que ha analizado el "diritto alla riservatezza" como un componente de la libertad personal, *vid*. TRONCOSO REIGADA, A.: *La protección de datos personales en busca del equilibrio*, Tirant lo Blanch, Valencia, 2010, pág. 52.

que estamos asistiendo a un proceso evolutivo de generaciones de derechos humanos[47].

Por consiguiente, el derecho fundamental a la protección de datos, como derecho autónomo, encontró su primera afirmación en la jurisprudencia del Tribunal Constitucional español, especialmente, a partir de la sentencia 254/1993, y se asentó definitivamente en las sentencias 290 y 292/2000. Estas sentencias supusieron el reconocimiento y la protección de un derecho fundamental nuevo, un derecho autónomo no previsto explícitamente por el texto constitucional.

En nuestra opinión, la jurisprudencia constitucional española es el resultado de la trascendencia que la cláusula del artículo 10.2 CE tiene en materia de la interpretación de los derechos fundamentales. La apertura al Derecho Internacional en materia de protección de datos, y, más concretamente, al citado Convenio 108, condujo a la conveniencia de reconocer un derecho fundamental nuevo. La STC 254/1993 representa el primer pronunciamiento del Tribunal constitucional en este sentido. En el recurso de amparo interpuesto contra la denegación del acceso a un fichero público que contenía datos personales del demandante, la resolución fue favorable al otorgamiento del amparo.

En el caso resuelto por la sentencia citada, la solicitud al Gobernador Civil de Guipúzcoa de información sobre los datos personales del interesado se

[47] PÉREZ LUÑO, A. E.: "Intimidad y protección de datos personales: del Habeas Corpus al Habeas Data" en GARCÍA SAN MIGUEL, L. (ed.): *Estudios sobre el Derecho a la intimidad*, Tecnos, Madrid, 1992, pág. 36.

fundó originalmente en el artículo 8, apartados a) y b) del citado Convenio[48]. La cuestión suscitada, en primer término, era la de si este instrumento podía ser invocado directamente. La inexistencia de desarrollo legislativo del apartado 4 del artículo 18 planteaba el problema de la aplicabilidad y fuerza vinculante del mismo. En referencia a esto, la jurisdicción ordinaria consideró que el Convenio no era de aplicación directa, sino que era preciso el complemento de la actividad legislativa y reglamentaria interna. Para el Tribunal Constitucional, el nudo gordiano del recurso consistía en determinar si el artículo 8 del Convenio surtía efecto directo, o, en su caso, interpretativo, en relación con los derechos fundamentales que enuncia el artículo 18 de la Constitución (FJ 4). La primera solución no habría de satisfacer al Tribunal Constitucional, lo cual le llevó a rechazar la alegación fundada en el artículo 96.1 de la Constitución para defender que el efecto vinculante que este precepto atribuye a los Tratados Internacionales permite hacer valer los derechos recogidos en el artículo 8 del Convenio.

En segundo lugar, se discutió si, al menos, el Convenio de Europeo de Derechos Humanos constituiría una fuente de valor interpretativo por imperativo del artículo 10.2 del texto constitucional. En palabras del Tribunal Constitucional, en virtud de este precepto, los textos internacionales ratificados por España pueden servir para configurar el sentido y el alcance de los

[48] Artículo 8: "Cualquier persona deberá poder: a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero; b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible." Disponible en https://www.agpd.es/portalwebAGPD/internacional/textosynormas/textos_consejo_europa/common/PDFs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf

derechos recogidos en la Constitución. De hecho, la sentencia propició el debate sobre si este instrumento internacional podía ser utilizado por el Alto Tribunal como un elemento de integración, ante la demora del desarrollo legislativo del precepto constitucional[49]. Lo cierto es que, debido a esta labor, el Tribunal concluyó que el contenido esencial del derecho a la intimidad integra el derecho de los ciudadanos a conocer los datos que constan sobre ellos en los archivos automatizados de las Administraciones públicas.

A partir de aquí, la sentencia plantea el problema de cuál debería ser ese contenido mínimo, provisional, en relación con este derecho o libertad que el ciudadano debe encontrar garantizado, aun en ausencia de desarrollo legislativo. En este sentido, para el Tribunal Constitucional, las pautas interpretativas que nacen del Convenio de protección de datos personales de 1981 conducen a la conclusión de que la garantía de la intimidad adopta un contenido positivo, en forma de derecho de control sobre los datos relativos a la propia persona.

Las consecuencias de este pronunciamiento serán trascendentales. En efecto, es la primera vez que se concibe en el seno del artículo 18.4 CE un nuevo derecho fundamental, de configuración legal. Así, en el fundamento jurídico sexto de su sentencia, el Tribunal Constitucional afirma: "De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva amenaza concreta a la dignidad y a los

---

[49] Voto particular del magistrado Rodríguez-Piñero y Bravo Ferrer. *Vid*. nota al pie 27, en TRONCOSO REIGADA, A.: *op cit.,* pág. 57. Y nota al pie 18, en LUCAS MURILLO DE LA CUEVA, P.; "La construcción del derecho a la autodeterminación informativa", *REP,* núm. 104, 1999, pág. 43. Sobre esto, cfr. DEL CASTILLO VÁZQUEZ, I. C.: *La protección de datos cuestiones constitucionales y administrativas* Aranzadi, Cizur Menor, 2007, págs. 128-129.

derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero *también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a la 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'"* (la cursiva es nuestra).

Por tanto, el derecho identificado por el Tribunal Constitucional se concreta en la facultad de vigilar el tratamiento informático de los datos personales. El control de la información no reside únicamente en la decisión respecto a su divulgación a terceros, sino que se amplía a la vigilancia en torno a la utilización posterior de los datos personales, una vez que han sido facilitados. Se reconoce que no todo tratamiento informatizado de la información es lícito, pese a que su titular la haya expuesto al general conocimiento. Esto es, la facultad de control sobre los datos personales no concluye en el momento en que el individuo se desprende de los datos personales, sino que integra su contenido el derecho a "perseguir" los datos, a conocer el camino que seguirán, para vigilar la utilización correcta y lícita de los mismos, en relación con los fines para los que se obtuvieron[50].

Y el hecho de que, hasta el momento, no se hubiera llevado a efecto su desarrollo legislativo no obstaba -como se expone en el fundamento jurídico sexto de la STC 254/1993- para que el citado derecho no tuviera la virtualidad

[50] HERRANZ ORTIZ, A.: *op. cit.,* págs. 91 y 92.

de amparar por sí mismo pretensiones individuales, ya que los derechos y libertades fundamentales son origen inmediato de derechos y obligaciones y no meros principios programáticos. Por tanto podía afirmarse que el derecho disponía de un contenido mínimo, que debía ser protegido por todos los poderes públicos, y también por el Tribunal Constitucional a través del recurso de amparo, en aplicación del artículo 53 CE. La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*).

Ciertamente, la sentencia no resulta clarificadora. A veces, en su argumentación, la libertad informática y el derecho a la intimidad parecen distintos, mientras que en otras ocasiones resultan equivalentes. Finalmente, el Tribunal no termina por perfilar ese nuevo derecho fundamental y, en su lugar, prefiere optar por su carácter instrumental, es decir, por considerar al artículo 18.4 como una garantía del derecho fundamental a la intimidad en el ámbito de la informática.

Ahora bien, el haber consagrado la eficacia directa de este derecho fundamental, a partir de la propia Constitución, a pesar de que en el momento de la interposición del recurso no se había llevado a cabo su desarrollo legislativo, supuso un avance fundamental en la consolidación de la protección de datos como derecho autónomo. El paso definitivo se dará cuando el Tribunal Constitucional aborde ya con total decisión la cuestión de la configuración constitucional del derecho fundamental a la protección de datos, lo que llevará a cabo a través de dos recursos de inconstitucionalidad en los que confirmará su naturaleza jurídica autónoma, pese a su relación instrumental con el derecho a la intimidad.

En el primero de ellos, interpuesto entre otros por la Generalidad y el Parlamento de Cataluña, el control de constitucionalidad tenía por objeto determinados preceptos de la LORTAD. En la STC 290/2000, el Alto Tribunal se pronunció sobre las funciones y potestades que esta ley atribuía a la Agencia de Protección de Datos y al Registro General, a pesar de la pérdida sobrevenida de objeto del recurso por tratarse de una norma ya derogada. En tal sentido, la sentencia ratificó la constitucionalidad de las competencias de la Agencia en todo el territorio nacional respecto a ficheros de datos de titularidad privada, en cuanto órgano garante del derecho fundamental a la protección de datos y de la igualdad de todos los españoles en su disfrute, sobre la base del artículo 149.1.1 CE. Sin embargo, el asunto más relevante de esta resolución desde el punto de vista constitucional fue que el Tribunal Constitucional reconoció la existencia del derecho a la protección de datos personales a partir del artículo 18.4 CE[51].

Esta actividad del Tribunal Constitucional, en el sentido de extender la tutela de los derechos fundamentales a parcelas de la realidad no expresamente consideradas por la Constitución, fue muy conveniente y tuvo especial relevancia en el caso que nos ocupa para adecuarla a los riesgos derivados de las nuevas tecnologías. Pero, de otra parte, no estuvo exenta de polémica, como puso de manifiesto el voto particular del magistrado Jiménez

[51] STC 290/2000, FJ 7: "…el derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos."

de Parga[52]. Este magistrado puso de relieve que la Constitución no contiene una cláusula abierta como remate de la lista de derechos fundamentales, a diferencia de otros textos constitucionales, como los de Portugal, Argentina o Estados Unidos. Consagrar *ex novo* derechos no recogidos por la Constitución podría exceder de las funciones del Tribunal Constitucional, en tanto no encuentren más acomodo en la Carta Magna que el genérico de la protección de la dignidad humana (art. 10 CE)[53]. Supondría una tarea reservada, en principio, al poder de reforma constitucional, puesto que el Alto Tribunal podría estar legitimado para interpretar los enunciados constitucionales, pero no para innovar la propia Constitución.

En este punto, señala Lucas Murillo de la Cueva que "es preciso advertir que la posición del juez constitucional a la hora de pronunciarse sobre la existencia de nuevas formas de derechos fundamentales no es la misma que la del constituyente. Este puede ensanchar los contenidos materiales del ordenamiento, ya que ejerce poderes originarios. Aquel solamente dispone de poderes derivados, constituidos, lo que le obliga a moverse en el marco de

---

[52] Frente a la opinión de la mayoría, el voto particular del magistrado Jiménez de Parga propuso que la libertad informática debía tener como sustento el artículo 10.1 CE, ya que es un derecho inherente a la dignidad humana, además de otros preceptos que facilitarían su configuración como derecho, como el párrafo primero del artículo 18 CE (derecho al honor, a la intimidad personal y familiar y a la propia imagen) y el artículo 20.1 CE (libertad de expresión y de información), así como los Tratados y Acuerdos Internacionales, en cuanto guías de la interpretación, conforme al artículo 10.2 CE. En este sentido, nuestro Alto Tribunal ha afirmado en otras ocasiones que nuestra Constitución ha elevado a valor jurídico fundamental la dignidad de la persona, que, sin perjuicio de los derechos que le son inherentes, se halla íntimamente vinculada con el libre desarrollo de la personalidad (art. 10) y los derechos a la integridad física y moral (art. 15), a la libertad de ideológica y religiosa (art. 16), al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1). Del sentido de estos preceptos puede deducirse que la dignidad "es un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respecto por parte de los demás" (STC 53/1985, FJ 8).

[53] ALGUACIL GONZÁLEZ-AURIOLES, J.: "La libertad informática: aspectos sustantivos y competenciales (SSTC 290 y 292/2000)", *Teoría y Realidad Constitucional*, núm. 7, 2001, pág. 370.

valores fijados por el artífice de la Constitución. Y, aunque el margen de maniobra del que disfruta es muy amplio, no en vano lo que distingue a las normas constitucionales es su indeterminación y elasticidad, y a pesar de que en último término, la Constitución es lo que el Tribunal Constitucional dice que es, su cometido debe desempeñarlo dentro de aquel ámbito para no desnaturalizar todo el conjunto. Esto significa que no cabe hablar, en general, de la creación de derechos fundamentales por la jurisprudencia, sino más bien de su descubrimiento, de su invención- en el sentido de la *inventio romana*- o hallazgo en el ordenamiento jurídico… Esto es lo que ha sucedido en el asunto que nos ocupa"[54].

Por consiguiente si bien es cierto, como afirma Pérez Luño, que la inclusión de la libertad informática en el catálogo de los derechos fundamentales representa en la actualidad una necesidad frente al progresivo avance informático[55], no lo es menos que los derechos fundamentales deben encontrar su fundamento en algún precepto constitucional, más allá de la conexión con la dignidad humana que tienen los bienes personales objeto de su protección. El Tribunal Constitucional está legitimado para interpretar los enunciados constitucionales, como ha ocurrido con el artículo 18.4 CE, pero no

[54] LUCAS MURILLO DE LA CUEVA, P.: "La Constitución y el derecho…", pág. 40. Por su parte, JIMÉNEZ CAMPO, J.: *Derechos fundamentales; concepto y garantías,* Trotta, Madrid,1999, pág. 72, señala que "quien interpreta no solo reproduce; también 'produce', al captar los intereses y exigencias del presente, la realidad que la tradición ha modelado, pues el lenguaje, también en el Derecho, vincula al intérprete solo en el marco de su significado vivo y actual". Y señala algunos ejemplos en que la labor interpretativa del TC ha dado lugar al reconocimiento e identificación de determinados derechos que sin estar contemplados explícitamente en la Constitución se hallan conectados con alguno de los derechos fundamentales a los que se refiere el artículo 53.2 CE.

[55] PÉREZ LUÑO, A. E.: "Nuevos derechos fundamentales de la era tecnológica: la libertad informática" *ADPEP*, núm. 2, 1989/90, pág. 194

para crear derechos fundamentales nuevos, por muy conveniente que fuera la necesidad de extender la tutela del Derecho a los cambios tecnológicos.

La segunda resolución, la STC 292/2000, representa la definitiva emancipación del derecho fundamental a la protección de datos personales respecto del derecho a la intimidad. En dicha sentencia, el intérprete supremo de la Carta Magna resuelve el recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra ciertos artículos de la LOPD. En esta ocasión, el Tribunal viene a afirmar que los derechos de información, acceso, rectificación, cancelación y oposición forman parte del derecho fundamental a la protección de datos personales, definiendo así su contenido.

A la vista de esta doctrina constitucional, el derecho a la protección de datos personales puede concebirse como "el poder de disposición y de control sobre los mismos que faculta a su titular 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"[56].

Una vez alcanzado su reconocimiento definitivo por la jurisprudencia constitucional española, el vertiginoso avance de la sociedad de la información demandaba un sistema jurídico uniforme de protección de los datos de carácter personal frente a las TIC. Esta necesidad se había hecho sentir a nivel mundial en la Resolución de Naciones Unidas relativa a los principios rectores sobre la reglamentación de los ficheros computerizados de datos personales allá por los

[56] STC 292/2000, FJ 7.

años noventa[57]. Sin embargo será la labor de la Unión Europea la que impulse el proceso de consagración del derecho a la protección de datos como derecho autónomo. De hecho, hoy en día, conforme al artículo 6.1 del Tratado del Unión Europea, "la Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados. Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados. Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones."[58] La Carta supone, en efecto, la incorporación al derecho comunitario de un catálogo propio de derechos y libertades, una especie de *Bill of Rights* que se hace visible frente a la acción de aquellos que operan en el ámbito de dicho ordenamiento jurídico[59].

[57] El 14 de diciembre de 1990 se aprueba la Resolución 45/95 de la Asamblea de Naciones Unidas, bajo el título "Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales", que contiene una lista básica de principios en materia de protección de datos. Sin embargo, este documento no deja de ser aún, únicamente un instrumento orientativo de la actividad de los Estados que integran esta organización. *Vid*. PUENTE ESCOBAR, A.: *op. cit.*, págs. 51-54. También, en TÉLLEZ AGUILERA, A.: *op. cit.*, págs. 48-51.

[58] DOUE C 306 de 17 de diciembre de 2007.

[59] CARRILLO, M.: "Los derechos fundamentales en la Constitución europea" en VIDAL-BENEYTO, J. (coord.): *El reto constitucional de Europa,* Madrid, Dykinson, 2005, págs. 201 y 202.

La proclamación en la Carta de Derechos Fundamentales de la Unión Europea -en adelante CDFUE-[60] del derecho fundamental a la protección de datos personales en su artículo 8, como derecho diferente del respeto de la vida privada y familiar[61], es, por tanto, jurídicamente vinculante para las instituciones y órganos de la Unión, así como para los Estados miembros cuando aplican el Derecho de la Unión[62]. Esto es coherente con el principio de atribución de competencias.

El Tribunal de Justicia de la Unión Europea -en adelante TJUE- será, así, competente para controlar la compatibilidad de los actos nacionales llevados a cabo en aplicación del Derecho de la Unión con la protección de los derechos contenidos en la CDFUE. El informe explicativo[63] sobre la Carta se remite a la jurisprudencia del TJUE para aclarar cuándo los Estados miembros aplican el derecho de la Unión. De esta manera, el Tribunal de Justicia ha

---

[60] La CDFUE fue proclamada por la Comisión, el Parlamento y el Consejo en la reunión del Consejo Europeo de Niza de diciembre de 2000. *Vid.* RODRÍGUEZ RUIZ, B.: "La Carta de Derechos Fundamentales de la Unión Europea: acuerdos y desacuerdos" en LEÑERO BOHÓRQUEZ, R. (coord.): *Una Constitución para la ciudadanía de Europa,* Aranzadi, Cizur Menor (Navarra), 2004, págs. 179-193. El Tratado de Lisboa, firmado el 13 de diciembre de 2007, ante todo, confirmó la competencia de la UE en esta materia. En su artículo 16 proclama que "toda persona tiene derecho a la protección de datos de carácter personal que le conciernan. El Parlamento Europeo y el Consejo establecerán las normas sobre protección de las personas físicas respecto al tratamiento de los 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".

[61] El articulo 8 CDFUE dice: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le 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 le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente". El artículo 7 CDFUE dispone: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".

[62] Artículo 51.1 CDFUE. Según el informe explicativo, esta norma se aplica tanto a las autoridades centrales como a las instancias regionales o locales así como a los organismos públicos cuando aplican el Derecho de la Unión.

[63] DOUE C-303/32 de 14 de diciembre de 2007. Disponible en Internet: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:ES:PDF

declarado "que las exigencias derivadas de la protección de los derechos fundamentales en el ordenamiento jurídico comunitario vinculan, asimismo, a los Estados miembros cuando aplican la normativa comunitaria…" (sentencia de 13 de abril de 2000, asunto C-292/97, Karlsson y otros**,** apartado 37)[64].

Cuando los Estados se acogen a una excepción prevista en los Tratados o en el Derecho derivado, el Tribunal de Justicia también será competente para examinar si el acto verdaderamente cabe en el ámbito de la excepción[65]. Incluso, acerca de esta jurisprudencia sobre el ámbito de aplicación de la Carta, la sentencia del Tribunal de Justicia de la Unión Europea -en adelante STJUE- Akerberg Fransson[66] ha declarado que si una norma estatal, que no haya sido aprobada para adaptar el Derecho nacional al Derecho de la Unión, da cumplimiento mediante su aplicación a una obligación impuesta por el Tratado de Funcionamiento de la Unión Europea a los Estados miembros, -en el caso resuelto por la sentencia la de sancionar de modo efectivo los actos que causen un perjuicio a los intereses financieros de la Unión- el asunto pasa a incluirse en el ámbito de aplicación del Derecho europeo.

---

[64] Y anteriormente las sentencias del Tribunal de Justicia de la Unión Europea de 13 de julio de 1989, asunto C-5/88 – Wachauf*;* de 18 de junio de 1991, asunto C-260/89 - ERT/DEP*,* y de 18 de diciembre de 1997, asunto C-309/96 - Annibaldi. *Vid.* MANGAS MARTÍN, A.: "Comentario al artículo 51" en MANGAS MARTÍN, A. (dir.): *Carta de los Derechos fundamentales de la Unión Europea, comentario artículo por artículo*, FBBVA, Bilbao, 2008, pág. 817.

[65] *Idem*, STJUE de 11 de enero de 2000, asunto C-285/98 Kreil. Según FERNÁNDEZ TOMÁS también cabría invocar la Carta cuando los Estados miembros actúen en un ámbito de aplicación cubierto por el Derecho de la Unión, aun cuando ello no dé lugar a un acto legislativo o reglamentario. FERNÁNDEZ TOMÁS, A. F.: "La Carta de Derechos Fundamentales de la Unión Europea tras el Tratado de Lisboa. Limitaciones a su eficacia y alcance generadas por el Protocolo para la aplicación de la Carta al Reino Unido y Polonia" en MARTÍN Y PÉREZ DE NANCLARES, J. (coord.): *El Tratado de Lisboa. La salida de la crisis constitucional.* Madrid, Iustel, 2008, pág. 146.

[66] STJUE de 26 de febrero de 2013, asunto C-617/10, asunto Akerberg Fransson.

Por tanto, la cuestión sobre el ámbito de aplicación de la Carta es sumamente casuística[67]. El articulo 51.1 CDFUE plantea muchos interrogantes. En principio la Carta no sería de aplicación respecto de aquellas actuaciones puramente estatales, realizadas en el ejercicio de la soberanía nacional. Es decir, aquellos actos que los Estados, las Comunidades Autónomas, etc., adoptan en el ejercicio de sus competencias que no se hayan cedido a la Unión Europea. Ahora bien, tales actos, en todo caso, deberán respetar los derechos fundamentales que se contienen en sus Constituciones nacionales y en los Tratados Internacionales de los que sean parte, y lo cierto es que la invocación de los derechos fundamentales de la Carta tanto por los justiciables como por los jueces y tribunales nacionales, incluido el Tribunal Constitucional, ha sido una constante incluso antes de su adopción en los más variados asuntos[68].

Esto supone la existencia de tres parámetros para la defensa del derecho fundamental a la protección de datos: la Constitución Española, el Convenio Europeo de Derechos Humanos y la Carta de los Derechos Fundamentales de la Unión Europea[69]. Será la jurisprudencia emanada de los Tribunales encargados de su tutela la que venga a delimitar de manera

---

[67] *Vid.* STJUE de 6 de octubre de 2015, asunto C-650/13 - Delvigne y las conclusiones del abogado general Cruz Villalón.

[68] CARMONA RUANO, M.: "Aplicación de la Carta de Derechos Fundamentales en la Unión Europea por la jurisprudencia española", seminario sobre la aplicación jurisprudencial de la carta de derechos fundamentales en la unión europea. Sevilla, 3 de noviembre de 2006, Disponible en Internet: http://www.juecesdemocracia.es/fundacion/ponenciassevilla/Aplicaci%F3ndelaCartaMiguelCarmona.pdf

[69] Los concretos problemas de articulación se solucionarán "…ponderando para cada concreto derecho y en sus específicas circunstancias las fórmulas de articulación y definición más pertinentes, en diálogo constante con las instancias jurisdiccionales autorizadas, en su caso, para la interpretación auténtica de los convenios internacionales que contienen enunciados de derechos coincidentes con los proclamados por la Constitución española." Declaración del Tribunal Constitucional 1/2004, de 13 de diciembre.

concluyente, en sus respectivos ámbitos, el contenido esencial del derecho fundamental a la protección de datos.

2. LA RELACIÓN DE LOS DERECHOS FUNDAMENTALES A LA PROTECCIÓN DE DATOS Y A LA INTIMIDAD PERSONAL Y FAMILIAR.

No cabe duda de que tanto la protección de datos personales como la intimidad son derechos fundamentales de la personalidad.

La intimidad es un concepto ligado al Estado democrático. La necesidad del reconocimiento y el respeto de nuestra personalidad, y, más concretamente, el derecho a poder aislarnos de los otros, surge cuando el individuo libre se pone en contacto con los demás. Su objeto es la protección del individuo en el contexto de la vida social. Sin el reconocimiento de los derechos de la personalidad, la libertad de los ciudadanos, tanto para la formación de la voluntad general, como para tomar decisiones autónomas, resultaría inviable. De ahí que, entre los valores inherentes a la intimidad personal, se encuentre en primer lugar la libertad (art. 1.1 CE), en segundo lugar la dignidad de la persona (art. 10.1 CE) y, en tercer lugar, el respeto a los derechos de los demás (art. 10 CE), lo que exige la consideración hacia la intimidad de los demás, sin la cual no se da esa "convivencia democrática" (Preámbulo CE, 2º párrafo) que persigue la Constitución[70]. Más aún, partiendo

[70] RUIZ MIGUEL, C.: *La configuración constitucional del derecho a la intimidad,* Tecnos, Madrid 1995, págs. 17-128. También el Tribunal Constitucional ha afirmado que el derecho a la intimidad personal y familiar es una derivación de la dignidad humana en SSTC 64/1988, FJ 1,

de la doble dimensión de los derechos fundamentales, desde el punto de vista objetivo, el derecho a la intimidad es una garantía institucional del pluralismo y la democracia. Como afirma Ruiz Miguel, "para que una democracia esté viva, es preciso que respete la intimidad de quienes la componen, pues solo así, desde la libertad e independencia de cada ciudadano, puede construirse una sociedad libre"[71].

Como es conocido, el derecho a la intimidad es un concepto reciente en el mundo del Derecho, que tiene su origen en los Estados Unidos, en el trabajo repetidamente citado *"The Right to Privacy"*, publicado en la *Harvard Law Review* por Samuel Dennis Warren y Louis Dembitz Brandeis, en 1890. El artículo tenía por finalidad fundamentar jurídicamente la acción penal contra la prensa por la intromisión en la vida privada de Warren. El termino *privacy*, concebido en un principio como instrumento de defensa, como derecho a estar solo, a ser dejado en paz (the *right to be alone*)[72], desplegó posteriormente su alcance, adquiriendo un significado mucho más amplio[73].

231/1988, FJ 3, 105/1990, FJ 8, 197/1991, FJ 3, 20/1992, FJ 3, 142/1993, FJ 7, 143/1994, FJ 6 entre otras.

[71] RUIZ MIGUEL, C.: *op. cit.,* pág. 120.

[72] En la clásica formulación del juez Cooley en su obra *The Elements of Torts* (1873) y recogida por Warren y Brandeis en *The right to privacy*. Traducida por Benigno Pendás y Pilar Baselga del original, WARREN, S. y BRANDEIS, L.: *El derecho a la intimidad*, Civitas, Madrid, 1996.

[73] La Constitución de Estados Unidos no recoge expresamente *the right of privacy*. De hecho, en 1965 la "privacidad" adquirió rango constitucional cuando el Tribunal Supremo afirmó que su reconocimiento estaba implícito en las "penumbras y emanaciones" de distintas enmiendas constitucionales. En este contexto, el Tribunal Supremo definió la *privacy* como la autonomía para tomar decisiones privadas*. Vid*. RODRÍGUEZ RUIZ, B.: *El secreto de las comunicaciones: tecnología e intimidad,* McGraw-Hill-Interamericana de España, Madrid, 1998, págs. 5-6. En este sentido, en el caso *Roe v. Wade* (1973) 410 U.S. 113, el Tribunal Supremo reconoció el derecho constitucional de la mujer embarazada a interrumpir el embarazo. En relación con la protección de datos personales, *vid*. el caso *Whalen v. Roe* (1977) 429 U.S. 589, en GUILLÉN LÓPEZ, E.: "Sentencia del Tribunal Supremo de los Estados Unidos *Whalen v. Roe* (1977) 429 U.S. 589, sobre protección de datos personales", *ReDCE*, núm. 7, 2007. Disponible en Internet: http://www.ugr.es/~redce/REDCE7/articulos/16sentenciasupremo americano.htm

La indeterminación de la *privacy* fue heredada por los ordenamientos europeos. En Alemania, el Tribunal Constitucional configuró la esfera privada como garantía general de la personalidad, derivada del artículo 2.1, en conexión con el artículo 1.1 de la Ley Fundamental. La imprecisión del término tiene su reflejo en la "teoría de las esferas"[74]. De acuerdo con esta teoría, que fue inicialmente esbozada por Heinrich Hubmann, cabría distinguir ante todo, la "esfera íntima", afectada por aquellas informaciones que inciden en el ámbito vital interno de las personas, especialmente en la vida sexual, así como en el mundo mental y sentimental y sus formas externas de manifestación, o aquellos datos relativos al ser físico del sujeto, como son los relativos a la enfermedad, nacimiento, muerte o desnudez. Con todo, la jurisprudencia constitucional alemana entiende que este ámbito no se puede definir en abstracto, sino en función de las peculiaridades del caso concreto[75]. En segundo lugar se halla la "esfera privada", que abarca cuestiones que afectan a la vida doméstica y al círculo de los familiares y amigos[76]. Y el último peldaño lo ocupa la "esfera individual, social o pública", que comprendería todo aquello que no ha sido incluido en las dos esferas anteriores y se refiere a las relaciones de una persona en su entorno social. No es difícil entrever lo complicado que resulta intentar delimitar claramente las distintas esferas y,

[74] Sobre la teoría de las esferas*, vid*. MEDINA GUERRERO, M.: *La protección constitucional de la intimidad frente a los medios de comunicación*, Tirant lo Blanch, Valencia, 2005, págs. 13-18.
[75] Sobre esta jurisprudencia, MEDINA GUERRERO, M.: *op. cit.,* pág. 14, cita *BVerGE* 80,367, 374, como ejemplo.
[76] *Ibidem,* pág. 15. Señala MEDINA GUERRERO sobre esta esfera: “se han incluido expresamente en la esfera de 'lo privado' acotada por el artículo 2.1 de la Ley Fundamental las reflexiones que uno pueda hacer sobre si mismo en su diario; la comunicación confidencial entre cónyuges; la identidad sexual; los tratamientos médicos; o, en fin, conductas socialmente marginales, como el consumo de drogas”.

precisamente por esto, esta teoría ha sido cuestionada, pues ha venido a generar aún mayor incertidumbre conceptual[77].

Lo cierto es que la "*privacy*" es un término sin traducción exacta en las lenguas latinas. El Convenio Europeo de Derechos Humanos, por ejemplo, reconoce el derecho a la vida privada en su artículo 8, mientras que en España la Constitución optó por el término intimidad. Sin embargo, hay una conexión directa entre ambos conceptos. Así, para Díez-Picazo, el artículo 18 de la Constitución consagra una pluralidad de derechos fundamentales cuyo fin último es proteger la vida privada[78]. Para Ruiz Miguel, es posible distinguir "entre intimidad en sentido estricto y privacidad o lo privado en sentido amplio como ámbitos diferentes pero consecuentes: lo íntimo sería un concepto estricto de dimensiones propiamente individuales y lo privado sería un ámbito que, abarcando lo íntimo, lo supera; pero también podría hablarse de intimidad en sentido amplio como comprensivo de lo privado"[79]. Otros autores, sin embargo, prefieren la distinción entre dichos conceptos. Así, defiende Sempere Rodríguez que el artículo 18 de la CE solo protege la intimidad, y no la vida

[77] Según Walter Schmidt, la teoría de las esferas no proporciona parámetros seguros que hagan previsibles el contenido y la extensión de la protección de la personalidad *Vid.* SCHMIDT, W. "*Die bedrohte Entscheidungsfreiheit*", *JZ* 1974, págs. 243-244, citado por MEDINA GUERRERO, M.: *op. cit.* pág. 38. Para Madrid Conesa, la teoría de las esferas no es válida dado que hoy los conceptos de lo público y lo privado son relativos, pues existen datos que *a priori* son irrelevantes desde el punto de vista del derecho a la intimidad, pero que, unidos unos con otros, pueden servir para configurar una idea prácticamente completa de cualquier individuo, "al igual que ocurre con las pequeñas piedra que forman un mosaico, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado", *vid*. MADRID CONESA, F.: *Derecho a la intimidad, informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984, pág. 45.

[78] DÍEZ-PICAZO, L. M.: *Sistema de derechos fundamentales*, Aranzadi, Cizur Menor (Navarra), 2013, pág. 229.

[79] RUIZ MIGUEL, C.: *op. cit.*, pág. 29.

privada en general[80]. Espín Templado expone que intimidad y vida privada habrían de contemplarse como la parte y el todo, en el sentido de que la intimidad constituiría el núcleo de la vida privada, esto es, su parte más esencial y característica[81].

A nuestro juicio, prueba de que el concepto de vida privada es más amplio y genérico es que nuestro Tribunal Constitucional entiende que el derecho al respeto a la vida privada y familiar reconocido por el artículo 8 del CEDH excede del contenido del artículo 18.1 CE, es decir, del derecho a la intimidad personal y familiar[82]. Así se extrae de las SSTC 236/2007 y 186/2013, en relación con la reagrupación familiar de extranjeros, y 60/2010, en relación con la vida familiar de los presos. Otro tanto ocurre con los riesgos provocados por la contaminación acústica. El Tribunal Europeo de Derechos Humanos ha apreciado que en determinados casos de especial gravedad ciertas inmisiones sonoras constituyen una vulneración del derecho al respeto a la vida privada y familiar (SSTEDH, caso López Ostra contra España, de 9 de diciembre de 1994, y caso Moreno Gómez contra España, de 16 de noviembre de 2004). Si

---

[80] SEMPERE RODRÍGUEZ, C.: "El artículo 18 derecho al honor, a la intimidad y a la propia imagen", en ALZAGA VILLAAMIL, O.: *Comentarios a la Constitución Española de 1978, tomo II,* Edersa, Madrid, 2006.

[81] ESPÍN TEMPLADO, E.: "Fundamento y alcance del derecho fundamental a la inviolabilidad del domicilio*", RCEC,* núm. 8, 1991, pág. 45.

[82] Así lo ha manifestado el Tribunal Europeo de Derechos Humanos en la sentencia de 27 de mayo de 2014, caso de La Flor Cabrera contra España, en el párrafo 30:" El Tribunal recuerda que la noción de 'vida privada' es una noción amplia, no susceptible de una definición exhaustiva, que cubre la integridad física y moral de la persona y, por tanto, engloba múltiples aspectos de la identidad de un individuo, tales como el nombre o los elementos que hacen referencia al derecho de imagen (Von Hannover contra Alemania [núm. 2], párrafos 95-96, 7 de febrero de 2012). Esta noción comprende las informaciones personales que un individuo puede legítimamente esperar que no sean publicadas sin su consentimiento (Flinkkilä y otros contra Finlandia, ap. 75, 6 abril 2010, Saaristo y otros contra Finlandia, ap. 61, 12 octubre 2010). La publicación de una foto interfiere en la vida privada de una persona, aunque esta persona sea una persona pública (Schüssel contra Austria, 21 febrero 2002). Con mayor motivo, el Tribunal afirma que la grabación de imágenes de vídeo constituye igualmente una injerencia en la vida privada de un individuo".

bien esta jurisprudencia ha sido acogida por el Alto Tribunal español, como lo demuestra la admisión a trámite de las demandas de amparo por violación de los derechos a la intimidad y a la inviolabilidad domiciliaria, en los casos de contaminación acústica[83], podemos afirmar que esta recepción por la vía del artículo 10.2 CE confirma que la noción de vida privada en el CEDH es más extensa y no se restringe al ámbito de lo íntimo. De hecho ninguno de los recursos de amparo interpuestos por vulneración del derecho a la "intimidad domiciliaria" ha sido estimado por el Tribunal Constitucional.

Todo esto nos lleva a afirmar que el derecho a la intimidad se caracteriza por su enorme imprecisión terminológica[84]. Como pone de manifiesto Rodríguez Ruiz, la flexibilidad conceptual de un derecho lleva consigo la dificultad de determinar qué situaciones quedan dentro de su ámbito de cobertura y cuáles quedan fuera e implica inseguridad en torno a sus límites, sin que ello prejuzgue que aquellos hayan de ser objeto de interpretación amplia o restrictiva[85].

Nuestro Tribunal Constitucional ha hecho referencia expresa a las dificultades de acotar con nitidez el contenido de la intimidad[86]. Partiendo de una concepción material de la intimidad, la jurisprudencia constitucional ha seleccionado materias que por su contenido pueden identificarse con lo íntimo y que integran el ámbito constitucionalmente protegido por el derecho fundamental reconocido en el artículo 18.1 de la Constitución. Así, formarían

---

[83] Sobre esta materia, *vid.* JIMÉNEZ-CASTELLANOS BALLESTEROS, I.: "A vueltas con la contaminación acústica: comentario a la STC 150/2011 de 29 de septiembre", *REDF,* núm. 18, 2011, págs. 249-274.
[84] *Vid*. LUCAS MURILLO DE LA CUEVA, P.: *El derecho a la autodeterminación informativa*…, pág. 88.
[85] RODRÍGUEZ RUIZ, B.: *op .cit.*, pág. 1.
[86] STC 110/1984, FJ 3.

parte de este espacio la intimidad corporal, entendiendo por tal no la entidad física del cuerpo, sino la entidad cultural, es decir, el criterio dominante en nuestra cultura sobre el recato corporal[87], las relaciones sexuales, de tal manera que el acoso sexual puede reputarse un caso de violación de la intimidad[88], la vida sentimental[89], el estado de salud[90], el consumo de alcohol y drogas[91], la filiación[92], los antecedentes penales[93] y la videovigilancia[94]. Por el contrario, no formarían parte de la intimidad la situación económica de las personas, ni las relaciones profesionales en que se desenvuelve la actividad laboral[95].

No obstante, el Tribunal Constitucional tampoco ha descartado la asunción de una concepción subjetiva de la intimidad[96], que implica que es la voluntad del interesado la que determinará esta esfera personal y no la naturaleza más o menos próxima a "una calidad mínima de vida humana"[97]. Así, la extensión de este ámbito privado variará de una persona a otra, dependiendo de lo que cada cual estime como propio de su intimidad. En esta línea, "el artículo 18.1 de la Constitución no garantiza una 'intimidad' determinada, sino el derecho a poseerla, a tener vida privada, disponiendo de un poder de control sobre la publicidad de la información relativa a la persona y su familia, con independencia del contenido de aquello que se desea mantener

[87] SSTC 37/1989, 57/1994, 207/1996, 156/2001, 218/2002 y 171/2013.
[88] SSTC 89/1987, 151/1997, 224/1999, 136/2001, y 121/2002.
[89] SSTC 176/2013 y 7/2014.
[90] SSTC 231/1988, 70/2009.
[91] SSTC 25/2005, 206/2007 y 196/2004.
[92] STC 197/1991 y 190/2003.
[93] SSTC 144/1999, 46/2002, 52/2002 y 135/2014.
[94] SSTC 98/2000, 186/2000 y 39/2016.
[95] SSTC 110/1984, 143/1994, 142/1993 y 170/1987.
[96] SSTC 134/1999, FJ 5, 144/1999, FJ 8 y 115/2000, FJ 4.
[97] STC 231/1988, FJ 3.

al abrigo del conocimiento público. Lo que el artículo 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan que somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio"[98].

La jurisprudencia constitucional pone de manifiesto que esta concepción subjetiva es una posición consolidada. De acuerdo con esta orientación, Marc Carrillo sostiene que "las señas de identidad del derecho a la intimidad se asientan más en la libertad de disponibilidad sobre lo privado que en el contenido del ámbito de los privado"[99]. No obstante, la asunción de la comprensión subjetiva del derecho a la intimidad no entraña la total desaparición de la concepción material. Como apunta Medina Guerrero, esta sigue conservando alguna presencia en la jurisprudencia constitucional, concretamente en la concurrencia de derechos fundamentales. Así, en relación con el derecho a la protección de datos de carácter personal, la violación del artículo 18.4 CE supondrá, además, la del artículo 18.1 CE si se aprecia que el dato no es solo personal, sino también "materialmente íntimo"[100].

---

[98] SSTC 134/1999, FJ 5, 115/2000, FJ4, 83/2002, FJ 5, 99/2002, FJ 6, 121/2002, FJ 2, 185/2002, FJ 3, 89/2006 FJ 5 y 176/2013, FJ 7.

[99] CARRILLO, M.: *El derecho a no ser molestado. Información y vida privada*. Aranzadi, Cizur Menor (Navarra), 2003, pág. 81. También, RODRÍGUEZ RUIZ, cuando afirma que "podemos definir el derecho a la intimidad como el derecho a controlar o autodeterminar nuestras zonas de retiro y de secreto", RODRÍGUEZ RUIZ, B.: *op. cit.,* pág. 17. En contra, Díez-Picazo, que sostiene que "es preferible el enfoque tradicional que concibe el contenido del derecho a la intimidad en clave predominantemente material". *Vid.* DÍEZ-PICAZO, L. M.: *op. cit.,* pág. 282.

[100] STC 292/2000, FJ 6. También señala como ejemplos de la concepción material de la intimidad las colisiones entre el derecho a la intimidad y la libertad de información, o entre el derecho a la intimidad y el secreto de las comunicaciones, o entre el derecho a la intimidad y el derecho a la propia imagen. *Vid*. MEDINA GUERRERO, M.: *op. cit.*, págs. 49 a 51.

El alcance del derecho a la intimidad, en su significación más clásica, consistiría esencialmente en la acepción estricta de lo íntimo, en el derecho a disfrutar de determinadas zonas de retiro y secreto. Su razón de ser se hallaría en la necesidad del individuo de excluir del conocimiento ajeno cuanto guardara relación con un ámbito propio y reservado[101].

En su concepción tradicional, por tanto, se trataría de un derecho de defensa frente a los ataques de los poderes públicos. El reconocimiento de una esfera privada, por su parte, comportaría una garantía de libertad para el individuo y un límite, ante todo, al poder del Estado, pero que se extiende en su concepto moderno hasta la salvaguardia de un espacio privado en el que los particulares no podrían entrar sin el consentimiento del titular. El Tribunal Constitucional ha afirmado que el derecho a la intimidad "atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia de una publicidad no querida"[102].

El desarrollo legislativo del derecho a la intimidad reconocido en el artículo 18.1 de la Constitución se materializó en 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 contempla estos derechos, principalmente, como límites a la libertad de expresión e información prevista en el artículo 20.4 del texto constitucional. No obstante, el peligro que representan las actuaciones abusivas o ilícitas en el tratamiento de los datos personales difiere de la intromisión de los medios de comunicación en la vida privada de las personas.

---

[101] *Vid*. LUCAS MURILLO DE LA CUEVA, P.: ”El derecho a la autodeterminación informativa y la protección de datos personales”, *Cuadernos de Derecho*, núm. 20, 2008, pág. 46.
[102] SSTC 236/2007, FJ 11, 134/1999, FJ 5, y 115/2000, FJ 4.

Además el carácter indemnizatorio de los sistemas de tutela propios del derecho a la intimidad no resulta eficaz para una adecuada protección del titular de los datos.

Con el despliegue de las TIC, hay autores que vieron en el derecho a la intimidad el amparo desde el que responder a las vulneraciones derivadas del uso incontrolado de la información personal. Desde esta perspectiva, la autodeterminación informativa no sería un nuevo derecho, sino que estaríamos hablando del derecho a la intimidad aplicado a una nueva realidad, el derecho a la intimidad informática[103]. Así, Ruiz Miguel afirma que varias Constituciones de Estados europeos acogen el derecho a la protección de los datos personales, bien expresamente y de forma autónoma (Portugal, Suecia) o bien como una derivación del derecho a la intimidad (o a la vida privada) ya consagrado (España, Finlandia, Holanda). Y donde no se dan estas circunstancias, la jurisprudencia crea *ex novo* el derecho (Alemania)[104]. Valga decir a estos efectos, afirma el autor, que las diversas manifestaciones jurídicas protectoras del ámbito privado o íntimo de la persona (intimidad en sentido estricto, vida privada, secreto de las comunicaciones, inviolabilidad del

[103] Sin poner en duda su naturaleza de derecho fundamental autónomo respecto de los demás protegidos en el artículo 18 CE, Carreras hace la distinción entre la intimidad física (art.18.1CE) y la intimidad informática (art. 18.4 CE). “La protección de la intimidad física es aquel ámbito material que una persona quiere que permanezca a resguardo de las intromisiones ajenas". La segunda es algo distinto: "el individuo va suministrando en su vida diaria, de forma voluntaria o por obligación legal, un gran número de datos referidos a su persona que combinados entre sí pueden ofrecer informaciones sobre su vida personal que no ha previsto y ni siquiera podía prever, que no desea que sean conocidos con carácter general aunque haya consentido que se sepan en determinados ámbitos". *Vid.* CARRERAS SERRA, F.: "El derecho fundamental a la protección de datos personales", en AA.VV.: *Los nuevos derechos fundamentales: seminario: Baeza, 13 y 14 de octubre de 2005 : XXV aniversario Tribunal Constitucional,* Academia de Ciencias Sociales y del Medio Ambiente de Andalucía, 2007, pág. 69.

[104] RUIZ MIGUEL, C.: “El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: Análisis crítico”, *Revista de Derecho Comunitario Europeo*, núm. 14, 2003, pág. 41.

domicilio, secreto profesional, intimidad genética) son reconducibles a un contenido último, a saber, la autodeterminación informativa o poder del sujeto de determinar qué información sobre su persona y sus circunstancias puede ser comunicada a terceros, bien porque en ese momento aún no es pública o bien porque no deba serlo. Este control de sujeto o autodeterminación informativa, en que consiste toda intimidad, se traduce en un conjunto de derechos (con sus correlativas obligaciones) que no solo tienen una naturaleza de "derechos subjetivos", sino que también tienen una vertiente objetiva, de tipo orgánico-procedimental, y aun una tercera dimensión valorativa, a la que a veces incluso se añade una dimensión cultural-nacional. Estas ideas, aplicadas al uso de ficheros, se traducen en el llamado derecho a la protección de datos personales[105]. La intimidad, en sentido amplio, sería pues, sinónimo de autodeterminación informativa, es decir, la facultad del individuo de controlar las informaciones propias en manos de terceros.

Para Ortí Vallejo, lo que la informática ha significado es una ampliación del concepto del derecho a la intimidad. El término privacidad es el mismo derecho a la intimidad, solo que reformulado y actualizado en función de las necesidades que demanda el cambio social y tecnológico[106].

La previsión del apartado cuarto del artículo 18 CE alude en primer lugar a la protección del honor y de la intimidad personal y familiar de los ciudadanos. De hecho, su concreta ubicación podía inducir a interpretar que el

---

[105] *Ibidem*, págs. 32-33.

[106] "Esta nueva prerrogativa jurídica tutela derechos de la personalidad ya formulados y existentes, en especial de la intimidad, que ha recibido una importante reformulación conceptual por influjo, precisamente, de la problemática informática" en este sentido, 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*, núm. 2, 1994, pág. 330.

bien jurídico que se deseaba proteger es la intimidad. Así, en el recurso de inconstitucionalidad[107] interpuesto contra la Ley Orgánica 5/1992, de 29 de octubre -LORTAD-, el Parlamento de Cataluña argumenta que “la Ley Orgánica recurrida viene a cumplir con el mandato contenido en el apartado 4 del artículo 18 CE, que, en puridad, no contiene derecho fundamental alguno, sino una vía de limitación de la informática, que constituye una específica garantía de los derechos fundamentales del artículo 18.1 CE, y en general de los derechos de la persona”.

Como garantía constitucional del derecho a la intimidad se configura el derecho fundamental a la protección de datos en la STC 143/1994, a propósito del tratamiento de la información obtenida a través de las operaciones con número de identificación fiscal (NIF) sin las garantías debidas. La sentencia puso de relieve las amenazas de un uso desviado de esa información y, como consecuencia, "la efectiva invasión de la esfera privada de los ciudadanos afectados". Reiteró, además, lo que ya había expuesto en la resolución del *habeas data*[108]*,* esto es que "el incremento de medios técnicos de tratamiento de la información pueden ocasionar este efecto y, correlativamente, se hace precisa la ampliación del ámbito de juego del derecho a la intimidad… incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho". Y aun reconociendo que esta conclusión derivaba de los compromisos internacionales asumidos por España sobre la base del artículo 10.2 CE, particularmente el Convenio 108, y a pesar de la referencia expresa a los principios de la

[107] STC 290/2000, antecedente segundo.
[108] STC 254/1993.

LORTAD, el Tribunal no alcanzó a deslindar este derecho de la garantía de la intimidad.

En términos similares, como intromisión ilegítima en el derecho a la intimidad, se contempla en la STC 144/1999, relativa a la infracción de las normas sobre acceso a los antecedentes penales. La interpretación constitucional atribuye al artículo 18.1 CE un sentido amplio y subjetivo, que "no garantiza sin más la 'intimidad', sino el derecho a poseerla, a tener vida privada disponiendo de un poder de control sobre la publicidad de la información relativa a nuestra persona y familia, sea cual sea el contenido de aquello que se desea mantener al abrigo del conocimiento público" (FJ 8). Por tanto, con independencia de que esa información sea objetivamente considerada de las íntimas, o de que su conocimiento o divulgación pueda ser perniciosa para la integridad moral o la reputación de aquel o aquellos a los que se refiere.

En realidad, se trata de la jurisprudencia clásica sobre derecho a la intimidad aplicado a la protección de datos. Esta jurisprudencia no surge al hilo de la protección de datos, pero halla en esta materia un nuevo campo de desarrollo. Lo positivo de esta jurisprudencia fue haber advertido la necesidad de reconocer facultades positivas que permitan el control de la información personal, aunque sea como garantía del derecho a la intimidad. En suma, la constatación de que el auge de las nuevas tecnologías ha generado nuevos riesgos en torno al tratamiento de la información que hacen necesario un concepto vasto de intimidad que acoja, bajo su regulación, facultades de control sobre los datos personales. Así pues, se presentaba como una necesidad cada vez más apremiante el reconocimiento al individuo de un

conjunto de facultades y garantías que le permitieran una defensa de su vida privada eficaz ante las nuevas condiciones creadas por el avance de la tecnología. Internet no deja a salvo resquicio alguno a la vida privada de las personas. No basta con el reconocimiento de un derecho de exclusión, de negación de información, porque dejaría indefenso a quien, habiendo cedido libremente sus datos personales, no pudiera constatar cuál hubiera sido su destino y la finalidad de su utilización o no pudiera conocer si aquellos han sido utilizados de forma desviada[109]. El derecho fundamental a la protección de datos, por tanto, es un derecho básicamente preventivo, que dota a su titular de garantías suficientes para evitar y, al mismo tiempo, controlar el uso abusivo o ilícito de la información personal. El derecho a la información, la prestación del consentimiento, el derecho de rectificación, oposición o cancelación, así como las garantías institucionales que configuran este derecho, hacen posibles tales objetivos.

Según explica Lucas Murillo de la Cueva, en otros ordenamientos se ha interpretado el concepto de intimidad de una forma amplia, esto es, centrada especialmente en la voluntad de cada individuo afectado y, por tanto, no habría excesiva dificultad en incluir dentro del contenido de tal derecho la tutela frente al uso de la informática, ya que el derecho a la intimidad incluiría la facultad de vedar la recogida y utilización de información personal, así como el control sobre esta última[110]. Sin embargo, entre nosotros prevalece la posición que sostiene la inconveniencia de manejar un concepto amplio de intimidad, que podría, según Del Castillo Vázquez, desnaturalizar el derecho que la tutela y,

[109] HERRANZ ORTIZ, A.: *op. cit.,* pág. 92.
[110] LUCAS MURILLO DE LA CUEVA, P.: *El derecho a la…*, pág. 26-27.

en consecuencia, mermar su nivel de protección[111]. Como explica Herranz Ortiz, los derechos nacen y se formulan bajo unas condiciones y circunstancias concretas. Así, el derecho a la intimidad no nace para enfrentarse a las nuevas tecnologías de la información, ni para controlar el tratamiento automatizado de los datos personales, por lo que encasillar la técnica de la protección de datos en las formulaciones tradicionales del derecho a la intimidad no conduce sino al inevitable desamparo de la persona frente a los avances tecnológicos[112].

Ahora bien, hay que reconocer que, al menos en parte, coinciden el derecho a la intimidad y el derecho a la autodeterminación informativa, y, en relación con las nuevas tecnologías, pueden producirse situaciones de potenciales agresiones a ambos derechos fundamentales. Sin embargo, no parece que puedan considerarse incluidas en el primero las exigencias relacionadas con la protección de datos de carácter personal no encuadrables en la noción de intimidad en sentido estricto. En efecto, todo lo relacionado con el control de la información personal plantea líneas absolutamente innovadoras con la irrupción de las nuevas tecnologías[113]. En especial, no sirve para el objetivo de la protección de datos la noción estricta de la intimidad, pues, normalmente, no son los datos personalísimos los que constituyen objeto de tratamiento automatizado. Si este fuese el bien jurídico que defender, como

[111] DEL CASTILLO VÀZQUEZ, I. C.: *op. cit.*, pág. 224.
[112] HERRANZ ORTIZ, A.: *op. cit.,* pág. 127.
[113] LUCAS MURILLO DE LA CUEVA, P.: *op. cit.*, pág. 26-27. En GUICHOT REINA, E.: *Publicidad y privacidad de la información administrativa*, Aranzadi, Cizur Menor (Navarra), 2009, pág. 183, el autor se plantea las dificultades que presenta la integración de la protección de datos en el contenido del derecho a la intimidad.

afirma del Castillo Vázquez, lo que habría que resguardar del peligro informático sería bastante poco[114].

Esta característica peculiar del derecho a la protección de datos empieza a aparecer en la jurisprudencia del Tribunal Constitucional con la STC 11/1998. Esta resolución es la primera de una serie en la que queda fortalecida la visión del derecho a la protección de datos como autónomo respecto al derecho a la intimidad. Así, aquel derecho se extiende a todas las informaciones que conciernan a la persona, aunque no pertenezcan al ámbito estricto de la intimidad, como era, en este caso, la afiliación sindical. En consecuencia, la protección de datos puede ser garantía de otros derechos fundamentales, como la libertad sindical, el derecho de huelga o el principio de igualdad.

Lo que se planteaba en la sentencia 143/1994 como hipotéticos riesgos para el derecho a la intimidad ante un posible uso abusivo de los datos económicos se convierte en una realidad en un conjunto de sentencias que dictará el Tribunal Constitucional a lo largo de los años 1998 y 1999[115]. Todas ellas comparten argumentos y fallo con la STC 11/1998. La utilización por la empresa Renfe de los datos de afiliación sindical de los trabajadores para detraer de su nómina las cantidades correspondientes a una huelga, dando por hecho que, por pertenecer a los sindicatos convocantes, habían secundado el paro, conduce al Tribunal Constitucional a declarar vulnerada su libertad sindical en conexión con el artículo. 18.4 CE. Según el Alto Tribunal, este último no solo entraña un específico instrumento de protección de los derechos

[114] DEL CASTILLO VÁZQUEZ, I. C.: *op. cit.*, pág. 224.
[115]SSTC 33/1998, 35/1998, 45/1998, 60/1998, 77/1998, 94/1998, 104/1998, 105/1998, 106/1998, 123/1998, 124/1998, 125/1998, 126/1998, 158/1998 ,198/1998, 223/1998, 30/1999, 44/1999 y 45/1999.

del ciudadano frente al uso torticero de la tecnología informática, sino que, además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la privacidad, según la expresión utilizada en la Exposición de Motivos de la LORTAD- pertenezcan o no al ámbito más estricto de la intimidad. Lo cierto es que en el asunto se utilizó un dato sensible, que había sido proporcionado con una determinada finalidad, la de descontar la cuota sindical y transferirla al sindicato, para otra radicalmente distinta, con menoscabo del legítimo ejercicio de la libertad sindical, y propiciando situaciones discriminatorias.

En la STC 202/1999, el Tribunal retoma el discurso de que la garantía de la intimidad adopta hoy un entendimiento positivo, que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es, así, el derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención[116]. No obstante, hay referencias a la protección de la vida privada fundamento último de la intimidad, como protección de la libertad y de las posibilidades de autorrealización del individuo. Además se termina por calificar la medida adoptada por el empresario de inadecuada y desproporcionada, por vulnerar el derecho a la intimidad y a la libertad informática del titular de la información.

[116] SSTC 254/1993, FJ 7, 11/1998, FJ 4, y 94/1998, FJ 4.

Finalmente, la protección que la Constitución quiere asegurar frente a las nuevas tecnologías tiene un alcance mucho más extenso que la que proporciona el derecho a la intimidad entendido en sentido estricto. Trata de dar respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona[117].

Como afirma Del Castillo Vázquez, no pueden identificarse intimidad y privacidad, entendida esta como protección de datos, pues siendo los dos derechos fundamentales, cada uno disfruta de un contenido esencial distinto. El contenido esencial del derecho a la intimidad se refiere a la garantía del ámbito propio y reservado de cada sujeto, mientras que el contenido esencial de la autodeterminación informativa responde a la decisión personal de preservar la identidad a través del control de la información concerniente a los datos de carácter personal. La dimensión del derecho a la intimidad significa el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, mientras que el derecho a la autodeterminación informativa garantiza la facultad de todo individuo de preservar su vida privada controlando el registro, uso y revelación de los datos que le conciernen[118].

No solo la doctrina pone de manifiesto las diferencias. También el Tribunal Constitucional ha trazado los lindes entre los derechos fundamentales a la protección de datos y a la intimidad con distintos argumentos. No cabe duda de que ambos comparten el objetivo de ofrecer una eficaz protección constitucional a la vida privada personal y familiar. Sin embargo, en el derecho a la protección de datos no nos hallamos ante un derecho de defensa, como

[117] STC 233/1999, FJ 7.
[118] DEL CASTILLO VÁZQUEZ, I. C.: *op. cit.*, págs. 224-226

lo es el derecho a la intimidad, que impone deberes de abstención, sino que nos encontramos ante una facultad de control sobre los datos relativos a la propia persona que impone verdaderas obligaciones de hacer. Así, el Tribunal Constitucional, en el fundamento sexto de la STC 292/2000, distingue la función de ambos derechos: en lo relativo a la intimidad, sería proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad[119]; en cambio, el derecho fundamental a la protección de datos persigue garantizar al individuo un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado. En definitiva, el derecho a la intimidad permite a la persona excluir ciertos datos del conocimiento ajeno, y, en consecuencia, resguardar su vida privada de una publicidad no querida[120], mientras que el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre sus datos. En este sentido, Frosini afirma que la libertad informática es, entonces, la nueva fórmula que sustituye al antiguo *right to privacy*, en cuanto no tiene solamente un significado negativo, de defensa ante la intervención ajena, sino que también ha adquirido un significado positivo. Ello consiste no solo en la afirmación de una esfera de privacidad, sino también en la facultad de acceso, de control, de rectificación y de cancelación de los datos personales insertos en un banco de datos[121].

---

[119] Por todas, STC 144/1999, FJ 8.
[120] SSTC 134/1999, FJ 5; 144/1999, FJ 8; 98/2000, FJ 5; 115/2000, FJ 4.
[121] FROSINI, V.: "La tutela de la privacidad: de la libertad informática al bien jurídico informático", *Revista del Colegio de Abogados de Buenos Aires*, núm. 2, 1989, pág. 96.

De ahí la singularidad de este derecho. Como explica el Tribunal Constitucional en el fundamento sexto de la STC 292/2000, el derecho a la intimidad personal y familiar confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en su esfera íntima y la prohibición de hacer uso de lo así conocido[122]. Por el contrario, el derecho a la protección de datos atribuye a su titular un haz de facultades, consistente en diversos poderes jurídicos, cuyo ejercicio impone a terceros deberes jurídicos que no se contienen en el derecho fundamental a la intimidad y que sirven a la capital función que desempeña este derecho fundamental, que es garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. Estos poderes se concretan en el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, en el derecho a saber y ser informado sobre el destino y uso de esos datos y en el derecho a acceder, rectificar y cancelar los mismos. En definitiva, el poder de disposición sobre los datos personales.

El contenido esencial del derecho a la protección de datos es el control, y no la garantía de un ámbito propio y reservado del conocimiento ajeno. De ahí que la lesión de este derecho no provenga de la injerencia o intromisión ilegítima en ese ámbito, ya que es el propio interesado el que la mayoría de las veces consiente en la entrega de sus datos personales de forma voluntaria o por imposición legal. La vulneración vendrá de la privación del haz de facultades y principios que conforman el poder de control del interesado sobre

[122] SSTC 73/1982, FJ 5; 110/1984, FJ 3; 89/1987, FJ 3; 231/1988, FJ 3; 197/1991, FJ 3 y, en general, las SSTC 134/1999, 144/1999 y 115/2000.

sus datos personales, con el resultado de que aquellos se usen para una finalidad distinta para la que fueron recabados o sin el consentimiento de su titular, se utilicen datos que no sean correctos, no se informe al afectado sobre los datos o sobre su cesión o los datos sean cedidos de forma irregular.

Además de por su naturaleza y por el haz de facultades que otorgan, ambos derechos difieren en cuanto a su objeto. De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce solo 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, o pueda suponer la creación de un perfil de la persona. Por consiguiente, también alcanza a aquellos datos personales públicos, que, pese a 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 solo tengan protección los relativos a la vida privada o íntima de la persona, sino que, por el contrario, 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"[123].

[123] STC 292/2000, FJ 6. Como señala HERRANZ ORTIZ, "resulta innegable que el derecho a la autodeterminación informativa se construye tomando como fundamento el concepto de intimidad o vida privada. (…) Ahora bien mediante el derecho a la autodeterminación informativa no se salvaguardan tan solo los datos que se denominan sensibles, sino también aquellos que sin pertenecer a la esfera más próxima al individuo son susceptibles de dañar su imagen o el ejercicio pleno de sus derechos. Más aún, ni tan siquiera los considerados datos sensibles representan siempre información íntima o secreta de la persona, el origen racial o determinadas enfermedades son tan evidentes y reconocibles externamente que de ellas poco

Por último, desde el punto de vista legislativo, la remisión que la Carta Magna hace al legislador para que establezca límites en el uso de la informática podría haber justificado que en las distintas leyes de desarrollo de los derechos fundamentales se hubiera tenido en cuenta la necesidad fijar tales límites. Por el contrario, el legislador ha optado por una regulación general, primeramente por la LORTAD, después en la LOPD, que ha establecido un régimen completo, no de prohibición, sino de garantía de los derechos de los ciudadanos. Esto último viene también a reforzar la consideración del derecho fundamental a la protección de datos como autónomo frente al derecho a la intimidad.

No podemos dejar de citar aquí la exposición de motivos de la LORTAD, por ser reveladora de cuanto decimos, al afirmar que “el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida". Nótese que se habla de *la privacidad* y no de *la intimidad*. Desde la perspectiva de la LORTAD, mientras la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona, como el domicilio y las comunicaciones, la privacidad constituye un conjunto más amplio y global de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca, pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado. De ahí que, para la ley, si la intimidad, en sentido estricto, está suficientemente

---

permanece reservado en la intimidad del individuo, y sin embargo, no puede dudarse de su carácter sensible como informaciones personales". *Vid.* HERRANZ ORTIZ, A.: *op. cit.,* pág. 75.

protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas, lo que justificaría la existencia de la propia LORTAD.

El debate doctrinal ha quedado hoy en un segundo plano a la vista de la jurisprudencia de nuestro Tribunal Constitucional, que ha consagrado el derecho a la protección de datos en relación con el derecho a la intimidad, pero con aspectos conceptuales propios que lo convierten en un derecho autónomo. Si bien ha existido algún intento de ampliar el concepto de intimidad, compartimos la opinión de Serrano Pérez de que no cabría más remedio que optar por esa solución solo si el ordenamiento no ofreciera otra alternativa. Sin embargo, una correcta interpretación del artículo 18.4 CE permite encajar en él perfectamente la protección de datos sin necesidad de hacer interpretaciones s extrañas de ámbito del derecho a la intimidad, tal y como ha hecho el Tribunal Constitucional en la sentencia 292/2000[124].

En resumen, podemos concluir con la afirmación de Herranz Ortiz relativa a que la construcción del derecho a la autodeterminación informativa se encuentra unida a la preocupación del individuo por reservar su vida del conocimiento ajeno, pero, fundamentalmente, por controlar la imagen que los

[124] SERRANO PÉREZ, M. M.: *El derecho fundamental a la protección de datos. Derecho Español y Comparado,* Thomson-Civitas, Madrid, 2003, pág. 148. Por el contrario, Guichot Reina se cuestiona si no sería más coherente con la ubicación del precepto y con el conjunto de la jurisprudencia constitucional sostener que el derecho a la intimidad comprende, dentro de su contenido, los principios, derechos y garantías a los que alude la STC 292/2000, que serían el nuevo contenido del derecho a la intimidad de la información personal, si bien es cierto que no escapa al autor que esta opción presenta algunas dificultades, GUICHOT REINA, E.: *op. cit.*, págs. 182-183.

demás puedan tener de él a través de los datos que se difunden relativos a su persona[125].

3. LA DELIMITACIÓN DEL CONTENIDO ESENCIAL DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES.

El avance de las nuevas tecnologías ha puesto en riesgo no ya nuestra intimidad, sino nuestra propia identidad y libertad, mediante el almacenamiento y tratamiento de datos personales aparentemente irrelevantes, sean o no íntimos, pero que permiten trazar el perfil de una persona. La vinculación del derecho a la protección de datos con la dignidad humana ha sido la base para la inclusión de este derecho en el catálogo de los derechos fundamentales, a partir de la interpretación del artículo 18.4 CE. La STC 254/1993, de este modo, afirma que "…nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza

[125] HERRANZ ORTIZ, A.: *op. cit.,* págs. 76 y 77. A modo de resumen señala esta autora: "Quienes defienden la necesidad de reconocer un nuevo derecho fundamental recurren con frecuencia a tres argumentos que se convierten en piedra angular de sus consideraciones. Así, los debates parlamentarios en torno a la aprobación del artículo 18.4 de la CE por un lado, la insuficiencia protectora de los mecanismos jurídicos propios del tradicional derecho a la intimidad por otro lado y finalmente, la naturaleza de los derechos y libertades amenazados se convierten en las razones fundamentales que conducen a la inevitable conclusión de admitir el nacimiento de un nuevo derecho fundamental vinculado al desarrollo de las nuevas tecnologías de la información", HERRANZ ORTIZ, A.: *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Dykinson, Madrid, 2002, pág. 77. En el mismo sentido Lucas Murillo de la Cueva para quien si no coinciden los ámbitos materiales que se quieren defender con el derecho a la intimidad y con la protección de datos personales; si aquel responde a una concepción preinformática y si ésta va configurándose como un sector especializado del ordenamiento jurídico, tal vez convenga abandonar la referencia a la intimidad y encabezar la problemática con un epígrafe distinto. No se trata de un cambio nominal, sino de una consideración sistemática, más acorde con la realidad, LUCAS MURILLO DE LA CUEVA, P.: *El derecho a la autodeterminación informativa…,* pág. 120.

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 distintos derechos fundamentales"[126].

El carácter autónomo del derecho a la protección de datos exige delimitar su contenido esencial, para lo cual hay que partir, como sabemos, de su naturaleza y de los intereses jurídicamente protegidos por este derecho. En palabras, ya clásicas, del Tribunal Constitucional, "para tratar de aproximarse a la idea de contenido esencial… cabe seguir dos caminos. El primero es tratar de acudir a lo que se suele llamar la naturaleza jurídica o el modo de concebir o de configurar cada derecho (…) Constituyen el contenido esencial de un derecho subjetivo aquellas facultades o posibilidades de actuación necesarias para que el derecho sea reconocible como pertinente al tipo descrito y sin las cuales deja de pertenecer a ese tipo y tiene que pasar a quedar comprendido en otro desnaturalizándose, por decirlo así. Todo ello referido al momento histórico de que en cada caso se trata y a las condiciones inherentes en las sociedades democráticas, cuando se trate de derechos constitucionales. El segundo (…) consiste en tratar de buscar lo que una importante tradición ha llamado los intereses jurídicamente protegidos como núcleo y médula de los derechos subjetivos (…) De este modo, 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"[127].

[126] STC 254/1993, FJ 6.
[127] STC 11/1981, FJ 8.

De lo expuesto se deduce que el contenido esencial del derecho a la protección de datos personales debe estar compuesto por aquellas facultades indispensables para hacer efectiva la decisión de la persona de preservar su identidad, es decir la privacidad en sentido amplio, a través del control de sus datos de carácter personal en las diferentes fases del tratamiento de la información[128]. Para ello, el titular de este derecho cuenta con diferentes recursos no solo en el momento de la recopilación y registro de la información personal, sino también en su uso posterior, en cualquiera de las modalidades del tratamiento de la misma.

Para delimitar el contenido del derecho a la protección de datos, la doctrina y la jurisprudencia han partido, ante todo, y como es necesario de nuestra Carta Magna, que lo ha contemplado como un derecho de configuración legal, lo que hace que haya correspondido al legislador orgánico, por mandato constitucional (artículo 18.4 CE) y mediante la transposición de la Directiva 95/46/CE, hoy derogada, determinar el alcance de la protección de este derecho. El Reglamento General de Protección de Datos supone la revisión de las bases legales del modelo europeo de protección de datos. Permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios[129]. Los reglamentos europeos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas

[128] STC 292/2000, FJ 6: "… el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado".
[129] *Vid.* considerando 8 del RGPD.

complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de "desarrollo" o complemento del Derecho de la Unión Europea. La adaptación al Reglamento General de Protección de Datos, que será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual[130].

De acuerdo con nuestra Constitución el uso de la informática encuentra su límite en el respeto "al honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos". El análisis de los intereses jurídicamente protegidos frente al poder informático empieza por el honor. Constituye una amenaza a la reputación personal el tratamiento de datos inexactos, incompletos, obsoletos o falsos que pongan en peligro el respeto de la persona frente a terceros, al suponer un juicio de valor sobre el titular de la información. Además, la lesión del derecho al honor puede producirse, aunque no se refiera a una información íntima de la persona. Lo cierto es que en muchos supuestos no será sencillo determinar si el bien jurídico lesionado es el honor o la intimidad; sin embargo, la dificultad queda orillada por el hecho de que esta última constituye también objeto de protección del derecho a la autodeterminación informativa. Por otra parte, la falta de previsión constitucional respecto a la consideración de la propia imagen como objeto de protección frente a las agresiones informáticas solo se entiende desde el descuido del constituyente español[131]. Si el dato personal es la información

[130] Exposición de motivos del Proyecto de Ley Orgánica de Protección de Datos de 24 de noviembre de 2017, BOCG, núm. 13.1, pág. 7. Disponible en Internet: http://www.congreso.es/publicoficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF

[131] HERRANZ ORTIZ, A.: *op .cit.*, pág. 145.

gráfica resulta un bien jurídicamente protegible la propia imagen, que puede ser también objeto del tratamiento de datos.

A la vista del enunciado del artículo 18.4 CE, el ámbito de protección del derecho examinado se extiende también a otros bienes de los individuos, y, por tanto, a cualesquiera otros derechos, reconocidos o no constitucionalmente. Para Álvarez Cienfuegos, el precepto legitima una lectura de todo el Capitulo Segundo del Título I de la Constitución en "clave informática"[132]. Así, la STC 11/1998 reconoció la violación de la libertad sindical en conexión con el artículo 18.4 CE; la STC 96/2012 resolvió la vulneración del derecho a la tutela judicial efectiva en relación con el derecho a la protección de datos de carácter personal. Por otra parte, en la STC 199/2013, el Tribunal Constitucional entra a resolver una supuesta vulneración de los derechos a la igualdad, intimidad y protección de datos personales, tutela judicial efectiva, presunción de inocencia y legalidad penal.

Como todo derecho fundamental, con base en el artículo 10.1 CE, la autodeterminación informativa[133] tiene un doble carácter. Desde su dimensión subjetiva, atribuye a la persona interesada el control sobre la propia

---

[132] ÁLVAREZ CIENFUEGOS SUÁREZ, J. M.: "El derecho a la intimidad personal, la libre difusión de información y el control del Estado sobre los bancos de datos", *Actualidad Administrativa,* núm. 37, 1999, págs. 457-465.

[133] La fórmula autodeterminación informativa, acuñada, como ya vimos, por el Tribunal Constitucional Federal alemán en su sentencia de 15 de diciembre de 1983, refleja, precisamente, la autonomía y el control sobre la información personal que afecta al individuo. Hay autores que prefieren la expresión libertad informática porque permite aproximarse más al contenido de las facultades que tiene el sujeto sobre sus datos, pues la libertad puede entenderse como libertad de control de los datos personales que queda garantizada constitucionalmente frente al poder del Estado y sus órganos y frente a los particulares. *Vid*. ORTÍ VALLEJO, A.: *op. cit.,* pág. 330-331. También Pérez Luño habla de libertad informática, al entender que con estos términos se acentúa la dimensión subjetiva que reviste la protección de las personas frente a determinados usos de las nuevas tecnologías. *Vid.* PÉREZ LUÑO, A. E.:" Los derechos humanos en la sociedad tecnológica" en AA.VV.: *Libertad informática y leyes de protección de datos personales*, Cuadernos y Debates, núm. 21, Centro de Estudios Constitucionales, Madrid, 1989, págs. 139-140.

información personal, otorgándole un haz de facultades que consisten en el poder jurídico de imponer a terceros la realización o la omisión de determinados comportamientos. Pero, desde el punto de vista objetivo, al propio tiempo, como señala Troncoso Reigada, la protección de datos personales "es un elemento esencial y objetivo que afecta al conjunto de la sociedad y concierne a la calidad de una democracia que demanda ciudadanos libres y con capacidad de decisión. Existe un interés público en el respeto a la protección de datos personales al ser también un instituto de garantía de otros derechos fundamentales, de tal manera que protegiendo los datos personales frente a los tratamientos estamos protegiendo al mismo tiempo el ordenamiento constitucional[134]".

La Carta de Derechos Fundamentales de la Unión Europea es el documento que más ha permitido avanzar en la definición y concreción del contenido esencial del derecho a la protección de datos personales, desde una perspectiva materialmente constitucional. Dentro del capítulo II "De las Libertades", contempla por separado el derecho al respeto a la vida privada y familiar (art. 7) y el derecho a la protección de datos de carácter personal (art. 8). Este último establece que: "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

[134] TRONCOSO REIGADA, A.: *Comentarios a la Ley Orgánica de Protección de datos de carácter personal*, Thomson Reuters-Civitas, Madrid, 2010, págs. 73-74.

y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

Este precepto tiene sus antecedentes en el Convenio 108 del Consejo de Europa. Al igual que ocurrió con este instrumento, las pautas que emergen de la Carta nos van a permitir delimitar el contenido esencial del derecho por la vía de la interpretación. Como ha declarado el Tribunal Constitucional, "la Carta de Derechos Fundamentales de la Unión Europea …cuyo artículo 8 reconoce este derecho, precisa su contenido y establece la necesidad de una autoridad que vele por su respeto… todos estos textos internacionales coinciden en el establecimiento de un régimen jurídico para la protección de datos personales en el que se regula el ejercicio de este derecho fundamental en cuanto a la recogida de tales datos, la información de los interesados sobre su origen y destino, la facultad de rectificación y cancelación, así como el consentimiento respecto para su uso o cesión. Esto es, como antes se ha visto, un haz de garantías cuyo contenido hace posible el respeto de este derecho fundamental"[135].

El artículo 8 de la CDFUE y el artículo 16 del TFUE[136] constituyen el fundamento de la nueva regulación en el ámbito de la Unión Europea. Actualmente, dicha regulación se concreta en el Reglamento General de

[135] STC 292/2000, FJ 8.

[136] Artículo 16 TFUE: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. 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. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea." *Vid.* DOUE C-202, de 7 de junio de 2016.

Protección de Datos de 4 de mayo de 2016, que no será de aplicación a los tratamientos de datos personales relacionados con actividades en las que la Unión Europea no tiene competencias[137].

Por consiguiente, habrá que tener en cuenta esta circunstancia para trazar dos regímenes jurídicos: uno más amplio, que en el ámbito de la Unión Europea está concretado hoy por el Reglamento General de Protección de Datos[138], que tiene como objetivo regular el derecho fundamental reconocido en el artículo 8 de la Carta, y por la LOPD y su Reglamento de desarrollo[139]. Y otro circunscrito a aquellos tratamientos de datos personales que quedan fuera del ámbito de aplicación del Derecho de la Unión, donde regirá la LOPD y su Reglamento de desarrollo[140]. Partiendo de estas premisas, y dada la complejidad de la exposición, se hará un tratamiento integrador indicando, en nota a pie, la fuente del derecho en la que nos hemos basado, atendiendo al esquema organizativo siguiente: normativa nacional y novedades que ha incorporado la aprobación del reciente RGPD.

---

[137] Artículo 2.2 RGPD. Entre estas actividades señala Uriarte Landa la seguridad nacional *vid*. URIARTE LANDA, I.: "Ámbito de aplicación material" en AA.VV.: *El Reglamento general de protección de datos hacia un nuevo modelo europeo de privacidad,* Reus, Madrid*,* 2017, pág. 66. También quedan fuera de su ámbito de aplicación material las actividades de política exterior y seguridad común que llevan a cabo los Estados miembros [art. 2.2.b) RGPD].

[138] Sin perjuicio del Reglamento (CE) nº 45/2001 y la Directiva 2000/32/CE y demás normativa sectorial. *Vid.* artículos 2.3 y 4 RGPD.

[139] Como acertadamente explica Troncoso Reigada, "el Reglamento general de protección de datos personales tendrá un alcance general, será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro por lo que su aprobación desplaza a la normativa española de protección de datos personales, en especial, a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (LOPD), y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RPDP), -así como a la legislación autonómica y a su normativa reglamentaria desarrollo-… que sean incompatibles con el Reglamento de la Unión Europea. Sin embargo, los poderes públicos, tanto el Legislador como el Gobierno, tienen la obligación, por razones de seguridad jurídica, de derogar las normas de Derecho interno incompatibles con el Derecho de la Unión". *Vid*. TRONCOSO REIGADA, A.: "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *REDE*, núm. 43, 2012, pág. 27.

[140] *Vid,* sobre el ámbito de aplicación territorial y material, el artículo 2 LOPD y los artículos 2, 3 y 4 RLOPD.

En primer lugar, la protección de datos personales se garantiza a todas las personas físicas, nacionales o extranjeras, mayores o menores de edad. Como señala la STC 17/2013, FJ 4: "es evidente que los extranjeros han de ser considerados titulares del mismo, tal como este derecho fundamental ha sido reconocido por el legislador orgánico, el cual no distingue entre españoles y extranjeros en dicho reconocimiento. Debe recordarse, asimismo, que la Carta de los derechos fundamentales de la Unión Europea recoge, en su artículo 8, el reconocimiento al derecho a la protección de datos, lo que también hace el Convenio núm. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal".

Este derecho, por su estrecha vinculación con la dignidad humana y el libre desarrollo de la personalidad (art. 10.1 CE), de acuerdo con la doctrina del Tribunal Constitucional emanada de la STC 236/2007, pertenece a la persona en cuanto a tal, y no como ciudadana. Será sujeto protegido en iguales condiciones toda persona física titular de los datos que sean objeto de tratamiento cuya identidad pueda determinarse directa o indirectamente[141], con

[141] Así resulta del artículo 3. a) LOPD, que añade "mediante cualquier información referida a sus circunstancias física, fisiológica, psíquica, económica, cultural o social". Según el artículo 5.1.o) RLOPD una persona física no se considerará identificable si dicha identificación requiere de plazos o actividades desproporcionadas. Conforme al artículo 2.3 RLOPD quedan fuera de su ámbito de aplicación los tratamientos de datos referidos a personas físicas que presten sus servicios en personas jurídicas consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. De este modo, cualquier tratamiento que contenga datos adicionales a los citados se encontrará plenamente sometido a la Ley Orgánica 15/1999, por exceder de lo meramente imprescindible para identificar al sujeto en cuanto contacto de quien realiza el tratamiento con otra empresa o persona jurídica. Por ello, no se encontrarían excluidos de la Ley los ficheros en los que, por ejemplo, se incluyera el dato del documento nacional de identidad del sujeto, al no ser el mismo necesario para el mantenimiento del contacto empresarial. Igualmente, se encuentran sujetos a la Ley Orgánica los ficheros del empresario respecto de su propio personal cuya finalidad sea el ejercicio de las potestades de organización y dirección que a aquel atribuyen las leyes. *Vid.* artículo 2 RLOPD.

independencia de su nacionalidad y, en el caso de extranjeros, de su situación administrativa.

En este mismo sentido se pronuncia la Carta de Derechos fundamentales al comenzar el reconocimiento del derecho con las palabras "toda persona". Según el RGPD[142], se considerará persona física identificable toda persona cuya identidad pueda identificarse 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 genética.

En términos generales quedan excluidos los datos personales de personas fallecidas. No obstante, la normativa española venía disponiendo que las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan los datos de este con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos[143]. En el mismo sentido, la Ley de Autonomía del Paciente[144] establece la posibilidad de que personas vinculadas a los pacientes fallecidos puedan tener acceso a la historia clínica, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. El RGPD sigue esta línea, si bien los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de las personas fallecidas[145].

---

[142] *Vid.* artículo 4.1) RGPD.
[143] *Vid.* artículo 2.4 RLOPD.
[144] *Vid.* artículo 18.4 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
[145] *Vid.* considerando 27 del RGPD.

Respecto a las personas jurídicas, la LOPD[146] excluye de su ámbito de aplicación sus datos sobre la base de que son públicos, puesto que constan en diferentes Registros, como el mercantil o el de cooperativas. Ahora bien, lo cierto es que también los datos públicos son objeto de este derecho fundamental, sin perjuicio de que, además, pueda haber datos que las personas jurídicas quieran mantener de forma reservada bajo su control. Así, Lucas Murillo de la Cueva afirma que "en estos casos lo que se estaría tutelando no sería la posición de un organismo abstracto, sino la propia de los individuos concretos que la integran"[147]. Tanto es así, que el tratamiento de sus datos puede afectarles igual que si se tratara de una persona física. En tales casos, a la luz de nuestro ordenamiento, las personas jurídicas podrán recurrir a la vía judicial civil o penal[148] para proteger sus datos, pero no podrán hacer uso de los derechos acceso, rectificación, cancelación y oposición ante la AEPD. Por su parte, el RGPD ha excluido expresamente el tratamiento de datos personales de las personas jurídicas[149].

Especial mención merecen los menores de edad. En la normativa española, pueden prestar el consentimiento para el tratamiento de sus datos

---

[146] *Vid.* artículos 1 y 3.a) y e) LOPD y artículo 2.2 RLOPD. En nuestro ordenamiento, es doctrina constitucional que pueden las personas jurídicas pueden ser titulares de derechos fundamentales en tanto que los mismos sean compatibles con su naturaleza, como enuncia, por ejemplo, la STC 23/1989, FJ 2.

[147] LUCAS MURILLO DE LA CUEVA, P.: *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992 de regulación del Tratamiento automatizado de datos de carácter personal),* Colección Cuadernos y Debates, núm. 43, Centro de Estudios Constitucionales, Madrid, 1993, pág. 51.

[148] Protección del derecho al honor o delito de descubrimiento o revelación de secretos.

[149] *Vid.* considerando 14 del RGPD. El ordenamiento jurídico otorga un amparo especial a cierto tipo de datos concernientes a las empresas, principalmente bajo la figura de la confidencialidad, que impide el acceso a los mismos de terceras personas, dado que los datos empresariales o comerciales constituyen un elemento esencial de la libertad de empresa, e, incluso, de garantía de la competitividad en el mercado. *Vid,* CANALS AMETLLER, D.: "El acceso público a datos en un contexto de transparencia y de buena regulación" en CANALS AMETLLER, D. (ed.): *Datos. Protección, Transparencia y Buena Regulación,* Documenta Universitaria, Girona, 2016, pág. 16.

personales a partir de los catorce años, excepto en los casos en que la ley prevea expresamente otra cosa, siempre que el tratamiento de datos no implique la comunicación relativa a sus familiares. En caso de menores de catorce años, los padres o tutores habrán de prestar el consentimiento. El Reglamento europeo regula expresamente la protección de sus datos personales prestándole una singular atención[150], al contemplar las condiciones aplicables a su consentimiento en el ámbito de los servicios de la sociedad de la información.

Respecto a los sujetos pasivos, deben entenderse obligados por este derecho no solo los poderes públicos, sino también los particulares. En relación con los primeros, el Tribunal Constitucional afirma que el derecho a la protección de datos impone a los poderes públicos la prohibición de que los individuos se conviertan en fuentes de información sin las debidas garantías y también les impone el deber de prevenir los riesgos del acceso o divulgación indebidos de dicha información[151].

En segundo término, conviene aclarar el concepto de datos personales. Podríamos definirlo como toda información sobre una persona física identificada o identificable[152]. En definitiva, los datos objeto de protección son aquellos que reflejan características, hábitos y opciones vitales de las personas, útiles para identificarlas. Este derecho amplía la protección que otorga el derecho a la intimidad, al abarcar no solo los datos íntimos, sino

[150] *Vid.* considerandos 38, 58, 65 y 75 y artículos 8, 6.1.f), 12.1, 40.2.g) y 57.1.b).
[151] STC 292/2000, FJ 6 y STC 151/2014, FJ 7.
[152] Artículo 3.a) LOPD y articulo 4.1) RGPD.

también cualquier dato que facilite la conformación de un perfil del sujeto, incluso públicos[153].

Con todo, cabe plantearse, como hace Guichot Reina, si ello no supone una expansión excesiva y desproporcionada que tiene efectos sobre el principio de transparencia, anudado al sistema democrático[154].

Desde el punto de vista objetivo, son objeto de tutela tanto los datos de carácter personal registrados en soporte físico susceptibles de tratamiento, como toda modalidad de uso posterior (automatizado o no) de estos datos por los sectores público y privado. Los datos abarcarían, por tanto, estas tres características:

-Cualquier información numérica, alfabética, grafica, fotográfica, acústica o de cualquier otro tipo[155]. El Reglamento europeo ha incluido los datos biométricos y los genéticos. Incluso las direcciones de localización que tenemos en Internet o en un dispositivo y las cookies cuando van asociadas a personas serían datos personales a estos efectos, porque pueden dejar huellas que pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas[156].

-Concerniente a personas físicas, independientemente de su nacionalidad o de su lugar de residencia.

---

[153] *Vid.* opinión sobre el concepto de datos personales del Grupo de Trabajo del artículo 29, 4/2007, pág. 10. Y la STJUE de 7 de mayo de 2009, asunto C-553/07, Rijkeboer, párrafos 42 y 43, que distingue entre los datos principales y la información relativa a los datos principales.
[154] GUICHOT REINA, E.: *op. cit.,* pág. 173.
[155] *Vid.* artículo 5.1.f) del RLOPD.
[156] *Vid.* considerando 30 RGPD. El Reglamento europeo viene a recoger las nuevas formas de identificar a las personas desarrolladas por la tecnología. A estos efectos, consúltese el dictamen 4/2007, del Grupo de Trabajo del artículo 29 sobre el concepto de datos personales. La Directiva creó este Grupo a través de su artículo 29. Con la entrada en vigor del RGPD, sus funciones serán asumidas por el Comité Europeo de Protección de Datos.

-Identificadas o identificables. Por contra, no sería dato de carácter personal aquel que no permitiera la identificación del afectado, lo que se denomina dato disociado[157]. Pero no es lo mismo la información anónima que los datos personales seudonimizados a los que alude el Reglamento europeo, que mantienen por separado la información adicional que serviría para identificar a una persona concreta[158].

Dentro de los datos de carácter personal, merecen una consideración especial los datos relacionados con la salud, es decir, las informaciones relativas a la salud pasada, presente, futura, física o mental de un individuo, incluida la prestación de servicios de atención sanitaria, que revelen información sobre el estado de salud del afectado[159].

El tercer aspecto relevante a los efectos del derecho que analizamos es el concepto de tratamiento de los datos personales. La normativa española se

---

[157] *Vid.* artículo 5.1.e) RLOPD.

[158] *Vid.* considerandos 26, 28 y 29 y artículo 4.5) RGPD. El Dictamen 05/2014 del Grupo de Trabajo sobre Protección de Datos del artículo 29, al tratar sobre técnicas de anonimización, afirma que "uno de los errores consiste en pensar que los datos seudonimizados son datos anonimizados.(…) los datos seudonimizados no constituyen información anonimizada, ya que permiten singularizar a los interesados y vincularlos entre conjuntos de datos diferentes. La probabilidad de que el seudoanonimato admita la identificabilidad es muy alta; por ello, entra dentro del ámbito de aplicación del régimen jurídico de la protección de datos. Esto reviste una especial relevancia en el contexto de las investigaciones científicas, estadísticas e históricas" (pág. 11). Disponible en Internet: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinión-recommendation/files/2014/wp216_es.pdf.

[159] En particular se consideran datos relacionados con la salud de las personas los referidos al porcentaje de discapacidad y a su información genética [art. 5.1.g) RLOPD]. En el ámbito del Derecho de la Unión Europea, *vid.* considerando 35 del RGPD, que aclara que, en particular, se incluye entre los datos personales relativos a la salud 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; todo número, símbolo o dato asignado a una persona física que la identifique de manera univoca 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 de 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 un una prueba diagnóstica *in vitro*".

aplica tanto al tratamiento total o parcialmente automatizado, como al tratamiento no automatizado de datos personales, contenidos o destinados a ser incluidos en un fichero[160]. El RGPD, en un sentido muy amplio, define el tratamiento como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no", y utiliza como ejemplos "la recogida, registro, organización, estructuración, conservación adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"[161]. Una de las novedades que aporta la norma europea es la eliminación de la obligación de notificar los ficheros a la autoridad de control competente. En su lugar, cada responsable deberá llevar un registro interno de las actividades efectuadas en el tratamiento de datos que deberá contener la información que hasta ahora había que incluir al notificar los ficheros[162].

---

[160] *Vid.* artículo 3.c) de la LOPD y artículo 5.1.t) del RLOPD. En cuanto a los tipos de ficheros, la LOPD y el Reglamento distinguen entre ficheros de titularidad pública, de titularidad privada, ficheros no automatizados y ficheros temporales. El régimen de protección de datos de carácter personal de la LOPD no será de aplicación a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas, es decir, los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares; a los ficheros sometidos a la normativa sobre protección de materias clasificadas; y a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. En relación con los libros de bautismo, la jurisprudencia del Tribunal Supremo, desde la STS de 19 de septiembre de 2008, ha afirmado que "los datos personales recogidos en los libros de bautismo no son un conjunto organizado, tal y como exige el artículo 3.b) de la Ley Orgánica 15/99, sino que resultan una pura acumulación de éstos que comporta una difícil búsqueda, acceso e identificación, en cuanto no están ordenados, ni alfabéticamente, ni por fecha de nacimiento, sino solo por las fechas de bautismo, siendo absolutamente necesario el conocimiento previo de la parroquia donde aquel tuvo lugar, no resultando además accesibles para terceros distintos del bautizado, que no podrían solicitar ajenas partidas de bautismo".

[161] *Vid.* artículo 4.2) RGPD.

[162] *Vid.* artículo 30 RGPD.

Entre las figuras que pueden intervenir en el tratamiento o comunicación de los datos de carácter personal, merece la pena destacar las figuras del responsable del tratamiento y el encargado del mismo. Tanto la normativa española como la europea[163] definen al responsable como la persona física o jurídica, autoridad pública servicio u otro organismo que solo o conjuntamente con otros determine la finalidad y medios del tratamiento de datos. Por su parte, el encargado es la persona física o jurídica, autoridad pública servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento o del fichero, mediante una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación del servicio[164].

3.1. Principios.

La definición del tratamiento de datos personales comprende todo el camino que recorren los datos, desde su recogida u obtención y registro, hasta su posible supresión. La LOPD les dedica el Titulo II, en sus artículos 4 a 12,

---

[163] *Vid.* artículo 3.d) y g) LOPD y artículo 5.1.q) e i) RLOPD. En el ámbito europeo, *vid*. artículos 4.7) y 8) del RGPD. Sobre los buscadores de Internet y la determinación del responsable del tratamiento, consúltese la STJUE de 13 de mayo 2014, asunto C-131/12 - Google Spain y Google.

[164] *Vid.* sentencia de la Audiencia Nacional de 28 de septiembre de 2005, FJ 4: "lo típico del encargo de tratamiento es que un sujeto externo o ajeno al responsable del fichero va a tratar datos de carácter personal pertenecientes a los tratamientos efectuados por aquel con objeto de prestarle un servicio en un ámbito concreto..... Siendo esencial para no desnaturalizar la figura, que el encargado del tratamiento se limite a realizar el acto material de tratamiento encargado, y no siendo supuestos de encargo de tratamiento aquellos en los que el objeto del contrato fuese el ejercicio de una función o actividad independiente del encargado. En suma, existe encargo de tratamiento cuando la transmisión o cesión de datos está amparada en la prestación de un servicio que el responsable del tratamiento recibe de una empresa externa o ajena a su propia organización, y que ayuda en el cumplimiento de la finalidad del tratamiento de datos consentida por el afectado." Sobre el contrato u otro acto jurídico que vincule al encargado respecto al responsable; *vid*. en el ámbito europeo el artículo 28 RGPD.

concretamente los de calidad, información, consentimiento y seguridad. El párrafo segundo del artículo 8 de la CDFUE alude a los principios relativos al tratamiento, que, en definitiva, conforman el contenido esencial del derecho que estamos analizando. Estos se desarrollan en el Capítulo II del Reglamento europeo, concretamente en su artículo 5. Estos principios sirven como criterios de interpretación para todos los operadores jurídicos que intervienen en el tratamiento de datos de carácter personal. En este sentido, informan e integran la normativa de protección de datos y pueden ser útiles para rellenar las lagunas jurídicas que se produzcan como resultado de la imparable evolución tecnológica. En cada fase del tratamiento de los datos personales, puede que unos principios tengan más protagonismo que otros, sin perjuicio de que haya principios que informen todas las fases del mismo. En la normativa europea, además, se impone al responsable del tratamiento estar en condiciones de demostrar que cumple los principios aplicables a la protección de datos de carácter personal (responsabilidad proactiva)[165].

3.1.1. Transparencia y derecho a la información.

El derecho a la información al interesado resulta connatural al principio de transparencia, que hoy recoge ampliamente el Reglamento europeo. La transparencia forma parte de la esencia del poder de control de la persona

[165] La denominada "accountability" por la que se exige una obligación proactiva y sistemática del cumplimiento de la normativa de protección de datos a través de la implantación de medidas técnicas y organizativas mucho más exigentes a las que se vienen practicando con la actual normativa. Como ejemplo, las evaluaciones de impacto y la protección de datos desde el diseño y por defecto. *Vid*. artículos 5.2, 24 y 25 RGPD.

sobre sus datos. Es decir, poca virtualidad práctica tendrán las facultades que atribuye el derecho a la autodeterminación informativa, si se desconoce quién y para qué tiene nuestros datos, o si antes no se ha tenido conocimiento de las irregularidades cometidas con la información registrada[166].

El poder de disposición que un individuo tiene sobre sus datos personales se manifiesta en la capacidad para consentir o rechazar un tratamiento de los mismos, decisión que solo podrá tomar si se le ha informado previamente. El deber de informar se conecta con el poder de disposición a través del consentimiento, incluso si el tratamiento no se apoya en esta base jurídica. En ese caso, para que sea efectivo el poder de disposición a través de la posibilidad de ejercer los derechos ARCO (acceso, rectificación, cancelación y oposición), hoy acceso, rectificación, supresión, limitación, portabilidad y oposición -en adelante ARSLPO- se requiere que previamente se haya suministrado a la persona información acerca del tratamiento[167]. En concreto, el derecho a la información forma parte del núcleo esencial del derecho fundamental a la protección de datos, lo que no impide que por ley pueda ser limitado[168].

La información expresa, precisa e inequívoca ya se venía exigiendo en la LOPD, si bien con el Reglamento esta obligación se ha vuelto más extensa. La norma española se refiere a la información como un derecho del interesado

---

[166] HERRANZ ORTIZ, A.: *op. cit.,* pág. 88.

[167] Como consecuencia del Reglamento Europeo, a los derechos ARCO hay que añadir los derechos a la limitación del tratamiento y a la portabilidad de los datos personales, además de la desaparición del término cancelación, que ha sido sustituido por el derecho de supresión o derecho al olvido. *Vid.* HERNÁNDEZ CORCHETE, J .A.: "Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos", en AA.VV.: *El Reglamento General de protección de datos*…, pág. 214.

[168] STC 29/2013, FFJJ 7 y 8.

y lo regula como un deber del responsable del tratamiento que deberá realizarse de forma previa, esto es, al tiempo de la recogida de los datos de carácter personal[169]. El cumplimiento de esta obligación no solo permite el consentimiento del afectado, sino también facilita el ejercicio del haz de facultades que el derecho comporta. Este deber es una garantía esencial[170] del

[169] Artículo 5 LOPD: "1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. 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. 2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior. 3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, este deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo. 5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o de organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten." *Vid*. también artículos 153 a 156 RLOPD. No procede esta obligación de información cuando esta afecte a la Defensa Nacional, a la Seguridad Pública o a la persecución de infracciones penales (art. 24.1 LOPD).

[170] En la STC 292/2000, entre los motivos de inconstitucionalidad que planteó el Defensor del Pueblo, destacan las limitaciones al principio de información, pues, si bien era legítima la excepción cuando ésta afectara a la defensa nacional, la seguridad pública o la persecución de infracciones penales, no lo era en los restantes casos. En este sentido, no cabe eximir a la Administración de cumplir con el deber de información cuando afecte al "interés público", o impida o dificulte gravemente la "función de control y verificación" de las Administraciones públicas, o cuando afecte a "la persecución de una infracción administrativa" o se trate de proteger "intereses de terceros más dignos de protección". Tales fórmulas reflejan tal grado de indeterminación que dejan un amplio margen a la discrecionalidad de la Administración Publica para conceder o denegar el principio de información en los tratamientos. A juicio del Tribunal

derecho fundamental a la protección de datos, pues estamos, de hecho, ante el único momento donde el interesado toma conciencia de que existen tratamientos de sus datos personales, ya que es poco frecuente el recurso al derecho de acceso.

El alcance del derecho de información ha sido una cuestión polémica desde el punto de vista constitucional en materia de videovigilancia laboral. En las SSTC 98/2000 y 186/2000[171] había sido tratado este asunto desde la perspectiva del derecho a la intimidad. Con el reconocimiento del derecho fundamental a la protección de datos, la jurisprudencia experimentó un cambio de orientación. Así, el Tribunal Constitucional recuerda que la imagen es un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la LOPD, que establece que "cualquier información concerniente a personas físicas identificadas o identificables", y, por ello, considera como dato de carácter personal la información gráfica o fotográfica. Es evidente, entonces, que para el almacenamiento en ficheros, uso y tratamiento de la imagen, deben observarse los principios que conforman el contenido esencial de este derecho y, en particular, el de información.

Constitucional, la LOPD se había extralimitado al ampliar las excepciones al principio de información más allá de lo que permitían las normas internacionales. El principio de información tiene una extraordinaria importancia para conocer la existencia de un tratamiento de nuestros datos personales y para el ejercicio del derecho de acceso, por lo que suprimir estas facultades o principios equivale a vaciar de contenido efectivo el derecho fundamental.

[171] En la STC 98/2000 se cuestionaba si la instalación por la empresa Casino de la Toja de un sistema de captación y grabación de sonido en determinadas zonas del centro de trabajo, en concreto la caja y ruleta francesa, había vulnerado el derecho a la intimidad personal del trabajador, consagrado en el artículo 18.1 CE. La STC 186/200 trajo causa de la admisión en un proceso por despido, como prueba de cargo, de las grabaciones de video presentadas por la empresa. *Vid.* JIMÉNEZ-CASTELLANOS BALLESTEROS, I.: "Videovigilancia laboral y derecho fundamental a la protección de datos", *TEMAS LABORALES*, núm. 136, 2017, págs. 133-134.

La STC 29/2013[172] toma como punto de referencia la STC 292/2000 para concluir que el derecho a la información, esto es, la facultad de saber quién dispone de los datos y a qué uso los está sometiendo, es un elemento caracterizador de la definición constitucional del derecho fundamental a la protección de datos personales del artículo 18.4 CE, en su núcleo esencial. Por tanto, es exigible, incluso, cuando existe habilitación legal para recabar datos sin necesidad del consentimiento del titular, como ocurre en el ámbito laboral. La STC 39/2016[173], sin embargo, supone una relajación del rigor, en relación con la exigencia del derecho a ser informado que hasta entonces había mantenido el Alto Tribunal. Aun reiterando la importancia del derecho a la información como contenido esencial del derecho a la autodeterminación informativa, considera suficiente cumplir lo establecido en una Instrucción de la AEPD, es decir, la colocación de un distintivo informativo en la zona objeto de control. Por consiguiente, considerando adecuada una actuación de videovigilancia así establecida, sobre la base de la finalidad de que el empresario obtenga prueba de las irregularidades cometidas por el trabajador, se legitiman controles ocultos que, en nuestra opinión, y como pusieron de

[172] En esta ocasión, el recurrente en amparo prestaba sus servicios en la Universidad de Sevilla. Ante las sospechas de irregularidades en el cumplimiento de su jornada laboral, el director de recursos humanos de esta institución dispuso que se emplearan las cámaras de video instaladas en la entrada del recinto para el control de acceso de personas con el fin de controlar el desempeño de la relación laboral de aquel. La instalación de estas cámaras estaba advertida con la debida señalización. *Ibidem,* pág. 136

[173] La empresa, a raíz de la instalación de un sistema de control informático de caja, había detectado irregularidades contables en la tienda donde prestaba servicios la recurrente en amparo. Ante la sospecha de una apropiación dineraria indebida por parte de alguno de los trabajadores, la entidad había encargado a una compañía de seguridad el establecimiento de un sistema de videovigilancia. Al comprobarse, a través de la cámara situada en la tienda y que controlaba la caja, que la trabajadora había sustraído dinero, fue despedida por transgresión de la buena fe contractual. De la instalación de la cámara había dejado constancia un distintivo informativo en un lugar visible del escaparate del establecimiento, pero no se había comunicado previamente a los trabajadores. *Ibidem*, pág. 141.

manifiesto los votos particulares a la citada sentencia, lesionan el derecho fundamental del trabajador.

El principio de transparencia requiere que toda información y comunicación relativa al tratamiento de datos personales sea fácilmente accesible. Este requisito ha sido potenciado por el RGPD[174] hasta el punto de que se exige que toda la información dirigida al público o al interesado sea concisa y fácil de entender, que se utilice un lenguaje claro y sencillo, y, en su caso, que se visualice. Se hace especial énfasis en que, cualquier información o comunicación cuyo tratamiento vaya dirigido a un menor de edad deberá cumplir estos mandatos. La información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto[175].

En la normativa europea se amplía el volumen de información que se debe facilitar a los afectados tanto si los datos se obtienen del interesado, como si se obtienen de otra fuente[176]. Así, en el primer caso, a diferencia de la ley orgánica, el RGPD exige el cumplimiento de esta obligación en el momento

---

[174] *Vid*. artículo 58 RGPD y, en el mismo sentido, su considerando 39.

[175] Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente, *vid*. considerando 60 del RGPD. La información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público mediante un sitio web. Ello es especialmente pertinente, en la práctica, cuando la complejidad tecnológica haga difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es el caso de la publicidad en línea.

[176] Cuando los datos personales no se hayan obtenido del interesado, el momento de proporcionar la información deberá ser dentro de un plazo razonable desde la obtención y, a más tardar, dentro de un mes. O bien, si es anterior, al tiempo de comunicar los datos tratados al interesado o terceros. El responsable del tratamiento le facilitará, además de las circunstancias anteriormente mencionadas, información de las categorías de datos personales de que se trate y de la fuente de la que proceden los datos personales, especificando, en su caso, si proceden de fuentes de acceso público. *Vid*. artículos 14.2 y 3 RGPD.

en que los datos se obtienen y no con carácter previo[177]. En cuanto al contenido, además de lo previsto en la normativa española, esto es, básicamente, la identidad del responsable y los fines del tratamiento, el responsable deberá facilitar al afectado información complementaria para garantizar un tratamiento leal y transparente[178]. Sin embargo, no terminan ahí las exigencias relativas a la información que se debe suministrar. También deberá indicarse el plazo de conservación de los datos o los criterios para determinarlo y se mantiene la necesidad de informar sobre la posibilidad del ejercicio de los derechos ARSLPO[179]. El responsable podrá obviar la información de todos los anteriores elementos cuando el interesado ya disponga de ella. Por otra parte, el responsable del tratamiento que proyecte tratar los datos para una finalidad distinta de aquella para la que se recogieron

[177] *Vid.* artículo 5.1 LOPD, en relación con el artículo 13.1 RGPD.

[178] *Vid*. artículos 13 y 14 RGPD. Entre los aspectos sobre los que se ha de informar destaca, además de la mención a los datos de contacto del delegado de protección de datos, la base jurídica del tratamiento que ha de acompañar a los fines del mismo. De igual forma, se añade la alusión a las categorías de destinatarios de los datos y los intereses legítimos del responsable o de un tercero, cuando esta sea la base jurídica que ampara el tratamiento. Asimismo, se informará de la pretensión del responsable de llevar a cabo transferencias internacionales de datos, ya sea a un tercer país o a una organización internacional, así como de la existencia o no de decisión de adecuación de la Comisión Europea o, en el caso de transferencias mediante garantías adecuadas, de normas corporativas vinculantes o de ausencia de estas condiciones existentes, la referencia a tales garantías y a los medios de obtener copia de ellas o al hecho de que se hayan prestado.

[179] Completan este cuadro otras informaciones, como la posibilidad de retirar el consentimiento cuando el tratamiento esté basado en el mismo y el derecho a presentar una reclamación ante la autoridad de control (actualmente la AEPD, la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía). Además, habrá que advertir si la comunicación de datos personales es un requisito legal, contractual o necesario para suscribir un contrato y si el interesado tiene la obligación o no de facilitar sus datos personales y las posibles consecuencias de no facilitarlos, e, incluso, la existencia o no de decisiones automatizadas, incluyendo la elaboración de perfiles y, al menos, información significativa de la lógica aplicada y la importancia y consecuencias que se prevén para el interesado en relación con dicho tratamiento.

debe proporcionar al interesado, antes de dicho tratamiento ulterior, información al respecto[180].

No obstante, no será necesario cumplir con la obligación de informar[181] cuando el interesado ya disponga de ella, o bien cuando la comunicación resulte imposible o exija esfuerzos desproporcionados. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adoptadas. Esta excepción operará, en particular, cuando el tratamiento persiga fines de archivo en interés público, de investigación científica o histórica, o bien fines estadísticos[182]. Tampoco habrá que informar cuando el Derecho de la Unión o de los Estados miembros expresamente prevea la obtención o la comunicación, o cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional[183]. La exigencia del deber de información se debe a que el legislador europeo, como señala Hernández Corchete, reconoce que, en un entorno tecnológico complejo, el mero cumplimiento por el responsable de los indicados deberes no garantiza de un modo efectivo que el interesado sea consciente de la lógica a que obedece el tratamiento de sus datos personales, de modo que crece su percepción de no tener un poder efectivo de disposición sobre ellos, lo que es particularmente grave porque amplios e importantes ámbitos de su actuar se materializan a través de cauces en los que quedan registrados sus datos personales[184].

---

[180] *Vid*. artículos 13.3 y 14.4 RGPD. En el mismo sentido, los considerandos 50 y 61.
[181] *Vid.* por todas, artículo 14.5 RGPD.
[182] *Vid*. artículo 14.5.b) RGPD. En el mismo sentido, considerando 62.
[183] Artículo 14.5.d) RGPD.
[184] HERNÁNDEZ CORCHETE, J.A.: *op. cit.,* pág. 207.

3.1.2. Consentimiento.

Los datos personales deberán ser tratados de manera lícita. La licitud del tratamiento implica, según el artículo 6 de la LOPD, que esta operación debe fundamentarse en alguna base jurídica, esto es, en el consentimiento del afectado, salvo que la ley disponga otra cosa.

Uno de los elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales es el derecho del afectado a consentir el tratamiento de los mismos[185]. El consentimiento es la garantía del poder de disposición de los datos personales por su titular, porque le faculta para decidir qué datos proporcionar a terceros o cuáles puede este tercero recabar. En definitiva, le faculta para controlar sus datos personales.

El tratamiento de los datos personales o su cesión requerirán con carácter general el consentimiento del interesado[186]. El consentimiento habrá de ser:

---

[185] STC 292/2000 y artículo 8.2 de la Carta de Derechos Fundamentales de la Unión Europea.

[186] Regulado en los artículos 6 y 11 de la LOPD y 10 a 17 del RLOPD. El responsable del tratamiento deberá tener en cuenta que "los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiere prestado previamente su consentimiento para ello" (art. 10.1 RLOPD). Según los artículos 6.2 LOPD y 10 RLOPD, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando el tratamiento o cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados, especialmente su honor y su intimidad personal o familiar; o bien cuando el tratamiento o cesión sean necesarios para que el responsable del tratamiento cumpla con un deber que le imponga una de dichas normas; cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato o de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; y cuando tengan por finalidad proteger una interés vital de interesado. *Vid.* STC 17/2013, sobre la cesión de datos

- Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno, en los términos regulados por el Código Civil. De acuerdo con el Reglamento europeo, 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[187].

- Específico, es decir, referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento.

- Informado, es decir, que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que aquel se produce. El interesado deberá conocer, como mínimo, la identidad del responsable del tratamiento y los fines a los cuales está destinado el tratamiento de los datos personales.

- Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado, siendo preciso que exista expresamente una acción que implique la existencia del consentimiento. No basta, por tanto, un consentimiento presunto.

La condición de inequívoco no significa que el consentimiento deba ser expreso en todo caso[188]. Importante novedad a este respecto incorpora el RGPD, al definir el consentimiento como "toda manifestación de voluntad, libre, específica, informada e inequívoca por la que el interesado acepta, *ya sea*

---

del padrón de habitantes cuando el titular es un extranjero y no dio su consentimiento para la cesión a un tercero para un tratamiento con fines distintos.

[187] *Vid*. considerando 42 RGPD.

[188] El artículo 14 RLOPD regula la forma de recabar y probar el consentimiento.

mediante declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen" (la cursiva es nuestra)[189].

El consentimiento, por tanto, debe darse mediante un acto afirmativo claro, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Si el consentimiento se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa, y no debe perturbar innecesariamente el uso del servicio para el que se presta. Por tanto, esto podría incluir marcar una casilla de un sitio web de Internet, escoger parámetros técnicos ("cookies") para la utilización de servicios de la sociedad de la información o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por el contrario, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Por consiguiente, cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos[190].

Para la AEPD, la normativa europea no admite formas de consentimiento tácito o por omisión, ya que se basan en la inacción[191]. Sin embargo, hay autores que opinan que la necesidad de que el responsable del tratamiento aplique medidas apropiadas a fin de garantizar que el tratamiento sea conforme con el RGPD, como exige el nuevo principio de responsabilidad

---

[189] Artículo 4.11) RGPD.
[190] *Vid.* considerando 32. El considerando 171 explica qué hacer con los tratamientos iniciados antes del 25 de mayo de 2018, fecha de la entrada en vigor del RGPD, que se basen en los requisitos de la Directiva 95/46/CE, ya derogada.
[191] *Vid.* Guía del Reglamento General de Protección de Datos para responsables de tratamiento, pág. 6. Disponible en Internet: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf

proactiva, implica que quienes recopilen datos deberán ser capaces de demostrar que el afectado, pudiendo manifestar su negativa, no lo ha hecho, entendiéndose, solo entonces, que ha dado su consentimiento de esta manera al tratamiento de datos de que fuera informado[192].

En la normativa española se contemplan situaciones en las que el consentimiento, además de inequívoco, ha de ser expreso: así ocurre en el tratamiento de datos sensibles[193]. Respecto a los datos relativos a la ideología, religión, creencias y afiliación sindical, la Ley exige que el consentimiento deba ser escrito y se advierta al interesado acerca de su derecho a no prestarlo, algo que es concreción del artículo 16.2 CE, según el cual "nadie podrá ser obligado a declarar sobre su ideología, religión o creencias". Ello, en particular, constituye una garantía de la protección de la libertad ideológica y religiosa y de la libertad sindical.

No será necesario recabar el consentimiento para el tratamiento de datos sobre la ideología utilizados por un partido político, sobre la religión o creencias, tratados por la iglesia o las distintas confesiones religiosas, y sobre la afiliación sindical, empleados por los sindicatos, siempre que se refieran a uno de sus miembros y dentro de sus respectivas finalidades. Sin embargo, la

---

[192] Artículo 24 RGPD y en el mismo sentido considerandos 74 y 78. *Vid.* PÉREZ CAMBERO, R.: "Análisis de las últimas e importantes novedades en protección de datos: Reglamento Europeo de Protección de Datos y Escudo de Privacidad UE- EE.UU", *AA,* núm. 11, 2016, pág. 5.

[193] *Vid.* artículos 7 y 8 LOPD y 10.5 RLOPD. Sin embargo esta regla tiene una excepción y este tipo de datos podrán ser objeto de tratamiento cuando este tenga por finalidad la protección del interés vital, es decir, para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea efectuado por un profesional sanitario o por persona sujeta igualmente al secreto profesional y si el objetivo del tratamiento fuera salvaguardar el interés vital del afectado o de otra persona en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento (art. 7.6 LOPD).

cesión de dichos datos ha de realizarse siempre con el consentimiento del afectado.

Por otra parte, la protección de los datos sobre la salud, origen racial y vida sexual responde a la garantía de los derechos al honor y a la intimidad personal, así como a evitar la discriminación. En vista de ello, estos datos solo podrán ser recabados, tratados o cedidos sin consentimiento del afectado en virtud de una habilitación legal[194]. Además, como regla general, se prohíbe la creación de ficheros con la finalidad exclusiva de recopilar cualquiera de los tipos de datos citados, para evitar que estas informaciones sean controladas con el único objetivo crear perfiles personales.

En relación con los datos sobre la salud, el Tribunal Constitucional, en aplicación de la concepción material de la intimidad, ha resuelto varios recursos de amparo sobre la vulneración de este derecho fundamental (art. 18.1 CE) prescindiendo en ocasiones de toda referencia al derecho fundamental a la protección de datos, al no haber sido alegado por el demandante de amparo

En la STC 202/1999, el Tribunal Constitucional sí tuvo en cuenta el derecho fundamental derivado del apartado cuarto del artículo 18 CE. El afectado denunció que en la entidad crediticia donde prestaba sus servicios existía una base de datos denominada “absentismo con baja médica" en la que figuraban datos sobre la salud de los empleados, sin el consentimiento expreso de estos y sin que la entidad hubiese alegado en ningún momento un interés

[194] En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud, cuando se realice para la atención sanitaria de las personas conforme a lo dispuesto en el Capítulo V de la Ley 16/2003 de 28 de mayo, de cohesión y calidad del sistema nacional de salud (art. 10.5 RLOPD).

contractual suficiente. El tratamiento y conservación en soporte informático de los datos atinentes a la salud del trabajador, prescindiendo del consentimiento expreso del afectado, constituye, a juicio del Tribunal Constitucional, una medida inadecuada y desproporcionada que conculca el derecho a la intimidad y a la libertad informática del titular de la información.

Por el contrario, en las SSTC 70/2009 y 159/2009, el Tribunal Constitucional prescinde de toda referencia al derecho fundamental a la protección de datos de carácter personal y la clave del otorgamiento del amparo se encuentra en el reconocimiento explícito de que el derecho a la intimidad comprende la información relativa a la salud física o psíquica de una persona, por cuanto se trata de una información íntima y especialmente sensible que requiere de una especial protección. La inclusión en el ámbito de protección del artículo 18.1 CE supone la facultad de excluir a terceros, así como la facultad de prohibir la revelación, divulgación o publicación no consentida de datos personales, apoyándose para ello, en ocasiones, en la STC 292/2000, en el Convenio 108 o en la Directiva 95/46/ CE.

En la STC 70/2009, estimó que existía vulneración del derecho a la intimidad del demandante de amparo, profesor de enseñanza secundaria, por las resoluciones administrativas que acordaron su jubilación forzosa por incapacidad permanente con fundamento en informes médicos emitidos por su psiquiatra particular que habían sido incorporados al expediente administrativo quebrando el derecho a la confidencialidad de la historia clínica. La sentencia afirma que "la información relativa a la salud física o psíquica de una persona, en suma, es no solo una información íntima (…), sino además especialmente sensible desde este punto de vista y por tanto digna de especial protección

desde la garantía del derecho a la intimidad (art. 6 del Convenio núm. 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, así como el art. 8 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos). El derecho a la intimidad queda así relevantemente afectado cuando, sin consentimiento del paciente, se accede a datos relativos a su salud o a informes relativos a la misma".

En la STC 159/2009, el recurrente fue excluido del proceso de selección para el ingreso en la categoría de agente de la escala básica de la Ertzaintza por estar afectado por una de las causas de exclusión contempladas en la convocatoria, en concreto, por padecer diabetes mellitus. Simultáneamente, participó en otro proceso de selección de 84 plazas de agentes de policía municipal de San Sebastián, y, tras superar el concurso-oposición y las pruebas médicas, realizó un curso de formación en la Academia de Policía Vasca que aprobó, siendo nombrado funcionario en prácticas. En ese período, uno de los facultativos integrantes del Tribunal médico del primer proceso selectivo reconoció al aspirante, y comunicó por teléfono a los servicios competentes del Ayuntamiento tal circunstancia, lo que finalmente comportó, tras la incoación de un expediente de expulsión del proceso selectivo de agentes de la policía local, la resolución de exclusión. A estos efectos, conviene advertir que los servicios médicos municipales se pusieron en contacto con la Directora de la Academia de Policía Vasca, la cual se negó a facilitar datos sobre la salud del recurrente por ser de carácter confidencial. De

hecho, los datos solicitados se encontraban en un fichero de datos de carácter personal, a los que una Orden de la Consejería de Interior del Gobierno Vasco atribuía un nivel alto de seguridad, y no podían facilitarse sin el consentimiento del afectado por imperativo de la LOPD. Al propio tiempo, no se practicaron nuevos reconocimientos médicos.

El recurso de amparo se fundamentó en el derecho fundamental a la intimidad. El Tribunal Constitucional reconoce que la información relativa al estado de salud de una persona forma parte del reducto de privacidad que garantiza el artículo 18.1 CE. Se trata de un dato íntimo que debe ser preservado del conocimiento ajeno[195].

El interesado prescindió de toda referencia al derecho fundamental a la protección de datos en la demanda de amparo. Esta circunstancia, unida al hecho de que el tratamiento de los datos gozaba de las garantías adecuadas, ya que la Directora de la Academia de Policía Vasca denegó la información solicitada por tratarse de datos especialmente protegidos que solo pueden

[195] STC 159/2009, FJ 3: "El derecho a la intimidad comprende la información relativa a la salud física y psíquica de las personas (STC 70/2009, FJ 2), quedando afectado en aquellos casos en los que sin consentimiento del paciente se accede a datos relativos a su salud o a informes relativos a la misma, o cuando, habiéndose accedido de forma legítima a dicha información, se divulga o utiliza sin consentimiento del afectado o sobrepasando los límites de dicho consentimiento. Dicha apreciación se cohonesta con nuestras pautas sociales, como lo demuestra el hecho de que en el ámbito de la legalidad ordinaria el acceso y el uso de información relativa a la salud se rodea de garantías específicas de confidencialidad, subrayándose la estrecha relación entre el secreto profesional médico y el derecho a la intimidad. También el Tribunal Europeo de Derechos Humanos, como recordamos en la ya citada STC 70/2009, ha insistido en la importancia que para la vida privada poseen los datos de salud (en este sentido, STEDH de 10 de octubre de 2006, caso L.L. c. Francia, párrafo 32), señalando que “el respeto al carácter confidencial de la información sobre la salud constituye un principio esencial del sistema jurídico de todos los Estados parte en la Convención”, por lo que “la legislación interna debe prever las garantías apropiadas para impedir toda comunicación o divulgación de datos de carácter personal relativos a la salud contraria a las garantías previstas en el artículo 8 del Convenio europeo de derechos humanos (SSTEDH caso Z. c. Finlandia, de 25 de febrero de 1997, párrafo 95, y caso L.L. c. Francia, de 10 de octubre de 2006, párrafo 44)”.

facilitarse con el consentimiento del afectado, llevaron al Tribunal Constitucional a eludir cuestiones subyacentes, como la cesión de datos sensibles entre Administraciones públicas que responden a la misma finalidad, en este caso, garantizar la competencia y aptitud de las fuerzas y cuerpos de seguridad en el ejercicio de sus funciones sin poner en peligro su seguridad o la de terceros (art. 104 CE). Como señala Guichot Reina, la *ratio decidendi* de esta sentencia fue la ausencia de procedimiento. Se hizo todo sin conocimiento del interesado y se dieron por buenos unos datos que no obraban en el expediente, no acordes con los reconocimientos médicos en el procedimiento de acceso a la policía local y no contrastados con nuevas pruebas. En mi opinión, la divulgación ilegítima de datos referentes a la intimidad personal, así como la vulneración del derecho fundamental a la protección de datos, al haberse tratado de un dato ilegítimamente divulgado y que constituía el único elemento determinante de una resolución administrativa que perjudicó al interesado, debieron haberse tenido en cuenta como fundamento de esta sentencia.

También tenemos ejemplos en la jurisprudencia constitucional sobre los datos relacionados con la ideología. El asunto resuelto por la STC 43/2009, tiene por objeto la impugnación del Auto de la Sala 61 del Tribunal Supremo por el que se declaran no conformes a Derecho y se anulan los acuerdos de las Juntas Electorales de los Territorios Históricos de Vizcaya, Guipúzcoa y Álava de proclamación de las candidaturas del partido político Askatasuna a las elecciones al Parlamento Vasco. Los recurrentes, integrantes de dichas candidaturas, invocaron violación del derecho a la intimidad en relación con los derechos a la libertad ideológica (art. 16.1 CE) y a participar en los asuntos

públicos por medio de representantes (art. 23.1 CE) sobre la base del tratamiento de sus datos personales que había llevado a cabo la policía y la guardia civil, sin su consentimiento. El Tribunal Constitucional, en relación con el derecho fundamental a la protección de datos, afirma en el fundamento jurídico duodécimo de la citada sentencia que "tal derecho persigue garantizar a las personas un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho afectado (STC 292/2000, FJ 6). Pero este poder de disposición no puede pretenderse con respecto al único dato relevante en este caso, a saber, la vinculación política de aquéllos que concurren como candidatos a un proceso electoral, pues, como hemos dicho, se trata de datos publicados a los que puede acceder cualquier ciudadano y que por tanto quedan fuera del control de las personas a las que se refieren. La adscripción política de un candidato es y debe ser un dato público en una sociedad democrática, y por ello no puede reclamarse sobre él ningún poder de disposición"[196].

La jurisprudencia constitucional[197] ha tenido también ocasión de pronunciarse sobre los datos genéticos, a propósito de una serie de casos en los que se planteaba la posible vulneración de los derechos a la intimidad personal y a la protección de datos a raíz de la condena penal del recurrente de amparo, sustentada en una prueba de ADN practicada irregularmente. En la demanda de amparo de la STC 135/2014, en relación con el derecho fundamental de autodeterminación informativa, se alegaba la necesidad del

[196] En el mismo sentido se pronuncian las SSTC 85/2003, FJ 21, 99/2004, FJ 13, 68/2005, FJ 15, y 110/2007, FJ 9.
[197] Sobre los datos relativos a muestras de ADN, SSTC 199/2013, 13, 14, 15 y 16/2014, 23/2014, 43/2014, y 135/2014.

consentimiento inequívoco del afectado[198], exigido en el artículo 6.1 de la LOPD. En este caso, para el Tribunal Constitucional, "resulta evidente que en las condiciones en las que se obtuvieron las muestras biológicas del detenido, esto es, sin mandamiento judicial, sin la presencia de su abogado y sin la presencia de un intérprete que le pudiera informar en su idioma del contenido, finalidad y trascendencia de la diligencia de intervención corporal que se le practicó, siendo por otro lado la finalidad que se hace constar en el acta distinta de la que se pretendía, no puede en absoluto considerarse que la policía contaba con el consentimiento libre, inequívoco, específico, informado y expreso del detenido para la recogida y tratamiento de sus datos genéticos de carácter personal". No hay que olvidar que en el acta de recogida de muestras de ADN se hizo constar por la policía que se informó al detenido de que dicha diligencia se realizaba tan solo a efectos identificativos, cuando lo cierto es que la finalidad de la misma era cotejar las muestras biológicas del recurrente con el ADN hallado en una prenda encontrada en el lugar de los hechos.

Sin embargo, el Tribunal Constitucional recuerda en la misma sentencia, tras reiterar la doctrina contenida en la STC 292/2000 sobre el derecho a la protección de datos, que ya en la STC 199/2013 se deja claro que el perfil de ADN obtenido a partir de una muestra biológica identifica a la persona, pero no puede decirse que incorpore otro tipo de datos que puedan contribuir a configurar una caracterización de la persona en sus aspectos "ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para

[198] Antecedente tercero.

el individuo" (STC 292/2000, FJ 6), lo cual constituye el ámbito de protección dispensada por el artículo 18.4 CE. En consecuencia, la sentencia resalta que en el caso tratado la identificación del demandante no se produjo como consecuencia de la incorporación de sus perfiles genéticos identificativos a una base de datos de personas sospechosas, sino que derivó de su comparación con los perfiles de ADN correspondientes a personas desconocidas que habían sido obtenidos a partir de muestras biológicas halladas en vestigios obtenidos con ocasión de unos hechos delictivos. Por lo demás, a juicio del Tribunal Constitucional, nada impediría al demandante reaccionar contra esta pretendida e hipotética conservación de sus perfiles de ADN solicitando su eliminación de la base de datos. Finalmente, la obtención de los caracteres identificativos del recurrente a partir del análisis su ADN se realizó para una finalidad constitucionalmente legítima, como es la investigación de un delito.

Pues bien, sobre la base de todo lo expuesto, el Tribunal Constitucional afirma que "el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los poderes públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución" (STC 292/2000, FJ 11)[199]. Además, el Alto Tribunal aprecia que tampoco consta que el perfil haya

[199] La normativa española contiene reglas especiales para los ficheros de las Fuerzas y Cuerpos de Seguridad (art. 22 LOPD). La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas está limitada a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al

sido utilizado para una finalidad distinta de aquella para la que se recogió, ni que haya sido objeto de cesión o tratamiento distinto de aquel para el que se obtuvo. Por todo ello, entiende que no hubo en el caso vulneración del derecho reconocido en el 18.4 CE.

Otros supuestos de tratamiento de datos sensibles en la jurisprudencia constitucional son los relativos a la afiliación sindical. Como ya tuvimos ocasión de analizar a propósito de la consagración del derecho a la protección de datos como autónomo respecto del derecho a la intimidad, en la relación de sentencias sobre este tema[200] se advierte de que se utilizó un dato sensible, que había sido proporcionado con una finalidad, para otra radicalmente distinta, con menoscabo del legítimo ejercicio de la libertad sindical y propiciando actitudes discriminatorias.

En referencia a los datos sensibles, la Unión Europea reconoce un margen de maniobra para que los Estados miembros especifiquen en sus normas el tratamiento de categorías especiales de datos personales.

El RGPD establece un régimen peculiar para algunos datos (art. 9), al prohibir el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física y datos relativos a la salud

---

efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad (art. 22.2 LOPD). Cuando sean los datos especialmente protegidos a que hacen referencia los apartados 2 y 3 del artículo 7 LOPD, la recogida y el tratamiento, y, por tanto, también la cesión, podrán realizarse en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o, en su caso, del control jurisdiccional.

[200]SSTC 11/1998, 33/1998, 35/1998, 45/1998, 60/1998, 77/1998, 94/199, 104/1998, 105/1998, 106/1998, 123/1998, 124/1998, 125/1998, 126/1998, 158/1998,198/1998, 223/1998, 30/1999, 44/1999, y 45/1999.

o datos relativos a la vida sexual o las orientación sexuales de una persona física. A esta regla general se le aplican algunas excepciones:

a) Si el interesado dio su consentimiento explícito para ello, salvo cuando esta posibilidad no esté prevista en el Derecho de la Unión o de los Estados miembros;

b) Si el tratamiento es necesario para atender las obligaciones laborales, siempre que esté autorizado por el Derecho de la Unión de los Estados miembros o por un convenio colectivo con arreglo al Derecho de los Estados miembros y se prevean las garantías adecuadas;

c) Si el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física y existe incapacidad física o jurídica para la prestación del consentimiento;

d) Si el tratamiento responde a la actividad legítima de una fundación, una asociación o similar, siempre que el tratamiento se refiera a los miembros o personas relacionadas y siempre que los datos personales no se comuniquen a terceros sin el consentimiento de los interesados;

e) Si el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) Si 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) Si el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros;

h) Si el tratamiento es necesario para fines de prestación de asistencia o tratamiento de tipo sanitario o social;

i) Si el tratamiento es necesario por razones de interés público en el ámbito de la salud pública[201];

j) Si el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

El repertorio de los supuestos en los que cabe el tratamiento de las categorías especiales de datos no constituye una lista cerrada. Por otra parte, los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, biométricos o relativos a la salud[202].

En el marco de la jurisprudencia del Tribunal de Justicia de la Unión Europea, en el caso Lindqvist, de 6 de noviembre de 2003[203], el Tribunal resolvió la cuestión de si los ficheros de datos religiosos podían excluirse del ámbito de aplicación de la Directiva 95/46/CE. En tal sentido, determinó que las actividades voluntarias o religiosas, como la que realizaba la señora Lindqvist, no pueden ser una excepción y, en consecuencia, entrarían dentro del marco de la normativa europea de protección de datos. El asunto tenía por objeto unas cuestiones prejudiciales planteadas al TJUE sobre la interpretación de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en el proceso penal seguido contra esta señora. La acusada era

[201] *Vid*. considerando 54 RGPD.
[202] Vid. artículo 9 del Proyecto de Ley de Protección de datos de 24 de noviembre de 2017.
[203] Sentencia del Tribunal de Justicia de la Unión Europea de 6 de noviembre de 2003, asunto C-101/01 – Lindqvist.

catequista y había sido inculpada por haber infringido la legislación sueca sobre la materia, al haber creado desde su domicilio y en su ordenador varias páginas web que contenían información sobre ella misma y varios feligreses (incluyendo nombre completo, situación familiar, número de teléfono e información adicional), sin haber informado ni solicitado el consentimiento a sus compañeros, ni haber comunicado la iniciativa a la autoridad competente. Lo más relevante de esta sentencia fue que perfiló la definición de datos personales, pero, a los efectos que ahora nos interesan, el Tribunal tuvo ocasión de pronunciarse sobre los datos relativos a la salud, al haberse publicado que uno de los catequistas, mencionados en la base de datos, sufría una lesión en el pie. Como deja claro el Tribunal de Justicia de la Unión Europea, en el Derecho de la Unión Europea está prohibido el tratamiento de esta categoría de datos, salvo las excepciones previstas en la normativa vigente.

En la sentencia del caso CN contra el Parlamento Europeo, de 3 de diciembre de 2015[204], el Tribunal de Justicia de la Unión Europea consideró que el demandante dio su consentimiento explícito para la divulgación en Internet de información sensible, concretamente relativa a su estado de salud. A la luz del Reglamento sobre protección de datos personales, en el tratamiento hecho por instituciones comunitarias[205] se desprende que, cuando el consentimiento tenga por objeto datos sensibles, debe ser explícito. En otras palabras, dicho

[204] Sentencia del Tribunal de Justicia de la Unión Europea en su formación de Tribunal General (Sala Sexta) de 3 de diciembre de 2015, T-343/13 - CN/Parlamento.

[205] Artículo 10, apartado 2, letra a), del Reglamento nº 45/2001, sobre 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. DOUE 12 enero 2001, núm. 8.

consentimiento debe ser expreso, sin que sea posible deducirlo implícitamente de las acciones de la persona de que se trate; por el contrario, cuando no se trate de datos sensibles, el consentimiento debe ser inequívoco, "dicho de otro modo, el tratamiento puede efectuarse cuando el interesado haya dado su consentimiento con certeza y sin ambigüedad"[206].

En la jurisprudencia del Tribunal Europeo de Derechos Humanos también encontramos referencias a datos sensibles. Destacamos el caso L.H. contra Letonia, resuelto por la sentencia de 29 abril 2014, en la que el citado Tribunal afirma que el respeto a la confidencialidad de los datos sobre la salud es un principio vital en los sistemas legales de todos las Partes de contratantes del Convenio[207]; y el caso LL. contra Francia, STEDH de 10 de octubre de 2006, donde se entendió que la divulgación de los datos médicos en un proceso de divorcio, a la vista del papel fundamental que juega la protección de los datos de carácter personal, no era proporcionada al fin perseguido y, por lo tanto, no era necesaria, en una sociedad democrática, para la protección de los derechos y libertades de los demás.

En relación con los datos biométricos, el Tribunal Europeo de Derechos Humanos, en la sentencia de 4 de diciembre de 2008, caso S y Marper contra Reino Unido, trata sobre la conservación en los registros policiales de las huellas dactilares, muestras biológicas y ADN de dos demandantes, después de ser absuelto uno de ellos y archivada la causa por los delitos de los que era

[206] Sentencia del Tribunal de Justicia de la Unión Europea en su formación de Tribunal General (Sala Sexta) de 3 de diciembre de 2015, T-343/13 - CN/Parlamento, párrafo 77.

[207] Sobre el carácter confidencial de la información sobre el estado de salud, *vid.* además, SSTEDH de 25 de febrero de 1997, caso Z contra Finlandia; de 17 de enero de 2012, caso Varapnickaite-Mazyliene contra Lituania; de 6 de junio de 2013, caso Avilkima y otros contra Rusia; de 15 de abril de 2014, caso Radu contra Republica de Moldavia y de 23 de febrero de 2016, caso YY contra Rusia.

sospechoso el otro recurrente. El Tribunal examinó si la conservación permanente de las huellas dactilares y los datos de ADN de todas las personas sospechosas, pero no condenadas, se funda en unos motivos pertinentes y suficientes, para concluir que se ha de considerar una limitación desproporcionada del derecho de los demandantes al respeto de su vida privada e innecesaria en una sociedad democrática.

Entre los datos especialmente protegidos cabe también mencionar los relativos a la comisión de infracciones penales o administrativas La LOPD dispone que solo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras[208]. En sentido similar, la normativa europea señala que el tratamiento de estos datos solo podrán llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros, siempre que se establezcan garantías adecuadas para los derechos y libertades de los interesados. En especial, solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas[209].

Por último, hay que hacer referencia, en relación con el principio del consentimiento, a que la normativa española reconoce en los tratamientos de datos basados en el mismo el derecho del interesado a retirarlo[210]. La revocación tiene dos limitaciones: que exista una causa justificada y que no se

[208] *Vid.* artículo 7.5 LOPD.
[209] *Vid.* artículo 10 RGPD.
[210] Artículo 6.3 LOPD.

le atribuyan efectos retroactivos. También se reconoce esta facultad en la cesión de datos[211].

El Reglamento General de Protección de Datos, sin embargo, ha superado el carácter restrictivo[212] que inspira a la norma española. Sobre este derecho proclama que "será tan fácil retirar el consentimiento como darlo". El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. El ejercicio de este derecho y su irretroactividad, así como los medios gratuitos para llevarlo a efecto, constituyen, de hecho, algunos de los contenidos necesarios de la información que debe de facilitarse al interesado para garantizar un tratamiento de datos leal y transparente[213].

Finalmente, especial atención presta el Reglamento a las condiciones del consentimiento cuando este va dirigido a menores de edad y a servicios de la sociedad de la información[214]. El tratamiento de datos personales de un menor se considerará lícito cuando aquel tenga como mínimo 16 años. Si fuera menor de esa edad, la licitud del tratamiento exigirá el consentimiento o la autorización del titular de la patria potestad o tutela. No obstante, los Estados miembros podrán establecer por ley una edad inferior, con el límite de los 13

---

[211] *Vid*. artículo 11.4 LOPD para la cesión, aunque no se sujeta a limitación. En cuanto al procedimiento, artículo 17 RLOPD.
[212] *Vid.* artículo 7.3 RGPD.
[213] *Vid.* artículo 13.2.c) RGPD.
[214] *Vid.* artículo 8 RGPD.

años[215]. En todo caso, el responsable del tratamiento deberá hacer esfuerzos razonables para verificar en estos casos el cumplimiento de este requisito.

3.1.3. Calidad de los datos.

La vida del dato como elemento que aporta información pasa por varias fases. Por tanto, el principio de calidad de los datos afecta a todo el proceso de su recogida y almacenamiento, de uso y conservación de la información y de supresión de datos del fichero. Como consecuencia, este principio se desglosa en el Reglamento europeo distinguiendo la limitación de la finalidad, la minimización de los datos, la exactitud, la limitación del plazo de conservación y la integridad y confidencialidad.

La determinación de la finalidad para la que se obtienen los datos constituye un requisito esencial que condiciona la recogida, cesión, conservación y supresión de la información. Los datos de carácter personal solo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento. La indicación de los fines del tratamiento es una condición que debe facilitarse por el responsable del tratamiento en el momento que estos se obtengan.

No valdrían finalidades vagas, inconcretas o tan generales que admitieran cualquier propósito, aunque fuera legítimo. Esto es así para que la

[215] Según la norma española, podrán prestarlos por sí mismos los mayores de 14 años (art. 13 RLOPD). El artículo 7 del Proyecto de Ley de Protección de Datos de 24 de noviembre de 2017 rebaja la edad a 13 años.

finalidad sea conocida por el titular de los datos y este pueda ejercer el control de la información personal y prestar su consentimiento.

La finalidad debe ser legítima. En los ficheros privados encuentra su límite en la Constitución y en la ley, admitiéndose prácticamente cualquier finalidad; sin embargo, en el ámbito de los ficheros públicos, la legitimidad tiene unos límites más restringidos, pues, para que la finalidad sea legitima, debe guardar relación con la competencia del órgano administrativo que recaba los datos[216].

Por otra parte, los datos personales no podrán ser utilizados para finalidades incompatibles con aquellas para las que los mismos se hubieran recogido. Por ejemplo, en el caso resuelto por la STC 11/1998, se emplearon los datos de afiliación sindical para una finalidad distinta de aquella para la que fueron recogidos, como era el control por el empresario de aquellos trabajadores que habían secundado una huelga. No obstante, es posible el tratamiento posterior para fines de archivo en interés público, de investigación histórica o científica, o estadísticos[217].

No basta con que la finalidad sea determinada, explícita y legítima para que lo sea el tratamiento. Debe existir una correlación entre la necesidad de los datos solicitados y el cumplimiento de las finalidades señaladas. Esto es lo que el Reglamento europeo llama "minimización de datos", que significa que la

---

[216] TRONCOSO REIGADA, A.: *Comentarios a la ley Orgánica de protección…*, pág. 343.

[217] Artículos 4.2 LOPD y 9.1 RLOPD. Cabe incluso la posibilidad de la utilización de los datos para finalidades distintas de las que originaron la recogida. Así, el artículo 15 del RLOPD regula la solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma. En cualquier caso, los datos objeto de tratamiento solo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con previo consentimiento del interesado (art. 11.1 LOPD).

recogida de datos y su posterior tratamiento solo es legítima si los datos son adecuados, pertinentes y limitados a lo necesario para obtener la finalidad.

El análisis de la legitimidad de algunos tratamientos de datos personales debe hacerse examinando el principio de calidad como principio de proporcionalidad. Con frecuencia ocurre que los tratamientos superan el juicio de idoneidad o adecuación, es decir, que los datos recabados ayudan realmente a la consecución del fin que se persigue. Por tanto, procede valorar si pasarían el juicio de necesidad, esto es, si no hay otro medio menos lesivo que permita alcanzar la finalidad que persigue el tratamiento de datos en cuestión. Y, salvado este segundo requisito, habría que llevar a cabo un juicio de proporcionalidad en sentido estricto, lo que obligaría a valorar el peso o importancia que se debe otorgar a la protección de los datos recabados en relación con la finalidad que justifica su registro[218].

El principio de calidad exige racionalizar los datos de carácter personal que se solicitan de los ciudadanos, sobre todo los especialmente protegidos, tratando únicamente los adecuados y pertinentes. Así, como señaló la STC 202/1999, el tratamiento de datos de salud del trabajador sin consentimiento expreso de aquel, en un fichero de recursos humanos de una entidad de crédito, no es adecuado para la finalidad propia de la relación laboral y constituye una limitación desproporcionada del derecho fundamental a la protección de datos personales. Con el fin de satisfacer las finalidades del tratamiento, el dato debe conservarse exacto y, si fuera necesario, actualizado. En este mismo sentido, la LOPD dispone que “los datos de carácter personal

[218] *Vid*. TRONCOSO REIGADA, A*, La protección de datos personales en busca…,* págs. 401-402.

serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado"[219].

Como consecuencia, el responsable del fichero está obligado a rectificar los datos inexactos, en todo o en parte, o incompletos, y sustituirlos de oficio por los correspondientes datos rectificados o completados[220] . Se persigue, por un lado, no tratar información inservible para el cumplimiento de la finalidad del fichero por su falsedad, pero, también, no ocasionar un perjuicio a otros derechos fundamentales del interesado[221]. Por ejemplo, la inexactitud de los datos del padrón municipal puede vulnerar los derechos fundamentales de participación política o el derecho a la educación[222]. De igual modo, la integridad de los datos es especialmente importante en el ámbito sanitario como instrumento de garantía del derecho a la vida y a recibir una adecuada asistencia sanitaria.

Además, el interés del dato desaparece cuando haya dejado de ser exacto y completo. En tal caso, los datos se conservarán a disposición de las Administraciones públicas, jueces y tribunales únicamente con el fin de responder a las responsabilidades surgidas del tratamiento, durante el plazo de prescripción de estas[223].

Especial relevancia tiene el principio de exactitud de los datos en los ficheros privados de las entidades que se dediquen a la prestación de servicios

---

[219] El artículo 4.3 LOPD emplea la expresión "actual", a diferencia de lo que decía la LORTAD que decía "real". *Ibidem,* págs. 412 y ss., y, sobre todo, la nota al pie 290, sobre el conflicto entre el derecho de protección de datos y la libertad de empresa.
[220] *Vid.* artículo 4.4 LOPD y artículo 8.5 RLOPD.
[221] *Vid*. TRONCOSO REIGADA, A*, La protección de datos personales en busca…,* nota al pie 282, pág. 409.
[222] *Vid*. voto particular del magistrado Pérez Tremps a la STC 17/2013.
[223] *Vid.* artículos 4.4 y 16.2 y 3 LOPD y articulo 8.5 RLOPD.

relativos a documentar la solvencia patrimonial y de crédito, por lo que la LOPD prevé la obligación, en tales casos, de registrar y ceder solamente los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados, y siempre con la condición de que respondan con veracidad a la situación actual del afectado[224].

Por último, la vida del dato llega a su término cuando haya dejado de ser necesario y pertinente para la finalidad para la que fueron recogidos, por lo que deberán ser mantenidos de forma que permitan la identificación de los interesados durante no más tiempo que el necesario para los fines del tratamiento. Procede la cancelación[225] cuando el dato no sea necesario para cumplir las funciones que motivaron su recogida[226]. Le corresponde al responsable del fichero, que es el que ha determinado la finalidad del tratamiento, decidir cuándo los datos han dejado de ser necesarios para la finalidad para la cual fueron recabados.

La LOPD señala que los datos personales 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[227]. Podrán conservarse durante periodos más largos,

---

[224] Artículo 29.4 LOPD. Sentencia del Tribunal de Justicia de la Unión Europea (Sala Tercera) de 23 de noviembre de 2006, asunto C-238/05 ASNEF-EQUIFAX. Sobre la viabilidad de la subsistencia de este artículo una vez que entre en vigor el Reglamento europeo, *vid*. ALONSO MARTÍNEZ, C. y CERQUEIRA SÁNCHEZ, M.: "Ficheros sobre solvencia patrimonial y crédito" en AA. VV.: *El Reglamento General de protección de datos*…págs. 662-664. *Vid.* artículo 20 sobre Sistemas de información crediticia del Proyecto de Ley Orgánica de Protección de Datos de 24 de noviembre de 2017.

[225] Artículo 5.1.b) RLOPD.

[226] Artículo 4.5 LOPD y artículo 8.5 RLOPD.

[227] Artículo 16.5 LOPD. De la misma manera, la Ley permite la conservación de los datos en dos circunstancias: por un periodo superior al necesario para el cumplimiento de los fines que originaron su recogida tras un proceso de disociación (art. 8.6 RLOPD) y por motivos históricos, estadísticos o científicos (arts. 9.2 y 157 y 158 RLOPD).

según la normativa europea, siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica y fines estadísticos, frente a la norma española, que exige la previa solicitud a la AEPD u autoridad equivalente de la Comunidad Autónoma para que acuerde el mantenimiento integro de determinados datos, atendidos sus valores históricos, estadísticos o científicos[228].

3.1.4. Seguridad de los datos.

En la normativa española, las personas que intervengan en cualquier estadio del tratamiento de los datos deben observar dos principios:

- En todo caso, el deber de secreto, como una garantía del control y dominio de la persona sobre sus datos. Este deber se corresponde, al propio tiempo, con el derecho que tiene el titular de evitar la publicidad no consentida sobre cualquier información personal que le concierna, aun cuando su divulgación no le cause ningún perjuicio.[229]

- La seguridad de los datos, que constituye uno de los elementos que forman parte del contenido esencial del derecho fundamental a la protección de

[228] Artículo 5.1.e) RGPD, sin perjuicio de la aplicación de las medidas técnicas y organizativas que prevé el RGPD a fin de proteger los derechos y las libertades del interesado. La norma española es el articulo 9 RLOPD en relación con los artículos 157 y 158 RLOPD, que regulan el procedimiento para la autorización de la conservación de datos para estos fines.

[229] Este principio se encuentra recogido en el artículo 10 de la LOPD y los artículos 82 y 83 del RLOPD. De acuerdo con el artículo 10 de la LOPD, 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. Obliga, por tanto, a todo el que intervenga en cualquier fase del tratamiento a la confidencialidad respecto de lo conocido como consecuencia del mismo y a su uso únicamente para la finalidad legítima que motivó su recogida.

datos (artículo 9 LOPD). La seguridad es una garantía de la integridad, de la disponibilidad y de la confidencialidad de la información. Como hemos visto, el principio de calidad exige conservar la información, respetando la exactitud, autenticidad e integridad de la misma.

En realidad, el principio de seguridad de datos debe entenderse como un derecho de las personas, aunque el legislador lo ha contemplado como una obligación impuesta al responsable del fichero y, en su caso, al encargado del tratamiento de adoptar medidas técnicas y organizativas concretas[230].

Según el Reglamento europeo, los datos serán tratados de tal manera que se garantice una seguridad adecuada de los mismos, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Además, el responsable del tratamiento debe ser capaz de demostrar que ha adoptado las decisiones adecuadas a tal efecto, lo que el Reglamento ha llamado la responsabilidad proactiva[231].

---

[230] Hasta el momento, opera sobre la base de círculos concéntricos de seguridad, imponiendo la implantación de mayores niveles de seguridad en atención al carácter de los datos objeto de tratamiento El nivel básico de seguridad es el que deben adoptar todos los ficheros o tratamientos de datos de carácter personal (art. 81 RLOPD), por ejemplo, los ficheros con datos personales identificativos, académicos y profesionales. Las medidas de seguridad del nivel medio, además de las de nivel básico, deberán ser adoptadas en los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, datos sobre la solvencia patrimonial y el crédito y datos de carácter personal que permitan obtener un perfil de la personalidad o del comportamiento de los ciudadanos. Este nivel de seguridad será también exigible a aquellos ficheros o tratamientos de los que sean responsables Administraciones tributarias respecto de los datos relacionados con el ejercicio de sus potestades tributarias, entidades financieras respecto de los relacionados con la prestación de servicios financieros, y Entidades, Servicios y Mutuas de la Seguridad Social respecto a los relacionados con el ejercicio de sus competencias. Las medidas de seguridad de nivel alto, además de las de nivel básico y medio, se aplicarán a los ficheros que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, los que contengan datos para fines policiales sin consentimiento de las personas afectadas y los que recojan datos derivados de actos de violencia de género.

[231] Artículos 5.1.f) y 5.2 del RGPD.

El responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas, aplicarán las medidas técnicas y organizativas apropiadas al nivel de seguridad adecuado al riesgo.

Entre las novedades de la normativa europea, se obliga al responsable del tratamiento a notificar a la autoridad de control competente toda violación de seguridad de los datos personales, de ser posible, en el plazo de 72 horas desde que tuvo conocimiento de ella. Asimismo, el encargado del tratamiento deberá notificar sin dilación a aquel las violaciones de la seguridad de los datos personales de las que tenga conocimiento. Cuando sea probable que esta violación de la seguridad entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado[232].

3.2. De los derechos ARCO a los derechos ARSLPO.

Constituyen la otra cara del contenido esencial del derecho fundamental a la protección de datos. Estas facultades concretas se convierten en el límite de los límites para el legislador y para los poderes públicos, sin las cuales este derecho no es reconocible y sin cuyo ejercicio los intereses jurídicos que

[232] *Vid*, artículos 32, 33 y 34 del RGPD y los considerandos 85 a 88 del RGPD. Sobre este particular, puede consultarse el Dictamen 3/2014 del Grupo de Trabajo del artículo 29 sobre notificaciones de violaciones de datos personales, de 25 de marzo de 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_es.pdf

representa quedan privados de protección. De ahí que cualquier restricción que afecte a este derecho debe venir justificada por la protección de otro bien o derecho constitucionalmente garantizado, debiendo cumplir con las exigencias del principio de proporcionalidad y, en todo caso, respetar su contenido esencial[233].

Estas facultades no solo van encaminadas salvaguardar el derecho a la protección de los datos personales como categoría autónoma, sino que en ocasiones operan como garantía instrumental de otros intereses, como el respeto a los derechos fundamentales al honor, a la intimidad o a evitar la discriminación.

A los tradicionales derechos ARCO hay que añadir, como consecuencia del Reglamento europeo, los derechos a la limitación del tratamiento y a la portabilidad de los datos personales, además de la desaparición del término cancelación, que ha sido sustituido por el derecho de supresión o derecho al olvido. Así, los derechos ARCO quedan sustituidos por los derechos ARSLPO.

En cuanto al ejercicio de estos derechos, la normativa española establece plazos máximos diferentes para que el responsable del tratamiento resuelva sobre la solicitud de los derechos ARCO. En el Reglamento[234], se unifican los plazos en los que el responsable del tratamiento debe facilitar al interesado la información solicitada con arreglo a los derechos ARSLPO, que como regla general se ha de dar en un mes, si bien con posibilidad de prórroga

[233] STC 254/1993, en relación con el derecho de acceso a los datos.
[234] Artículo 12.3 RGPD. Del mismo modo, el párrafo cuarto del artículo 12 establece que si el responsable del tratamiento no atiende la solicitud, deberá informar al interesado, en el plazo máximo de un mes, de los motivos de la dilación, así como de la posibilidad de reclamar ante la autoridad de control competente y de ejercitar acciones judiciales para la defensa de sus legítimos intereses.

de dos meses si la complejidad y el número de solicitudes lo requiere. En este caso, se deberán justificar los motivos de la demora.

Se impone la gratuidad como principio general en la normativa española para el ejercicio por el interesado de sus derechos en materia de protección de datos[235]. Sin embargo, en caso de solicitudes manifiestamente infundadas o excesivas y reiteradas, el Reglamento permite al responsable elegir entre cobrar un canon razonable en función de los costes administrativos o denegarlas, si bien la carga de la prueba recaerá sobre el responsable del tratamiento[236].

En particular, podríamos definir el derecho de acceso[237] como la facultad de solicitar y obtener información de si se están tratando o no datos personales del interesado. Solo accediendo a los datos personales el afectado puede comprobar la licitud del tratamiento y ejercitar el haz de facultades que conforma el derecho fundamental a la protección de datos. La información incompleta o extemporánea supone una vulneración del derecho de acceso y justificaría la reclamación del ciudadano ante la AEPD u órgano equivalente de la Comunidad Autónoma.

El derecho de acceso es independiente del derecho a acceder a archivos o registros administrativos, reconocido en el artículo 105.b) de la Constitución y desarrollado por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Difiere en que este se ejerce solamente frente a la Administración pública, su objeto es la

[235] El artículo 28.3 RLOPD contempla también una excepción a la gratuidad.
[236] Artículo 12.5 RGPD.
[237] Como curiosidad, este tema está regulado en el artículo 15 tanto en la LOPD, como en el RGPD.

información administrativa -esté o no sometida a tratamiento- y se extiende a toda clase de datos, propios o de terceras personas[238].

El derecho de acceso no es un derecho absoluto, sino que está sometido a límites. Como resulta de la LOPD[239], los responsables de los ficheros creados por las Fuerzas y Cuerpos de Seguridad podrán denegar el acceso, rectificación y cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se están realizando. Igualmente, los responsables de los ficheros de la Hacienda Pública podrán denegar el ejercicio de estos derechos cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras. En todo caso, el afectado podrá ponerlo en conocimiento de la AEPD u órgano equivalente de la Comunidad Autónoma, que deberá resolver sobre la procedencia o improcedencia de la denegación.

A este respecto, hay que tener en cuenta que la Ley preveía otras limitaciones a los derechos de los afectados, concretamente “por razones de interés público o intereses de terceros más dignos de protección”, que fueron

---

[238] Como pone de relieve Rodríguez Álvarez, "la vigente Ley de Transparencia no hace distinciones para el ejercicio del derecho de acceso a la información pública en función de que dicha información incluya datos personales del propio solicitante o de terceros. Configura un único procedimiento para ambos supuestos, sin perjuicio de que el derecho sustantivo aplicable en cada caso pueda ser distinto. Al mismo tiempo, permanece inalterado el régimen del derecho de acceso de la LOPD, de suerte que si lo que el interesado pretende no es acceder a la información pública, sino únicamente a sus datos personales, puede optar por este cauce". *Vid.* RODRÍGUEZ ÁLVAREZ, J. L.: "Transparencia y protección de datos personales: criterio legales de conciliación", en CANALS AMETLLER, D (ed.): *op. cit.,* pág. 66.

[239] Artículo 23 LOPD.

declaradas inconstitucionales en la STC 290/2000. Según esta sentencia, “los motivos de limitación adolecen de tal grado de indeterminación que deja excesivo campo de maniobra a la discrecionalidad administrativa, incompatible con las exigencias de la reserva legal en cuanto constituye una cesión en blanco del poder normativo que defrauda la reserva de ley. Además, al no hacer referencia alguna a los presupuestos y condiciones de la restricción, resulta insuficiente para determinar si la decisión administrativa es o no el fruto previsible de la razonable aplicación de lo dispuesto por el legislador (SSTC 101/1991, FJ 3, y 49/1999, FJ 4)" (FJ 18). En consecuencia, el Tribunal Constitucional declaró dicha previsión contraria a los artículos 18.4 y 53.1 CE.

La normativa de la Unión Europea, ha ampliado notablemente la información que deberá obtener el interesado que ejercite el derecho de acceso frente responsable del tratamiento[240]. El Reglamento ha venido a plasmar la jurisprudencia del Tribunal de Justicia en las STJUE de 7 de mayo de 2009, en el asunto C-553/07, Rijkeboer, y STJUE de 12 de diciembre de 2013, en el asunto C-486/12, X[241]. En caso de obtener confirmación del tratamiento, el afectado podrá acceder a los datos personales y a la información sobre los fines del tratamiento, las categorías de datos personales de que se trate, los destinarios a los que se comunicaron o se comunicarán los datos personales, el plazo de conservación de los datos personales, los derechos de rectificación o supresión u oposición, el derecho a reclamar ante una autoridad de control, el origen de los datos si no se obtuvieron del interesado, así como la existencia de decisiones automatizadas incluida la elaboración de perfiles. Por lo tanto,

[240] Artículo 15 RGPD.
[241] STJUE de 7 de mayo de 2009, en el asunto C-553/07, Rijkeboer; STJUE de 12 de diciembre de 2013 en el asunto C-553/12, X.

supone una obligación para el responsable del tratamiento distinta del cumplimiento del principio de información, pues permite recabarla en un momento posterior al de la recogida de los datos. Se reconoce el derecho a obtener una copia de los datos personales objeto de tratamiento.

Sin embargo, el derecho de acceso puede colisionar con la protección de otros derechos fundamentales, por ejemplo, cuando los datos no han sido aportados por el interesado, sino por terceras personas cuya intimidad debe protegerse. Así, encontramos un ejemplo en la jurisprudencia del Tribunal Europeo de Derechos Humanos, el caso Gaskin contra el Reino Unido, resuelto por la STEDH de 7 de julio de 1989, en que se denegó el acceso al expediente de un centro de acogida dependiente de la Administración local. El carácter reservado del contenido de dicho expediente favorecía la eficacia del sistema de asistencia a la infancia y pretendía proteger tanto los derechos de los informantes, que habían aportado los documentos, como los de los niños que necesitaban los cuidados.

Para el Tribunal Europeo de Derechos Humanos, las personas que estén en la situación del demandante tienen un interés primordial en recibir las informaciones necesarias para conocer y comprender su infancia y sus años de formación. Sin embargo, hay que tener también en cuenta que el carácter reservado de los expedientes administrativos es muy importante si se quiere disponer de informaciones objetivas y merecedoras de crédito, y que, además, puede ser necesario para proteger a terceras personas. Desde este punto de vista, un sistema como el británico, que subordina el acceso a este tipo de expedientes al consentimiento de los informantes puede considerarse, en principio, compatible con el artículo 8 CEDH, teniendo en cuenta el margen de

apreciación del Estado. No obstante, cuando no se consigue entrar en relación con el informante o este niega abusivamente su conformidad, el sistema debe proteger los intereses de cualquiera que pretenda consultar los datos sobre su vida privada y familiar; y la negativa al acceso solo estará de acuerdo con el principio de proporcionalidad si dispone de un órgano independiente que, en el supuesto de que un informante no conteste o no dé su consentimiento, pueda adoptar la resolución definitiva sobre la cuestión. Esto no sucedió en este asunto y el Tribunal declaró lesionado el derecho al respeto a la vida privada.

Los derechos de rectificación, cancelación, oposición y limitación de tratamientos serán objeto de estudio en el capítulo II de este trabajo.

Para terminar, el Reglamento de la Unión Europea ha ampliado el catálogo de los tradicionales derechos que acabamos de exponer con el derecho a la portabilidad de los datos (ARSLPO). Estrechamente relacionado con el derecho de acceso, presupone que el interesado tendrá derecho a recibir copia de los datos "en un formato estructurado, de uso común y lectura mecánica". El propósito de este derecho es darle más control al interesado sobre sus datos personales. Pero, además, este derecho sirve como complemento del derecho de acceso, pues constituye una herramienta que facilitará la transmisión de datos personales en el marco de la Unión Europea, al permitir la transmisión directa de datos personales de un responsable del tratamiento a otro cuando sea técnicamente posible[242].

Cuando una persona ejerce su derecho a la portabilidad de datos, se entiende sin perjuicio de los derechos de revocación, oposición y supresión a

[242] Artículo 20 RGPD.

que se refiere el artículo 17 RGPD. El derecho de portabilidad no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Es posible el ejercicio de este derecho cuando el tratamiento esté basado en el consentimiento del interesado o en un contrato del que aquel sea parte y se efectúe por medios automatizados.

Respecto a los datos personales objeto de este derecho, alcanzará a aquellos que incumben al interesado que los haya facilitado a un responsable del tratamiento. En general, dados los objetivos de la norma reguladora del derecho a la portabilidad de los datos, el término "proporcionados por el interesado" debe interpretarse en un sentido amplio y excluir únicamente los "datos inferidos" y los "datos deducidos", que incluyen los datos personales que genera un proveedor de servicios, como por ejemplo, resultados algorítmicos. Un responsable del tratamiento puede, por tanto, excluir esos datos inferidos, pero debe incluir todos los demás datos personales proporcionados por el interesado por medios técnicos dispuestos por el responsable del tratamiento.

Así pues, la expresión "proporcionados por" incluye los datos personales que guardan relación con la actividad del interesado o se derivan de la observación del comportamiento de una persona, pero no el análisis posterior de dicho comportamiento. En cambio, todos los datos personales que hayan sido generados por el responsable del tratamiento como parte del tratamiento de datos, por ejemplo, mediante un proceso de personalización o recomendación, mediante categorización de usuarios o creación de perfiles, son datos que se deducen o se infieren de los datos personales aportados por

el interesado y no están cubiertos por el derecho a la portabilidad de los datos[243].

Por último, el derecho a la portabilidad de los datos no deberá afectar negativamente a los derechos y libertades de otros.

3.3. La autoridad de control independiente.

Nuestra Constitución no exigió el establecimiento de una autoridad de control para la protección de datos. Sin embargo, hoy en día la existencia de un ente de este tipo está generalmente admitida como exigencia necesaria para la garantía del derecho que venimos estudiando. Así lo confirma la STEDH de 7 de julio de 1989, ya examinada, y el artículo 8.3 de la Carta de Derechos Fundamentales, que concluye imponiendo que el respeto de estas normas quedará sujeto al control de una autoridad independiente.

De hecho el legislador español optó, ya en la LORTAD, por la configuración de esta, la Agencia de Protección de Datos, como un ente de derecho público que actúa con plena independencia en el ejercicio de sus funciones[244]. A partir de 2004 se denomina Agencia Española de Protección de Datos -en adelante AEPD- para plasmar la distribución competencial de

[243] Sobre esto, *vid.* directrices sobre el derecho a la portabilidad de los datos de 13 de diciembre de 2016, del Grupo de trabajo del artículo 29 sobre protección de datos. https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricesportabilidad.pdf

[244] De conformidad con lo dispuesto en el artículo 34.2 y en la disposición final primera de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, se aprueba el Estatuto de la Agencia de Protección de Datos, por Real Decreto 428/1993, de 26 de marzo. En este sentido, el artículo 35 de la Ley Orgánica15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.

nuestro Estado de las Autonomías[245]. Actualmente comparte funciones con la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía[246].

Desde la perspectiva del Derecho de la Unión, el establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal.

Los Estados miembros tienen la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa.

---

[245] En virtud del artículo 79 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social: "La Agencia de Protección de Datos pasa a denominarse Agencia Española de Protección de Datos. Las referencias a la Agencia de Protección de Datos realizadas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en las normas a las que se refiere su disposición transitoria tercera y cualesquiera otras que se encuentren en vigor deberán entenderse realizadas a la Agencia Española de Protección de Datos". Por otra parte se crearon tres agencias autonómicas: en Cataluña por Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, en País Vasco por Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos y en Madrid. La Agencia de Protección de Datos de la Comunidad de Madrid fue un ente de derecho público autonómico creado por Ley 13/1995, de 21 de abril, de regulación del uso de la informática en el tratamiento de datos personales por la Comunidad de Madrid para ejercer las competencias derivadas de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Con motivo de la aprobación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que deroga la normativa anterior de 1992, y amplía el ámbito de actuación de las autoridades de control autonómicas al extender su actuación sobre los ficheros de datos de carácter personal creados o gestionados por la Administración Local del ámbito territorial de la Comunidad Autónoma de que se trate, la Comunidad de Madrid amplió las competencias de la agencia por medio de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid. Fue suprimida el 1 de enero de 2013 en virtud de la Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas de la Comunidad de Madrid, y sus funciones pasaron a ser asumidas por la Agencia Española de Protección de Datos.

[246] El Consejo de Transparencia y Protección de Datos de Andalucía, creado por el artículo 43 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, es la autoridad independiente de control en materia de transparencia y protección de datos en la Comunidad Autónoma de Andalucía

La independencia de las autoridades de control no debe significar que dichas autoridades queden exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial[247].

Cada autoridad de control debe ser competente para el examen de reclamaciones presentadas por un interesado, la realización de investigaciones sobre la aplicación del Reglamento y el fomento de la sensibilización del público acerca de los riesgos, las normas, las garantías y los derechos en relación con el tratamiento de datos personales.

En la normativa española, la tutela de los derechos corresponde, como se ha dicho, a la Agencia Española de Protección de Datos o, en su caso, al organismo competente de la Comunidad Autónoma[248].

No se agota ahí la defensa del derecho fundamental a la protección de datos de carácter personal, pues muchas violaciones de este lo son también de los derechos al honor y a la intimidad personal. Si el origen de la vulneración está en el responsable de un fichero privado, procederá acudir, en tales casos al juicio civil ordinario con las especialidades previstas en la LEC para la tramitación de las demandas relativas a estos derechos y a los demás

[247] *Vid.* considerandos 117 y 118 RGPD. Conforme al considerando 122, a fin de garantizar la independencia de la autoridad de control, sus miembros deben actuar con integridad, abstenerse de cualquier acción que sea incompatible con sus funciones y no participar, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada. La autoridad de control debe tener su propio personal, seleccionado por ella o por un organismo independiente establecido por el Derecho de los Estados miembros, que esté subordinado exclusivamente al miembro o los miembros de la autoridad de control.

[248] De acuerdo con el artículo 41 de la LOPD, las funciones de la Agencia de Protección de Datos reguladas en el artículo 37 LOPD, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49 de la LOPD, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido. *Vid.* también artículos 117 a 119 RLOPD.

derechos fundamentales[249]. Si, por el contrario, la lesión procede del responsable de un fichero público, será de aplicación el procedimiento preferente y sumario regulado en la Ley 29/1998, de la Jurisdicción Contencioso-Administrativa, paralelamente al contencioso administrativo que corresponda.

También cabe la protección penal a través de los tipos descritos en el Titulo X del Código Penal. En este caso, la apertura de un proceso penal obligará a suspender el procedimiento administrativo[250].

Según el Reglamento de la Unión Europea, todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control única, en particular en el Estado miembro de su residencia habitual, y se debe garantizar su derecho a la tutela judicial efectiva, de conformidad con el artículo 47 de la CDFUE, si considera que se vulneran sus derechos con arreglo al Reglamento, o en caso de que la autoridad de control no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger sus derechos[251].

En el capítulo VIII del Reglamento se contemplan el derecho a presentar una reclamación y el derecho a la tutela judicial efectiva contra una autoridad de control y contra un encargado del tratamiento. Para facilitar la presentación

---

[249] Artículo 249.1.2 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil: "Se decidirán en el juicio ordinario, cualquiera que sea su cuantía: 2. Las que pretendan la tutela del derecho al honor, a la intimidad y a la propia imagen, y las que pidan la tutela judicial civil de cualquier otro derecho fundamental, salvo las que se refieran al derecho de rectificación. En estos procesos, será siempre parte el Ministerio Fiscal y su tramitación tendrá carácter preferente." Igualmente en relación con el juez competente el artículo 52.6º de la LEC y sobre el recurso de casación los artículos 477.2.1º y 487.2 de la LEC. *Vid*. CARRASCO DURÁN, M.: *Los procesos para la tutela judicial de los derechos fundamentales*, CEPC, Madrid, 2002, págs. 395-400.
[250] Artículo 10.2 LOPJ.
[251] Artículo 77 RGPD.

de reclamaciones, cada autoridad de control debe adoptar medidas tales como el suministro de un formulario de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

3.4. Límites.

Como todo derecho fundamental, el relativo a la protección de datos personales no es un derecho absoluto. Esta afirmación se recoge expresamente en el Reglamento europeo, que añade que se "debe mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad"[252].

Los límites deben ser dispuestos por ley, han de respetar el contenido esencial del derecho y deben justificarse en aras de garantizar otro bien o derecho constitucional merecedor de protección. Esta necesidad se puso de manifiesto en el Convenio 108 del Consejo de Europa (art. 9.1ª) y, después, en la Directiva 95/46/CE (art. 13.1.e).

En este sentido, el Convenio citado señala que serán posibles excepciones a los principios que contiene “cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:

a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;

---

[252] *Vid*. considerando 4 del RGPD.

b) Para la protección de la persona concernida y de los derechos y libertades de otras personas".

El Tribunal Europeo de Derechos humanos, en relación con el artículo 8 del CEDH, que regula el respeto a la vida privada y familiar, aplicable también al tratamiento de datos de carácter personal, reconoce que este derecho podría tener límites tales como la seguridad del Estado (STEDH, caso Leander de 26 de enero de 1987 (párrafos 47 y ss.)[253] o la persecución de las infracciones penales (SSTEDH, caso *Z* contra Finlandia, de 28 de febrero de 1997 y Funke contra Francia de 25 de febrero de 1993).

De su jurisprudencia se extrae que el almacenamiento y conservación de datos a través de medidas de vigilancia secreta, los registros personales, la toma de huellas dactilares, de fotografías etc., son injerencias en el derecho al respeto a la vida privada en su manifestación de protección de datos personales. No obstante, las facultades que conforman el derecho a la protección de datos de carácter personal, pueden ser limitadas por parte de los poderes públicos.

El artículo 8.2 del CEDH enumera los bienes o valores que pueden justificar una restricción a este derecho. La injerencia estará justificada siempre que esté establecida por la ley, responda a una finalidad legítima y sea necesaria en una sociedad democrática. Si falta alguna de estas condiciones,

---

[253] El Tribunal Europeo de Derechos Humanos afirmó que el registro secreto de la policía encerraba, sin lugar a dudas, datos relativos a la vida privada del señor Leander. Tanto el almacenamiento de estos datos como su comunicación a la autoridad militar, unido ello a la negativa a concederle la facultar de refutarlos, atentaba contra su derecho a la vida privada garantizado por el artículo 8.1 del CEDH. No obstante, el Tribunal antepuso los requerimientos de la seguridad nacional sobre el interés del demandante, y, como resultado de esta ponderación, concluyó que la injerencia que el señor Leander sufrió no podía ser considerada como desproporcionada al fin legítimo perseguido, párrafo 47.

el límite no estará justificado y se habrá violado el artículo 8 CEDH. En este sentido, la jurisprudencia del Tribunal Europeo de Derechos Humanos ha afirmado el principio según el cual se produce lesión del derecho al respeto a la vida privada cuando se recogen, almacenan y tratan datos personales y la norma que regula estos procedimientos no establece las garantías necesarias. Sobre la base de estas consideraciones, el Tribunal Europeo de Derechos Humanos aclara que la ley que permita la injerencia debe ser clara y concisa y debe establecer el tratamiento que se va a seguir; la información que va a ser recogida o almacenada, y en este último supuesto, por cuánto tiempo y bajo qué condiciones; los procedimientos de acceso y cesión de datos personales, en los que debe establecerse qué autoridades son las que pueden tener acceso y a quiénes pueden cederse los datos; y los procedimientos de información, rectificación y cancelación de los datos recopilados[254] .

En el ordenamiento jurídico español, como recuerda nuestro Tribunal Constitucional, aunque la Constitución no imponga expresamente a la protección de datos límites específicos, ni remita a los poderes públicos para su determinación, como ha hecho con otros derechos fundamentales, mediante la

[254] En la STEDH de 4 de mayo de 2000, caso Rotaru contra Rumanía, los hechos demostraron que el Servicio Rumano de Información -SRI- conservaba, entre otros, datos falsos sobre el presunto pasado legionario del demandante que, de mantenerse, atentarían gravemente contra su dignidad y su honor, constituyendo una injerencia en el derecho al respeto a su vida privada. En este supuesto, la falta de previsión legal sobre las condiciones que autorizaban al SRI a la recogida, almacenamiento y comunicación de datos sobre la vida privada de una persona, en cuanto a la antigüedad de las informaciones o a la duración de su conservación, unido a la inexistencia de garantías adecuadas, llevaron al Tribunal Europeo de Derechos Humanos a deducir que hubo violación del artículo 8. Además, la insuficiencia normativa impidió al Tribunal Europeo de Derechos Humanos controlar la legitimidad del fin perseguido o si, en su caso, las medidas adoptadas eran "necesarias en una sociedad democrática" (párrafo 62).

imposición de límites a la autodeterminación informativa se contribuye a dotar a la Constitución de un significado unitario[255].

Por tanto, el principio de unidad de la Carta Magna obliga a interpretarla como un todo, y no cabe duda de que el derecho fundamental a la protección de datos puede entrar en conflicto con los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos. La resolución de estas controversias mediante la imposición o aplicación de un límite al ejercicio del derecho a la protección de datos debe respetar los requisitos del principio de proporcionalidad[256], es decir, la restricción debe ser el medio adecuado, necesario y proporcional para conseguir el fin de la tutela del derecho o bien constitucional con el que, en un caso determinado, haya entrado en conflicto.

Para determinar los bienes y finalidades constitucionalmente legítimos aptos para restringir el derecho del artículo 18.4 de la CE, nuestro Tribunal Constitucional ha efectuado una "constitucionalización" de la normativa europea, al mismo tiempo que los ha identificado con los límites al derecho de acceso a la información pública, contenido en el artículo 105.b) CE[257]. Así, la seguridad y la defensa del Estado, la persecución y el castigo de los delitos constituyen bienes dignos de protección constitucional a juicio del Alto Tribunal, ya que a través ellos se defienden otros como la paz social y la seguridad ciudadana (arts. 10.1 y 104.1 CE)[258]. Por otra parte, en las SSTC 110/1984 y 143/1994 considera el máximo intérprete de nuestra Carta Magna que la distribución equitativa del sostenimiento del gasto público y las actividades de

[255] STC 292/2000, FJ11.
[256] Sobre la ponderación de la proporcionalidad de la medida adoptada en los casos de videovigilancia laboral, *vid* STC 39/2016.
[257] GUICHOT REINA, E.: *op. cit.*, pág. 174.
[258] STC 292/2000, FJ 9, así como las SSTC 166/1999, FJ 2 y 127/2000, FJ 3, y ATC 155/1999.

control en materia tributaria (art. 31 CE) son intereses constitucionalmente aptos para limitar el ejercicio de este derecho.

Con el argumento del principio de reserva de ley a la hora de establecer límites a los derechos fundamentales, el Tribunal Constitucional consideró inconstitucional la posibilidad prevista en el texto original de la LOPD[259] de que una norma reglamentaria pudiera autorizar la cesión de datos entre Administraciones Públicas para ser empleados en el ejercicio de competencias o para materias distintas a las que motivaron su originaria recogida sin necesidad de recabar previamente el consentimiento del interesado, pues dicha norma soslayaba el artículo 53.1 CE, que reserva en exclusiva a la ley la regulación y limitación del ejercicio de un derecho fundamental, vulnerando, por consiguiente, el derecho fundamental mismo, al privarlo de una de sus garantías.

Al propio tiempo, el Tribunal Constitucional señaló que las restricciones al derecho a la protección de datos deben estar justificadas en otros derechos o bienes constitucionales y han de ser proporcionadas, así como precisas y previsibles en aras de la seguridad jurídica. Según el máximo intérprete de la Carta Magna, el legislador, en este caso, no impuso limitaciones generales al ejercicio del derecho fundamental a la protección de datos frente a la Administración Pública, sino que permitió que aquella, en ciertos supuestos, pudiera conceder o denegar discrecionalmente el ejercicio de las facultades que integran el contenido esencial del derecho. Con esto, se produjo una vulneración de la función de garantía propia de toda reserva de ley relativa a

[259] Artículos 21.1 y 24.1 y 2 LOPD declarados inconstitucionales y nulos por la STC 292/2000, FJ 2.

los derechos fundamentales, y, al propio tiempo, se permitió que el derecho fundamental pudiera ceder ante intereses o bienes jurídicos de rango infraconstitucional[260].

En ocasiones, el Tribunal Constitucional[261] ha admitido que, incluso en ámbitos reservados por la Constitución a la regulación por ley, es posible la intervención auxiliar o complementaria del Reglamento, pero siempre que el ejercicio de la potestad reglamentaria fuera indispensable por motivos técnicos o para atender a finalidades de la propia Constitución o la ley. Lo que no es admisible es una renuncia del legislador, transfiriendo tal facultad al titular de la potestad reglamentaria.

Actualmente, la normativa europea ha recogido las limitaciones del derecho a la protección de datos, como colofón del capítulo III, dedicado a los derechos del interesado. A través de medidas legislativas, el Derecho de la Unión o de los Estados miembros podrá limitar el alcance de las obligaciones y los derechos ARSLPO, así como de los principios relativos a aquellos. En todo caso, tales limitaciones[262] deberán respetar en lo esencial los derechos y libertades fundamentales y ser necesarias y proporcionadas en una sociedad democrática para salvaguardar: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; e) otros objetivos importantes de interés público general de la Unión o de un Estado

[260] En contra de esta declaración de inconstitucionalidad, *vid.* TRONCOSO REIGADA, A.: "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional" *Cuadernos de Derecho Público,* núm. 19-20, 2003, págs. 301 y ss.
[261] STC 127/1995, FJ 5, con remisión a la STC 83/1984, FJ 4, y a la STC 99/1987, FJ 3 a).
[262] Artículo 23 RGPD.

miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; f) la protección de la independencia judicial y de los procedimientos judiciales; g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g); i) la protección del interesado o de los derechos y libertades de otros; j) la ejecución de demandas civiles.

4. EL RÉGIMEN JURÍDICO DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES.

Para estudiar el régimen jurídico del derecho a la protección de datos personales es preciso tener en cuenta la asunción de la competencia sobre su regulación por parte de la Unión Europea.

En el ámbito de la seguridad, el Tratado de la Unión Europea, firmado en Maastricht el 7 de febrero de 1992, estableció entre sus objetivos una mayor cooperación entre las fuerzas policiales, las autoridades aduaneras y demás competentes, ya directamente o a través de la "Oficina Europea de Policía" (Europol). En el plano de la cooperación policial y judicial penal, se celebraron acuerdos a nivel sectorial, al amparo del Título VI del Tratado de la Unión Europea, los cuales facilitaron la captación, el intercambio y el uso de la

información por parte de las autoridades competentes para prevenir, investigar y reprimir los delitos fruto de la creación de un espacio de libre circulación de personas[263].

El cambio de milenio vino marcado por los trágicos atentados de Nueva York en 2001, seguidos -dos y cuatro años más tarde respectivamente- por los de Madrid y Londres. Estos acontecimientos incrementaron la preocupación por la seguridad pública y pusieron de manifiesto, por un lado, el alcance internacional de la amenaza y, por otro, que uno de los elemento clave en la lucha contra el terrorismo es el uso de los datos personales recopilados. Sin embargo, faltaban en la cooperación policial estándares comunes de protección. Reflejo de esta realidad fue el Convenio de Prüm[264], que contenía disposiciones sobre el intercambio de datos (relacionados con el ADN, huellas dactilares, matrículas de los vehículos, etc) entre un pequeño grupo de Estados miembros. No obstante, dicho Tratado sería plenamente incorporado al ámbito

[263] El Convenio Europol se firmó el 26 de julio de 1995, basado en el artículo K.3 del Tratado de la Unión Europea. DOC 316, de 27 de noviembre de 1995. La Oficina Europea de Policía no comenzó sus actividades de manera oficial hasta el 1 de julio de 1999. La creación de un espacio de libre circulación de personas fue el resultado de la celebración de dos acuerdos: el Acuerdo de Schengen de 14 de junio de 1985, y el Convenio de aplicación del Acuerdo de Schengen, que se firmó el 19 de junio de 1990 y entró en vigor el 26 de marzo de 1995. Este último (firmado únicamente por Alemania, Bélgica, Francia, Luxemburgo y los Países Bajos) apuntaba a la cooperación intergubernamental en los ámbitos de la justicia e interior. El incremento de la delincuencia organizada a nivel internacional reclamaba una mayor cooperación entre los Estados. En el Título IV del mencionado Convenio, se creaba el Sistema de Información de Schengen (SIS). Su desarrollo permitió a las autoridades nacionales en materia judicial y de control de fronteras intercambiar datos y obtener información sobre determinadas categorías de personas y de bienes, mediante una base de datos, en aras a la prevención de la criminalidad. El protocolo número 2 anejo al Tratado de Ámsterdam (1997) determinó la transferencia del "acervo de Schengen" al marco jurídico de la Unión Europea. El acervo Schengen figura impreso en su totalidad en el DOUE L 239, de 22 de septiembre de 2000.

[264] Firmado el 27 de mayo de 2005 por Alemania, Austria, Bélgica, España, Francia, Holanda y Luxemburgo. A él se unieron paulatinamente otros Estados: Bulgaria, Estonia, Finlandia Hungría, Rumania, Eslovaquia y Eslovenia.

de la Unión a través de la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008[265].

La multiplicación de normas comunitarias de intercambio de datos de carácter personal con fines penales fue relevando a un segundo plano la garantía de los derechos a la intimidad y protección de datos de los ciudadanos. Había más preocupación por la seguridad pública que por la protección de los derechos fundamentales.

De ahí que, como reacción ante este contexto normativo, se presentara en el año 2006 la iniciativa legislativa que se aprobaría como la Decisión Marco 2008/977/JAI, de 27 de noviembre de 2008, de protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. No obstante, aunque este proyecto se concibió para colmar la falta de una regulación general en la materia, lo cierto es que este instrumento, por su propia naturaleza y por no derogar ni modificar la normativa anterior, no tuvo repercusión práctica en aras a una postura más garantista[266]. Habría que esperar al período posterior a la firma del Tratado de Lisboa para que se materializaran las aspiraciones por un mayor respeto al derecho a la protección de datos de carácter personal en el ámbito penal.

---

[265] Otros instrumentos *ad hoc* de tratamiento de datos importantes en el ámbito de la cooperación policial y judicial penal fueron, sin ánimo exhaustivo, la unidad europea de cooperación judicial (EUROJUST) y los sistemas de información de visados (SIV) de comparación de huellas dactilares (EURODAC), de información aduanera (SIA) o el de información europeo de antecedentes penales (ECRIS).

[266] *Vid.* sobre los déficits de la Decisión, OUBIÑA BARBOLLA, S.: "Cambio de enfoque en la cooperación judicial penal y policial en la UE en relación con la transmisión de datos personales: las nuevas propuestas normativas y la STJUE de 8 de abril de 2014", en COLOMER HERNÁNDEZ, I. (dir.), OUBIÑA BARBOLLA, S. (dir.): *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Cizur Menor (Navarra), Aranzadi, 2015, págs. 81-91.

En el ámbito económico, la importancia que el tratamiento de datos iba a tener en el tráfico comercial llevó a las instituciones europeas a ocuparse de la protección de datos de una manera general y garantista. Los textos comunitarios más relevantes en esta notable labor homogeneizadora han sido la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995, sobre la protección de las personas físicas en los que respecta al tratamiento de datos personales y a la libre circulación de datos, y el Reglamento (CE) nº 45/2001, del Parlamento Europeo y el 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.

En primer término, la idea de una Directiva de protección de datos se remonta al año 1975, cuando el Parlamento Europeo aprueba una Resolución sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática. En la misma se afirmaba la conveniencia de elaborar "con toda urgencia" una Directiva sobre "la libertad individual y la informática, no solo para asegurar a los ciudadanos de la Comunidad la mejor protección posible contra los abusos o los fallos de los métodos de tratamiento de los datos, sino igualmente para evitar la elaboración de legislaciones nacionales contradictorias"[267].

Se inició así un largo proceso que culminaría en octubre de 1995. A lo largo de su elaboración, surgieron ciertas dudas en cuanto a la competencia de

[267] DOC 60, de 13 de marzo de 1975. *Vid*. HEREDERO HIGUERAS, M.: *La Directiva Comunitaria de Protección de datos de carácter personal,* Aranzadi, Pamplona, 1997, págs. 17-18.

la Comunidad Europea para intervenir en este ámbito. Precisamente, el ámbito de aplicación de la Directiva planteó problemas de interpretación que fueron resueltos por la STJCE de 20 de mayo de 2003, caso Österreichischer Rundfunk[268]. Se cuestionaba si entraba dentro del ámbito de aplicación de la Directiva la obligación que imponía la Ley Federal austríaca de recoger datos sobre los ingresos de ciertos empleados públicos con el fin de incluirlos y publicarlos en el informe anual del Tribunal de Cuentas austríaco. En las conclusiones presentadas por el Abogado General[269], afirma que esta actividad no era competencia de la Comunidad Europea, pues se estaría atribuyendo a la Directiva, además de la finalidad de promover la libre circulación de datos personales, el objetivo ulterior de garantizar la tutela del derecho a la protección de datos personales. No obstante, el Tribunal entiende aceptable acudir al artículo 100 A del TCE como base jurídica para amparar las medidas dirigidas a garantizar la libre circulación entre Estados miembros de los datos personales mediante la armonización de las normas nacionales que protegen a las personas físicas en lo que respecta al tratamiento de estos datos[270]. Asimismo, la propuesta de Directiva sufrió diversas modificaciones, dada la dificultad de armonizar los sistemas de los Estados miembros[271].

La norma partía de una realidad evidente: en la Comunidad se recurría cada vez más al tratamiento de datos personales en los diferentes sectores de

---

[268] Sentencia del Tribunal de Justicia de 20 de mayo de 2003, asunto C-465/00 - Österreichischer Rundfunk y otros.

[269] Conclusiones del Abogado General Sr. Antonio Tizziano de 14 de noviembre de 2002. Asunto C-465-00 *(*Rechnungchof contra Ósterreichischer Rundfunk y otros) y asuntos acumulados C138/01 y C139/01 (Neukomm y Lauermann contra Österrichischer Rundfunk).

[270] Sobre esta sentencia, *vid.* ARENAS RAMIRO, M.: *op.cit.,* pág. 246; GUERRERO PICÓ, M. C.: *op. cit.,* págs. 66-71 y PIÑAR MAÑAS, J. L.: *op. cit*., págs. 58-59.

[271] *Vid*, sobre el proceso de su elaboración y aprobación, CONDE ORTIZ, C.: *op. cit.*, págs. 37-45 y págs. 53-55.

la actividad económica y social. Las diferencias en los niveles de protección de los derechos y libertades de las personas en el tratamiento de datos personales, debido a la disparidad legislativa, estaban obstaculizando el ejercicio de una serie de actividades económicas a escala comunitaria. En este tenor, Guerrero Picó afirma que, a diferencia del Convenio 108 al que completa, la Directiva no es directamente un instrumento de protección de los derechos de las personas, sino que se concibe como una herramienta para impedir las trabas a la libre circulación de información personal en el contexto del mercado interior[272]. Con todo, a la vista de las Resoluciones que precedieron su elaboración, sí podemos concluir que existía en las instituciones europeas la inquietud de que se garantizase al mismo tiempo la protección de datos entre los derechos fundamentales de las personas[273].

La Directiva 95/46/CE se basa en los principios enunciados en el Convenio 108 del Consejo de Europa, si bien los concreta y en algunos casos los amplía[274]. Precedida por 72 considerandos a modo de preámbulo, vino a mejorar la redacción de dicho Convenio, fundamentalmente en cuanto que superaba la generalidad del mismo, respondía a los avances de las tecnologías

[272] GUERRERO PICÓ, M. C.: *op. cit.*, pág. 63.
[273] Así, por ejemplo, en la Resolución de 9 de marzo de 1982, del Parlamento Europeo sobre la protección de los derechos de las personas ante el desarrollo de los progresos técnicos en el ámbito de la informática, se afirma: "12. se puede contemplar fundadamente la posibilidad de considerar si el derecho a la protección de datos personales puede y debe figurar expresamente, como derecho del hombre y derecho fundamental, en la lista del Convenio europeo de derechos humanos y libertades fundamentales bajo la forma de un sexto protocolo adicional".
[274] *Vid*. considerando 11 de la Directiva 95/46/CE.

de la información y trataba de paliar los efectos de la disparidad de las legislaciones de los Estados miembros[275].

Vale la pena destacar, asimismo, la creación del Grupo de protección de las personas en lo que respecta al tratamiento de sus datos personales, "Grupo del artículo 29"[276], como se le denominó en la práctica, al que se atribuyeron funciones de control y vigilancia del cumplimiento de la Directiva. Se trata de un órgano consultivo independiente en materia de protección de datos y vida privada, establecido en virtud del referido precepto de la norma comunitaria. El Grupo estaba compuesto por representantes de las autoridades nacionales de protección de datos de los Estados miembros, de la autoridad creada por las instituciones y organismos comunitarios y de la Comisión.

Todas estas exigencias encontraron su correlativa garantía en sectores específicos, como el de las comunicaciones electrónicas[277], y en el sometimiento de las instituciones de la Unión Europea a la normativa sobre protección de datos a través del Reglamento 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre de 2001. Del contenido de este último, muy similar a la Directiva 95/46/CE, conviene resaltar la creación de una autoridad

---

[275] A pesar del espíritu de la Directiva, las diferencias entre los ordenamientos jurídicos subsisten. A este respecto, BRU CUADRADA, E.: “La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad”, *IDP*, núm. 5, 2007, contiene una comparativa del régimen sancionador de las legislaciones de protección de datos de España, Alemania, Francia, Italia y Suecia.

[276] http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

[277] Directivas 97/66/ CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 sustituida por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002. La Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre conservación de datos generados y tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, fue declarada invalida por el Tribunal de Justicia de la Unión Europea mediante sentencia de 8 de abril de 2014, asunto C-293/12 -Digital Rights Ireland, por constituir una injerencia de especial gravedad en la vida privada y la protección de datos.

de control independiente, el Supervisor Europeo de Protección de datos (capítulo V)[278]. Este órgano es el encargado de velar por que los derechos y libertades fundamentales de las personas físicas, en particular, su intimidad, en el tratamiento de los datos de carácter personal, sean respetados por los organismos comunitarios. Nombrado por el Parlamento y el Consejo conjuntamente por un período de cinco años, supervisa la aplicación de las disposiciones del Reglamento y asesora en todas las cuestiones relacionadas con la protección de datos. Entre otras competencias, está legitimado para intervenir en los asuntos presentados ante el Tribunal de Justicia de la Unión Europea[279].

Pero, sin lugar a dudas, el paso de gigante en esta materia lo marcó la aprobación de la Carta de Derechos Fundamentales de la Unión Europea, aprobada en el Consejo de Niza el 18 de diciembre de 2000[280.] Tras el fracaso de la Constitución Europea, el Tratado de Lisboa, firmado el 13 de diciembre de 2007, confirmó la competencia de la Unión Europea en esta materia[281]. El artículo 16 del TFUE ratifica su título competencial en lo que a protección de datos se refiere y el artículo 6 del TUE atribuye a la Carta el mismo valor jurídico que los Tratados[282].

---

[278] De conformidad con el artículo 286 del Tratado de la Comunidad Europea.

[279] *Vid*. artículo 47 del Reglamento 45/2001. La Decisión 1247/2002/CE del Parlamento Europeo, del Consejo y de la Comisión, de 1 de julio, establece el estatuto y las condiciones generales del ejercicio de las funciones del Supervisor.

[280] DOUE C 364, de 18 de diciembre de 2000.

[281] Artículo 16 B que modifica el artículo 286 del Tratado de la Comunidad Europea. DOUE núm. 306, de 17 de diciembre de 2007.

[282] La Carta se incorporó al TUE a través de la referencia en el artículo 6.1. La postura adoptada por Reino Unido y Polonia se tradujo en la imposibilidad de incluir la Carta en el Tratado de la Unión Europea y dio lugar a la aprobación de un Protocolo sobre la aplicación de la Carta de los Derechos Fundamentales de la Unión Europea a estos dos países.

Los rápidos avances tecnológicos de las últimas dos décadas han planteado nuevos desafíos para la protección de datos personales. Desde el 25 enero de 2012 se venían tramitando por el procedimiento legislativo ordinario sendas propuestas de la Comisión Europea de nuevos actos normativos[283]. Tras una larga tramitación parlamentaria, han cristalizado en el Reglamento General de Protección de Datos (UE) 2016/679 y en la Directiva sobre protección de datos en el ámbito penal (UE) 2016/680, publicados en el Diario Oficial de la Unión Europea.núm. 119, de 4 de mayo de 2016. No obstante, el Reglamento General de Protección de Datos se aplicará a partir del 25 de mayo de 2018 y la transposición de la Directiva debe hacerse en cada Estado miembro, a más tardar el 6 de mayo de 2018.

La elección de la fuente reglamentaria como medio para regular la protección de datos no carece de trascendencia, pues esta norma jurídica es directamente aplicable en los Estados miembros. El objetivo es mantener un marco normativo único para toda la Unión Europea, uniformando el régimen jurídico actual, así como facilitar la libre circulación de datos personales en el marco de la Unión Europea y con otros países e instituciones internacionales[284]. El Reglamento se fundamenta en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, que, al tiempo que reconoce el derecho a la protección de datos de carácter personal, hace referencia a la libre circulación de los datos. Esta circunstancia no es baladí, y debe interpretarse en el sentido de que la

[283] Sobre esta materia *vid.* RALLO LOMBARTE, A. y GARCÍA MAHAMUT, R. (ed.): *Hacia un nuevo Derecho Europeo de Protección de Datos,* Tirant lo Blanch, Valencia, 2015.
[284] Considerandos 7, 9 y 10 RGPD.

libre circulación de los datos personales en la Unión debe, en todo caso, respetar el contenido del derecho a la protección de datos[285].

Por tanto, la Unión Europea se toma en serio la salvaguardia del derecho a la protección de datos personales y, además, está decidida a que se cumpla de manera uniforme en todo su territorio, lo que va a provocar un cambio radical en el sistema de protección de datos de carácter personal, ya que pasamos a un único marco legislativo europeo de referencia en esta materia. Para Piñar Mañas, el Reglamento introduce un nuevo modelo, que pasa de la gestión de los datos al uso responsable de la información. Esto se aprecia en cuestiones tales como el principio de *accountability,* traducido por «responsabilidad proactiva», los principios de privacidad desde el diseño y por defecto, la aproximación a la protección de datos basada en el análisis de riesgos, la figura del Delegado de protección de datos, el fortalecimiento de los códigos de conducta, la exigencia de llevar un registro de actividades del tratamiento o la regulación de las medidas de seguridad, entre otras[286].

Esto último, unido a la labor, tanto de la jurisprudencia del Tribunal Europeo de Derechos Humanos, como del Tribunal de Justicia de la Unión Europea, seguramente influya en el futuro en la configuración constitucional del derecho fundamental a la protección de datos de carácter personal, que habrá de ser perfilada en España por el Tribunal Constitucional. Como puede apreciarse, el Reglamento se inscribe en lo dispuesto en la Carta de Derechos Fundamentales de la Unión y en la jurisprudencia que ha dictado el Tribunal de

---

[285] PIÑAR MAÑAS, J. L.: *op. cit.*, pág. 60.
[286] PIÑAR MAÑAS, J. L.: "Introducción: hacia un nuevo modelo europeo de protección de datos", en AA.VV.: *Reglamento general…,* pág. 16.

Justicia de la Unión Europea. En realidad, el Reglamento tiene en cuenta la jurisprudencia desarrollada en sentencias tales como Google Spain, relativa al derecho al olvido (C-131/12), Digital Rights Ireland, que anuló la Directiva sobre conservación de datos en materia penal (C-293/12 y C-594/12) o Schrems, que cuestiona la protección de datos personales transferidos por Facebook desde Irlanda a Estados Unidos (C-362/14).

En el ámbito interno, cumpliendo el mandato constitucional de limitar el uso de la informática, el legislador aprobó -catorce años más tarde- la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, que incorpora el contenido del Convenio 108 sobre Protección de Datos Personales del Consejo de Europa. Para transponer al ordenamiento interno la Directiva 95/46/CE, sobre Protección de datos personales, la LORTAD sería reemplazada por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Esta disposición nació con el objetivo de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, su honor e intimidad personal y familiar. El objeto de la Ley no puede ser otro, en palabras del Tribunal Constitucional, que la protección de los datos personales[287]. Esta norma no persigue poner límites al uso de las nuevas tecnologías, sino buscar el equilibrio entre Internet y la protección de los derechos fundamentales.

El legislador orgánico estableció, esencialmente, los principios que deben regir cualquier tratamiento de datos personales, los derechos de los

[287] STC 290/2000, FJ 11 *in fine.*

titulares de los mismos, las disposiciones sobre creación de ficheros, tanto públicos como privados, y la creación de la Agencia Española de Protección de Datos, teniendo en cuenta que, respecto a estas dos últimas materias, la Disposición final segunda de la LOPD[288] dispone que las normas que las regulan no tienen carácter orgánico, pues no constituyen el desarrollo en sentido estricto del derecho fundamental. En estas materias, las Comunidades Autónomas son competentes para aprobar normas legales.

Junto a esto, el ejecutivo ha elaborado toda una normativa de desarrollo a través del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de la LOPD. Además, existe una normativa sectorial específica precedente que conforma un sistema mixto en el cual la ley general ha quedado como norma supletoria.

Con la aprobación del Reglamento europeo de protección de datos, se conserva la normativa estatal, horizontal y sectorial, en materia de protección de datos[289]. La Ley Orgánica y su reglamento no pueden considerarse derogados, aunque sí desplazados en muchos ámbitos por la normativa europea. Cabe, en este sentido, precisar que el RGPD no se aplica en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión. Además, este instrumento permite que los Estados miembros incorporen a su derecho nacional elementos del mismo en la medida en que sea necesario por razones de coherencia y para que las disposiciones

[288] Disposición Final segunda de la LOPD: "Los Títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria".

[289] Sobre la normativa horizontal *vid*. artículos 2.3 y 4 RGPD, en relación con el Reglamento 45/2001 sobre los tratamientos realizados por las instituciones europeas, y la Directiva 2000/31/ CE, sobre comercio electrónico.

nacionales sean comprensibles para sus destinatarios (considerando 8). Al propio tiempo, concede amplios márgenes de maniobra a los Estados para concretar a escala nacional sus disposiciones[290].

[290]A tales efectos debe tenerse en cuenta que se encuentra en tramitación en el Congreso de los Diputados el Proyecto de una nueva Ley Orgánica que complemente en este sentido el Reglamento Europeo.

Capítulo segundo

EL DERECHO AL OLVIDO DIGITAL

1. LOS DERECHOS RELACIONADOS CON EL PRINCIPIO DE CALIDAD DE LOS DATOS. 2. EL DERECHO AL OLVIDO. 3. EL DERECHO AL OLVIDO DIGITAL.

1. LOS DERECHOS RELACIONADOS CON EL PRINCIPIO DE CALIDAD DE LOS DATOS.

El principio de calidad de los datos, tal y como se recoge en el artículo 4 de la LOPD[291], toma su contenido del artículo 5 del Convenio 108 y del artículo 6 de la Directiva 95/46/CE.

El Convenio 108 del Consejo de Europa había recogido entre los principios relativos al tratamiento de la información el de calidad de los datos (art. 5), definido como aquel en virtud del cual los datos de carácter personal objeto de un tratamiento automatizado se obtendrán y tratarán leal y legítimamente; se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; deberán ser adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado, además de exactos y si fuera necesario puestos al

[291] Artículo 4 de la LOPD. Calidad de los datos."1. Los datos de carácter personal solo 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. 2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos. 3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan como veracidad a la situación actual del afectado. 4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16 .5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos".

día; y, finalmente, se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Paralelamente se contemplaban entre las garantías de la persona afectada la de obtener, llegado el caso, la rectificación de los datos o el borrado de los mismos, cuando se hubieran tratado con infracción de las disposiciones del derecho interno que hubieran hecho efectivos los principios básicos enunciados en los artículos 5 y 6 del Convenio[292]. Este último hace referencia a los datos sensibles: “Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales".

En el marco de la Unión Europea, la Directiva 95/46/CE de 24 de octubre, del Parlamento Europeo y del Consejo, sobre protección de datos personales, regulaba el principio de calidad de los datos en términos muy similares a los expuestos en el Convenio 108, determinando expresamente que los Estados miembros dispondrán que los datos personales sean: a) tratados de manera leal y lícita; b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados

[292] Artículo 8.c) del Convenio 108.

miembros establezcan las garantías oportunas; c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados; e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos. 2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1. Este principio pretende asegurar a los individuos que sus datos personales no se van a mantener indefinidamente, con el consiguiente riesgo de poder ser utilizados en cualquier momento, condicionando todas sus actividades.

El principio de calidad de los datos es parte del contenido esencial del derecho fundamental a la protección de datos, tal y como ha sido reconocido en la Carta de Derechos Fundamentales de la Unión Europea. Así, conforme al artículo 8.2 de la CDFUE, "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".

En el mismo sentido, en el espacio del derecho de la Unión Europea, el Reglamento General de Protección de Datos ha recogido el principio de calidad

tanto en el momento de recogida de los datos, como en su posterior tratamiento, e incluso para el momento de la cancelación de los mismos por haberse cumplido la finalidad para la que fueron recabados o porque fuera procedente su borrado[293]. Bajo el título de "principios relativos al tratamiento", el artículo 5 de esta norma recoge el principio de calidad de los datos desglosado en siete apartados, que se concretan en: licitud, lealtad y transparencia; limitación de la finalidad, minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad. Se impone la adopción de todas las medidas que sean razonables para suprimir o rectificar sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

Con base en estas premisas, podemos afirmar que un tratamiento de datos personales, para ser legítimo, debe apoyarse en el consentimiento del afectado o en otro fundamento legal, pero, además, debe respetar el principio de calidad, lo que implica que los datos que se procesan deben ser fieles a la finalidad concreta para la que se obtienen. Desde esta perspectiva, los datos personales registrados deben ser adecuados, pertinentes y no excesivos para el fin para el que han sido recabados, al propio tiempo que la finalidad del tratamiento debe ser igualmente legítima, determinada y explícita. En particular, la finalidad debe respetar la Constitución y la Ley. No es suficiente para la legalidad del tratamiento que el interesado hubiera prestado su consentimiento, si la finalidad del mismo no es legítima.

[293] PUYOL MONTERO, J.: ”Los principios del derecho a la protección de datos”, en AA. VV.: *Reglamento General de Protección de datos*…, págs. 138-139.

Además, el principio de calidad de los datos hace necesario, en todo caso, que los datos sean exactos y respondan con veracidad a la situación actual del afectado. Con la finalidad de conseguir que el tratamiento de los datos personales sea fiel reflejo de la realidad, este principio impone a los responsables de los tratamientos la obligación de velar por la exactitud, actualidad y veracidad de los datos registrados, en relación con las finalidades para las que se hayan obtenido[294].

Directamente ligado a este principio están, por tanto, los derechos de rectificación y cancelación[295]. En la Directiva, el derecho de cancelación se contemplaba en el artículo 12 b) y c) junto con el derecho de rectificación, como la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la normativa europea, en particular a causa del carácter incompleto o inexacto de los datos. La Directiva no ofrecía más criterio para definir el concepto de bloqueo que su inclusión en el concepto de tratamiento (art 2.b). El derecho de bloqueo fue una novedad introducida por la Directiva que implica identificar los datos almacenados con el fin de restringir su ulterior uso. El derecho de cancelación adquirió perfil propio durante la prolongada vigencia de la Directiva 95/46/CE.

---

[294] Sobre el deber de actualización, *vid.* el comentario al artículo 4 LOPD de APARICIO SALOM, J.: "La calidad de los datos", en AA. VV.: *Comentario a la Ley Orgánica de Protección de datos de carácter personal*, Aranzadi, Cizur Menor (Navarra), 2010, págs. 330-336. Especial mención merecen los ficheros sobre solvencia patrimonial y de crédito regulados en el artículo 29 LOPD. *Vid.* sentencia del Tribunal Supremo (Sala de lo Civil, Sección 1ª) de 21 mayo de 2014 y sentencia del Tribunal Supremo (Sala de lo Civil, Sección 1ª) de 1 de marzo de 2016.

[295] Artículo 16 de la LOPD y artículos 31 y siguientes del RLOPD. En el RGPD se contemplan en la sección 3, artículo 16 derecho de rectificación y artículo 17 derecho de supresión ("el derecho al olvido"). En el Proyecto de ley orgánica de protección de datos de 24 de noviembre de 2017 en los artículos 14 y 15 respectivamente.

Los derechos de rectificación y cancelación forman parte del contenido esencial del derecho a la protección de datos como resulta de la STC 292/2000. El principio de calidad de los datos permite al interesado exigir la rectificación en el supuesto de datos inexactos o incompletos; en tanto que podrá solicitar la cancelación, cuando los datos sean inadecuados o excesivos en relación con la finalidad perseguida por el tratamiento o este se lleve a cabo al margen de la normativa vigente. Ambos derechos contemplados desde la perspectiva del principio de calidad de los datos se convierten en una obligación para el responsable del tratamiento pues en el caso de que tenga constancia de la existencia de datos incompletos o inexactos, deberá proceder de oficio a su sustitución por los datos rectificados o completados. Al propio tiempo, cuando dejen de ser necesarios o pertinentes para la finalidad para la que se hubiesen recabado, deberá proceder a cancelarlos[296]. En el primer supuesto, por tanto, el responsable persiste en el tratamiento de los datos rectificados o completados, mientras que en el segundo caso cesa en el uso de los mismos, al suprimirlos.

Sobre la base del RLOPD, podemos definir el derecho de rectificación como la facultad que tiene el afectado de obtener la modificación y actualización de aquellos datos que resulten inexactos o incompletos. En particular, el derecho de cancelación dará lugar a que se supriman aquellos datos personales que sean inadecuados, innecesarios o excesivos[297].

El ejercicio del derecho de cancelación tiene como propósito último la desaparición física de los datos, su eliminación, lo que supone necesariamente

[296] *Vid.* artículo 4.4 y 4.5 LOPD.
[297] *Vid*. artículo 31 RLOPD.

el cese en el uso de los mismos. La rectificación, por el contrario, responde a una necesidad de corregir o completar una información.

El interesado, al ejercitar los derechos de rectificación y/o cancelación, deberá indicar al responsable del fichero a qué datos se refiere, además de acompañar la documentación que justifique su solicitud. El responsable del fichero resolverá en el plazo de diez días desde su recepción[298]. Transcurrido el plazo sin recibir respuesta, el afectado podrá interponer reclamación ante la AEPD u órgano autonómico equivalente.

En caso de cesión, el responsable del fichero deberá comunicar que los datos han sido rectificados o cancelados al cesionario para que proceda a rectificarlos o cancelarlos[299].

En cuanto a sus efectos, tras el ejercicio del derecho de rectificación el dato seguirá existiendo, pero corregido, completado o, en su caso, actualizado, mientras que tras el ejercicio del derecho de cancelación se suprimirá. La rectificación no conlleva la cancelación de los datos[300]. Para Marc Carrillo, rectificar, en relación con la veracidad informativa, es reducir una cosa a la exactitud que debe tener, por lo que su ámbito parece contraerse al mundo de los hechos[301]. Como consecuencia de la cancelación, el responsable cesa en el uso de los datos.

---

[298] *Vid*. artículo 16.1 LOPD.
[299] *Vid.* artículo 16.4 LOPD.
[300] GUERRERO PICÓ, M. C.: *El impacto de Internet en el*…, pág. 298.
[301] CARRILLO, M.: "Derecho a la información y veracidad informativa (Comentario a las SSTC 168/86 y 6/88)", *REDC*, núm. 23, 1988, pág. 191.

No obstante, la LOPD adolece de poca claridad en esta materia al disponer que la cancelación dará lugar al bloqueo de los datos[302]. En ocasiones, la interrupción en el tratamiento de los datos puede ocurrir sin que se haya procedido previamente a la eliminación de los datos. Ello se da cuando se produce el bloqueo[303], que es un paso previo a la supresión, es decir, una situación transitoria que surge cuando no se pueda proceder inmediatamente ella. Por ejemplo, se puede dar cuando a pesar de haber desaparecido la finalidad para la que fueron recabados los datos, estos deban conservarse para finalidades históricas, estadísticas o científicas. En palabras de la AEPD, "existirán determinados supuestos en que la cancelación o bien no podrá tener lugar, dada la obligación de conservación impuesta por la Ley, o bien deberá suponer una fase previa de bloqueo de los datos que, produciendo unos efectos similares al borrado físico de los mismos, salvo en determinadas circunstancias, no implicará automáticamente ese borrado"[304]. Es decir, el bloqueo también obliga al titular del fichero a no disponer de los datos, si bien sin llegar a suprimirlos, sino manteniendo la información, pero sometida a condiciones que garanticen el derecho del afectado a la protección de sus datos de carácter personal.

Procederá el bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para atender las responsabilidades surgidas del tratamiento y durante el plazo de

---

[302] Artículo 16.3 LOPD.
[303] Artículo 32 del Proyecto de Ley Orgánica de Protección de Datos de 24 de noviembre de 2017.
[304] *Vid*. el informe de la AEPD 2001-0000 sobre el bloqueo de los datos de carácter personal, pág. 2. http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/derecho_acceso_rectificacion_cancelacion_oposicion/common/pdfs/2001-0000_Bloqueo-de-datos-de-car-aa-cter-personal.pdf

prescripción de estas, pues, una vez finalizado aquel, los datos deberán suprimirse. Las causas del bloqueo deberán fundarse en lo establecido "en las disposiciones aplicables" o "para la atención de las posibles responsabilidades nacidas del tratamiento", tal y como prevé la LOPD[305]. En este sentido, el mantenimiento del dato bloqueado supone una excepción al borrado físico del mismo, que, en definitiva, es el fin último de la cancelación. Por consiguiente, ha de tenerse en cuenta que la STC 292/2000 viene a imponer, expresamente, el principio de reserva de Ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier causa que justifique el bloqueo de los datos, como restricción al derecho de cancelación, deberá constar en una disposición con rango de Ley para que dicho bloqueo pueda considerarse lícitamente efectuado[306].

Finalmente, también son supuestos que pueden dar lugar a la cancelación de los datos los casos de revocación del consentimiento.

Íntimamente conectado con los derechos anteriores, está el derecho de oposición del interesado al tratamiento de sus datos personales. El Tribunal Constitucional lo define como la facultad de exigir a quien corresponda que ponga fin a la posesión y el uso de nuestros datos personales (STC 290/2000 FJ 7). Se reconoce por la LOPD el derecho del afectado a que no se lleven a cabo tratamientos de sus datos personales o bien a que no se continúe con el

[305] *Vid.* artículo 16.3 y 5 LOPD.
[306] Así, a título de ejemplo, podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento, en los términos previstos por la legislación civil o mercantil. *Vid.* informe AEPD 2001-0000.

mismo[307]. Los supuestos en los que procede el ejercicio de este derecho son en primer lugar, cuando para el tratamiento de los datos no sea necesario el consentimiento del afectado haciendo constar los motivos fundados y legítimos relativos a su concreta situación personal y siempre que una ley no disponga lo contrario; igualmente, cuando se trate de ficheros con fines publicitarios y de prospección comercial; en tercer y último lugar, cuando el tratamiento tenga por finalidad la adopción de decisiones basadas únicamente en el tratamiento automatizado. La relevancia de este supuesto, al que el legislador le dedicó un precepto específico[308], estriba en reconocer al afectado el derecho a impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento automatizado de la información personal.

Definidas de conformidad con la LOPD las facultades de rectificar, cancelar y oponerse que tiene el titular de los datos, hemos de advertir cómo estas, y en particular el derecho de cancelación, están sujetas a límites. El derecho de cancelación presenta excepciones, entre otras razones por motivos históricos, estadísticos o científicos. De la misma manera, no procederá la cancelación cuando así este previsto por la ley o en la relación contractual o por razones interés de público previstas en la normativa sectorial.

En el ámbito del derecho de la Unión Europea, el RGPD contempla los derechos de rectificación, supresión ("el derecho al olvido") y oposición, al tiempo que ha ampliado el catálogo de facultades del interesado, al contemplar

[307] Artículo 6.4 LOPD. Artículo 18 del Proyecto de Ley Orgánica de Protección de Datos de 24 de noviembre de 2017.
[308] Artículo 13 LOPD.

otros derechos, como la limitación del tratamiento, en el Capítulo III, sección tercera y cuarta. Así, cuando los datos sean inexactos el interesado tendrá derecho a obtener sin dilación su rectificación, así como, en caso de resultar incompletos, su suplemento.

Una de las novedades que introduce el Reglamento europeo de protección de datos en la materia que nos ocupa es que sustituye la denominación "derecho de cancelación" por la de "derecho de supresión". La supresión en sí misma implica un tratamiento de datos de carácter personal[309]. Regulado en el artículo 17 de manera más amplia que la del tradicional derecho de cancelación, este derecho se traduce en una obligación de cese en el tratamiento y borrado de los datos para todo responsable del mismo en determinados supuestos, entre los que se incluye el derecho al olvido digital, entendiendo por tal la supresión en el contexto de los motores de búsqueda u otros responsables del tratamiento en Internet.

En relación con su contenido, el ejercicio de este derecho implica la solicitud de que se supriman los datos personales sin dilación indebida en los siguientes cuatro supuestos: si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, lo que resulta en intima conexión con la minimización de los datos como manifestación del principio de calidad; si los interesados han retirado su consentimiento para el tratamiento y este no se basa en otro fundamento jurídico (este derecho es pertinente, en particular, si el interesado dio su consentimiento siendo menor de edad, no siendo

[309] Artículo 4 RGPD.

plenamente consciente de los riesgos que implicaba el tratamiento[310]) ; si el interesado se opone al tratamiento de datos personales que le conciernen[311] o si, finalmente, el tratamiento de datos personales incumple de otro modo el Reglamento General de Protección de Datos.

Además, como señala Berrocal Lanzarot[312], con el fin de reforzar el "el derecho al olvido", el derecho de supresión se amplía de tal forma que además de la supresión de los datos, el responsable del tratamiento que haya hecho públicos los datos personales y esté obligado a su borrado deberá indicar a los responsables del tratamiento que estén tratando tales datos personales que, supriman todo enlace a ellos, o las copias o réplicas de tales datos siendo esta una obligación accesoria de información que acompaña a la principal de supresión.

Teniendo en cuenta la tecnología disponible y el coste de su aplicación, el responsable del tratamiento adoptará medidas razonables que posibiliten la supresión, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales, de la solicitud del interesado de

---

[310] Este inciso viene a llamar la atención sobre la necesidad de garantizar un “derecho al olvido” de los datos personales aparentemente inocuos que los menores cuelgan en Internet, pues el paso del tiempo y la perennidad de las informaciones en la red de seguro plantearán en el futuro inconvenientes que afectarán a su privacidad. *Vid.* PÉREZ LUÑO, A. E.: “La protección de datos personales del menor en Internet”, *Revista Española de Protección de Datos*, núm. 5, 2008, pág. 166.

[311] El interesado tendrá derecho a oponerse, en cualquier momento, por motivos relacionados con su situación personal, a que sus datos personales sean objeto de tratamiento basado en el cumplimiento de una misión realizada, en interés público; o en el ejercicio de los poderes públicos conferidos al responsable del tratamiento; o para la satisfacción de intereses legítimos perseguidos por este o por un tercero; o cuando el tratamiento tenga por objeto la mercadotécnica directa, incluida la elaboración de perfiles (art. 21 RGPD).

[312] BERROCAL LANZAROT, A. I.: *El derecho de supresión de datos o derecho al olvido,* Reus, Madrid, 2017, pág. 233.

supresión (artículo 17.2 RGPD)[313]. Esto es positivo porque elimina la carga que supondría para el interesado localizar a todos los posibles cesionarios de los datos cuya cancelación o rectificación ha solicitado.

El apartado tercero del artículo 17 enumera los límites a la aplicación del derecho de supresión ("derecho al olvido"), que se dan cuando el tratamiento responda al ejercicio de las libertades de expresión o información; o bien sea necesario por imperativo legal o para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; o bien el tratamiento responda a razones de interés público en el ámbito de la salud pública o sea necesario con fines de archivo en interés público, de investigación científica o histórica o estadísticos; o, finalmente, cuando los datos sean tratados para la formulación, el ejercicio o la defensa de reclamaciones[314].

Completa este cuadro el derecho a la limitación del tratamiento que es un concepto novedoso definido como "el marcado de los datos de carácter personal con el fin de limitar su tratamiento en el futuro"[315]. Opera a solicitud del interesado e implica que no se aplicarán a los datos las operaciones de tratamiento que en su caso corresponderían.

Se trataría de una especie de bloqueo de los datos. Para ello, debe concurrir alguna de las siguientes condiciones: que el interesado haya ejercitado los derechos de rectificación u oposición y el responsable del

---

[313] En este sentido el párrafo 39 de la sentencia del Tribunal de Justicia de la Unión Europea del caso Google.
[314] Sobre los límites en el ejercicio del derecho de supresión de datos vid, BERROCAL LANZAROT, A. I.: *op. cit*., págs. 242-263.
[315] *Vid*. artículos 4.3) RGPD.

tratamiento esté en proceso de determinar si procede atender la solicitud; que el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos; finalmente, que los datos ya no sean necesarios para los fines del tratamiento, lo que determinaría su supresión, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.

Durante el plazo que dure la limitación, el responsable del tratamiento procede a conservar los datos. Solo podrán ser objeto de tratamiento con el consentimiento del interesado para la formulación, ejercicio o defensa de reclamaciones, para proteger los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro. Antes de concluir el plazo de la limitación, el interesado deberá ser informado por el responsable del levantamiento de la misma[316].

Entre los métodos para limitar el tratamiento de datos personales podemos encontrar los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, o bien en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio en Internet. En los ficheros automatizados, la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema[317].

La rectificación, la supresión o la limitación del tratamiento deberán ser notificadas a cada uno de los destinatarios a los que se hayan comunicado los

[316] Artículo 18 RGPD.
[317] *Vid.* considerando 67.

datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado.

La Comisión Europea de Derechos Humanos[318], al actuar como órgano de admisión de las demandas previo a la intervención del Tribunal Europeo de Derechos Humanos, tuvo ocasión de pronunciarse sobre la supresión de datos personales[319]. Así, entendió que procedía en relación con datos del pasado que pudieran dar lugar a la elaboración de un perfil del individuo que el interesado quería mantener en el olvido, o con respecto a datos personales pretéritos que habían dejado de ser necesarios para la finalidad para la que se recogieron y cuyo titular quería proceder a su destrucción. Curiosamente, son todos casos de inadmisión, resueltos por la Comisión y que no llegaron al Tribunal Europeo de Derechos Humanos.

En el caso Chave née Jullien contra Francia[320], la demandante fue internada en un hospital psiquiátrico durante cinco meses, en ejecución de una orden dictada por un órgano de gobierno regional[321] . El Tribunal de Apelación de París, en sentencia de 6 de noviembre de 1978, resolvió que aquel acto administrativo había sido ilegal y ordenó que la recurrente fuera indemnizada. El internamiento forzoso en un hospital psiquiátrico era, según el Tribunal, una

---

[318] La Comisión Europea de Derechos Humanos fue desde 1954 hasta la entrada en vigor del Protocolo 11 de la Convenio Europeo de Derechos Humanos el 31 de octubre de 1998, el órgano encargado de la admisión de los asuntos, pues los particulares no podían tener acceso directo al Tribunal Europeo de Derechos Humanos. De acuerdo con el Protocolo 11, la Comisión continuó en funciones durante un año más (hasta el 31 de octubre de 1999) para instruir los casos declarados admisibles antes de la entrada en vigor del Protocolo.

[319] Decisión de la Comisión de 5 de abril de 1995, caso Martin contra Suiza disponible en: http://hudoc.echr.coe.int/eng#{"fulltext":["Martin"],"documentcollectionid2":["DECISIONS"],"itemid":["001-26302"]}

[320] Decisión de la Comisión Europea de Derechos Humanos de 9 de julio de 1991 disponible en: http://hudoc.echr.coe.int/eng?i=001-24622

[321] Prefecto del Departamento de Vaucluse.

medida que implicaba un menoscabo grave para la persona, pues se había causado un perjuicio injustificado a la demandante, que era bien conocida en la población del mismo Departamento, donde había trabajado como maestra de escuela primaria. Considerando que la compensación concedida no constituía una reparación suficiente por el daño que había sufrido, la demandante alegó que el Estado francés le había denegado la reparación integral de la lesión producida por un internamiento confirmado como abusivo. En consecuencia, solicitó que el Tribunal declarara que el mantenimiento en un fichero de datos concernientes a tal internamiento constituía una injerencia en su derecho al respeto a la vida privada, así como que su nombre y sus datos se "borraran" (*disparaissent)* del registro central (*Fichier)* de los pacientes con enfermedad mental en el Departamento de Vaucluse y de cualquier otro registro.

En el procedimiento ante la Comisión, el Estado francés alegó, entre otras cuestiones, que el hecho de que el equipo médico de la institución hubiera tenido contacto con la demandante después de su ingreso involuntario no era una prueba de la existencia de un archivo de enfermos mentales en el servicio público de salud, sino que, simplemente, aquello entraba dentro del ejercicio normal del control médico del paciente. No obstante, el Gobierno admitió la existencia de un expediente de la demandante y de un registro en el establecimiento hospitalario donde fue internada. Estos documentos, según manifestó, no deberían ser asimilados a ficheros, porque tenían por finalidad proteger la salud y los derechos de los pacientes y, por otra parte, su utilización estaba estrictamente regulada por las normas, que preveían que no pudieran ser accesibles al público, sino solamente por las autoridades públicas en el marco de los límites de sus atribuciones. Sin embargo, la demandante planteó

a la Comisión la cuestión de la posible violación del Convenio por el mantenimiento en cualquier fichero de informaciones de carácter personal, concretamente las menciones relativas al internamiento psiquiátrico del que fue objeto.

La Comisión partió de la base de que el derecho de cancelación no es absoluto y ponderó los intereses en conflicto. En este sentido, argumentó que el expediente y el registro contenían indudablemente información relativa a la vida privada de la solicitante, y admitió que la conservación de estos datos podía considerarse como una interferencia con el respeto a su vida privada garantizada por el párrafo 1 del artículo 8 CEDH. Ahora bien, en cuanto a si estaba justificada a la luz del párrafo segundo, la Comisión alegó que cuando el Estado, para la protección de la salud y la de los derechos y libertades, autoriza el mantenimiento de los archivos y registros personales en el hospital donde se trata a las personas afectadas, debe proporcionar garantías eficaces contra el abuso. Así, la Comisión consideró que las garantías incorporadas en el sistema francés de supervisión (confidencialidad, no acceso al público, reserva de ley) cumplían con los requisitos del párrafo 2 del artículo 8 del CEDH. Por consiguiente, concluyó que la injerencia sufrida por la demandante no había sido desproporcionada con respecto al fin legítimo perseguido. La protección de la salud, en este caso, constituía una limitación al ejercicio del derecho de cancelación o borrado.

En relación con la recogida de datos personales consistentes en imágenes, en el caso X contra Reino Unido[322], el demandante reaccionó contra la conservación de unas fotografías suyas tomadas por la policía contra su voluntad, en el curso de una manifestación pacífica que tuvo lugar durante un partido de rugby y que la policía se había negado a destruir. La Comisión constató que las imágenes estaban relacionadas con un incidente público en el que el demandante participó voluntariamente y que fueron tomadas únicamente con el propósito de su futura identificación en eventos públicos similares. Asimismo, entendió que no había indicios de que las fotos se hubieran puesto a disposición del público en general o se hubieran destinado a cualquier otro propósito. Teniendo en cuenta estos factores, la Comisión concluyó que la toma y la retención de las fotografías del solicitante por parte de la policía no podía considerarse una injerencia en su vida privada en el sentido del artículo 8.

En el marco del derecho de la Unión Europea, el Tribunal de Justicia ha aplicado los criterios de enjuiciamiento utilizados por el Tribunal Europeo de Derechos Humanos para esclarecer si la injerencia en los derechos fundamentales contenidos en los artículos 7 -vida privada- y 8 -protección de datos personales- de la CDFUE era o no proporcionada en los términos del artículo 52.1 de la CDFUE. Merece la pena citar la STJUE de 8 de abril de 2014, dictada en los asuntos acumulados C-293/12 y C-594/12, Digitals Rights Ireland[323], que declaró inválida, a la luz de los citados preceptos de la CDFUE,

[322] Decisión de la Comisión Europea de Derechos Humanos de 12 de octubre de 1973, disponible en Internet: http://hudoc.echr.coe.int/eng?i=001-3184

[323] STJUE de 8 de abril de 2014, casos C-293/12 y C-594/12, Digitals Rights Ireland y Seitlinger y otros.

la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo, sobre la conservación de datos generados o tratados por los operadores de los servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones. La citada norma venía a modificar la Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas[324], que establecía la confidencialidad de las mismas y de los datos de tráfico de los abonados y usuarios, debiendo borrarse -o hacerse anónimos- una vez dejaran de ser necesarios para mantener la comunicación o la facturación. Por el contrario, la Directiva 2006/24/CE introdujo una profunda reforma de la normativa aplicable a los datos relativos a las comunicaciones electrónicas[325], al disponer un controvertido sistema de recopilación y almacenamiento de datos de telecomunicaciones que obligaba a los proveedores de dicha clase de servicios a conservar los datos de tráfico entre seis meses y dos años y a cederlos a las autoridades competentes, siendo su finalidad la de perseguir los delitos graves.

Siguiendo las directrices del abogado general Cruz Villalón[326], la sentencia aprecia que dicha obligación de conservación afecta de manera específica a los derechos a la vida privada y a la protección de datos de carácter personal[327]. Si bien la lucha contra el terrorismo es un objetivo de

---

[324] El Tribunal Supremo de Irlanda y el Tribunal Constitucional de Austria plantearon sendas peticiones de decisión prejudicial ante el Tribunal de Justicia de la Unión Europea: la primera, el 11 de junio de 2012, como consecuencia de la demanda presentada por la sociedad *Digital Rights* contra la normativa de aquel país que transpuso la directiva; la segunda, el 28 de noviembre de 2012, a raíz de la demanda interpuesta por el gobierno del *Land* de Carintia, los señores Seitlinger y Tschohl y otros 11.128 demandantes para pedir la anulación de un artículo de la Ley de telecomunicaciones introducido con motivo de la transposición de la Directiva 2006/24 al ordenamiento jurídico interno. *Vid.* OUBIÑA BARBOLLA, S.: *op. cit.,* pags. 109-120.
[325] Artículos 13.1 de la Directiva 95/46 y 15.1 de la Directiva 2002/58.
[326] Conclusiones presentadas el 12 de diciembre de 2013.
[327] *Vid.* STJUE 8 de abril de 2014, párrafo 37

interés general para la Unión Europea, este fin no puede justificar por sí solo una medida de conservación como la planteada. Por consiguiente, para el Tribunal de Justicia de la Unión Europea, la injerencia que implica la Directiva 2006/24/CE sobrepasaba los límites del principio de proporcionalidad y carecía de las garantías imprescindibles.

La sentencia, en fin, pone de relieve que la norma no establecía reglas claras y precisas que determinaran el alcance de la injerencia. En concreto, la obligación de conservación no se circunscribía a los datos estrictamente necesarios, pues afectaba a toda clase de personas que utilizaran los medios de comunicación electrónica, prácticamente a toda la población europea, con independencia de que sus conductas estuvieran relacionadas siquiera indirectamente con la comisión de delitos. Tampoco contemplaba la Directiva ninguna conexión entre los datos y las amenazas a la seguridad pública[328]. Finalmente, no establecía requisitos objetivos y subjetivos para el acceso a los datos almacenados, puesto que la obligación de conservación se refería a un periodo temporal, pero sin precisar que la determinación del plazo de conservación debiera basarse en criterios objetivos, para garantizar que se limitara a lo estrictamente necesario. Por último, en lo que respecta a las reglas relativas a la seguridad y a la protección de datos, no se contenían garantías suficientes para asegurar una protección eficaz de los datos conservados contra los riesgos del abuso y contra cualquier acceso y utilización ilícitos de los mismos.[329]

---

[328] *Vid*. STJUE de 8 de abril de 2014, párrafos 56 a 59

[329] *Vid.* párrafo 66 de la STJUE de 8 de abril de 2014. *Vid.* LUCAS MURILLO DE LA CUEVA, P.: "La distancia y el olvido en la Red. Comentario a la de 13 de mayo de 2014 en el asunto C-131-12" en AA.VV.: *El juez del derecho Administrativo. Libro homenaje a Javier Delgado Barrio.*

Más recientemente, en relación con el derecho de supresión de datos, se ha pronunciado el Tribunal de Justicia de la Unión Europea para resolver una cuestión prejudicial planteada por la Corte Suprema de Casación italiana en la STJUE de 9 de marzo de 2017, dictada en el asunto C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce contra Salvatore Manni. El origen del litigio estaba en la demanda presentada por señor Manni, administrador único de una sociedad a la que se adjudicó un contrato para la construcción de un complejo turístico en Italia contra la Cámara de Comercio de Lecce. A su juicio, los inmuebles de dicho complejo no se vendían debido a que los potenciales adquirentes tenían acceso a sus datos personales, recogidos en el registro de sociedades, donde constaba que había sido administrador de otra sociedad, declarada en concurso de acreedores en 1992 y liquidada en 2005.

El Tribunal de Justicia de la Unión Europea, en primer lugar, admite que esta clase de información entra dentro del concepto de dato personal, sin perjuicio de que se integre en el contexto de una actividad profesional y que la autoridad encargada de su registro lleva a cabo un tratamiento de datos personales del cual es responsable. A continuación, para determinar si los Estados miembros están obligados a garantizar a las personas físicas el derecho a solicitar a la autoridad encargada del registro que suprima o bloquee, tras un determinado lapso de tiempo, los datos personales inscritos en dicho

---

Marcial Pons, Madrid, 2015, págs. 488-490. *Vid.* GALÁN MUÑOZ, A.: "La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos: hacia una nueva orientación de la política criminal en la Unión Europea", en COLOMER HERNÁNDEZ, I (dir.): *op. cit*., págs. 57-61.

registro, o que restrinjan su acceso, procede a establecer cuál es la finalidad de esta inscripción.

Para la sentencia, la publicidad de los registros de sociedades tiene por objeto garantizar la seguridad jurídica en las relaciones entre las sociedades y los terceros. En consecuencia prevalece, en principio, la necesidad de proteger los intereses de terceros en relación con las sociedades anónimas y las sociedades de responsabilidad limitada y de garantizar la seguridad jurídica y la lealtad en las transacciones comerciales.

Esta interpretación no conduce, según el Tribunal de Justicia de la Unión Europea a una injerencia desproporcionada en los derechos fundamentales de los interesados concretamente, en el derecho al respeto de la vida privada y el derecho a la protección de datos personales, garantizados por la Carta de los Derechos Fundamentales de la Unión, en la medida en que en el registro de sociedades solo está inscrito un número limitado de datos personales, y está justificado que las personas físicas que deciden participar en los intercambios económicos mediante una sociedad anónima o una sociedad de responsabilidad limitada, que solo ofrecen su patrimonio social como garantía respecto a terceros, estén obligadas a hacer públicos los datos relativos a su identidad y a sus funciones dentro de aquéllas.

No obstante, el Tribunal de Justicia de la Unión Europea no excluye que, en situaciones concretas, razones legítimas propias de la situación particular del interesado, puedan justificar, excepcionalmente, que el acceso a los datos personales que le conciernen se limite al expirar un plazo suficientemente largo tras la liquidación de la sociedad de que se trate. Tal limitación debe realizarse sobre la base de una apreciación caso por caso. Incumbe a cada Estado

miembro decidir si desea establecer esta limitación en su ordenamiento jurídico.

En el caso de autos, el Tribunal de Justicia consideró que el mero hecho de que los inmuebles del complejo turístico no se vendieran debido a que los potenciales adquirentes de estos inmuebles tenían acceso a los datos del señor Manni recogidos en el registro de sociedades no puede justificar una limitación del acceso de terceros a estos datos, considerando concretamente el interés legítimo de éstos a disponer de esa información. Esta conclusión nos conduce a la problemática del derecho al olvido, que pasamos a analizar[330].

2. EL DERECHO AL OLVIDO.

El derecho al olvido surge con el afán de controlar y limitar la difusión de hechos verídicos, ocurridos tiempo atrás que pueden condicionar negativamente la vida del interesado, frente a su divulgación actual, con identificación y sin el consentimiento del afectado careciendo de interés público vigente y ocasionando un menoscabo al perjudicado.

En términos similares se ha pronunciado la doctrina[331]. Para Leturia Infante el derecho al olvido puede definirse como el fundamento jurídico que

[330] Tribunal de Justicia de la Unión Europea, comunicado de prensa núm. 27/17, Luxemburgo, 9 de marzo de 2017: "El Tribunal de Justicia considera que no existe derecho al olvido en relación con los datos personales recogidos en el registro de sociedades", disponible en: https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-03/cp170027es.pdf.

[331] Aproximaciones al derecho al olvido han proliferado en el Derecho civil y el Derecho Penal, como puede apreciarse en la doctrina francesa e italiana. Algunos ejemplos son: LETTERON, R.: "Le droit à l'oublie", *Revue du Droit Public et de la Science Politique en France et a*

permite que ciertas informaciones del pasado no sean actualmente difundidas cuando son capaces de provocar más daños que beneficios[332]. Por su parte, Rolla entiende que el derecho al olvido reconoce al individuo la legítima pretensión de no ver evocados hechos inherentes a su propia persona, sin interés público actual, que forman parte de experiencias ya superadas de su vida pasada[333]. El elemento temporal, por tanto, es pieza clave en este derecho, de manera que hechos que fueron públicos en el pasado vuelven a la esfera privada.

Compartimos la posición de Leturia Infante cuando afirma que el derecho al olvido puede, y debe, ser analizado desde la lógica de los derechos fundamentales, y, más concretamente, desde la lógica de los conflictos de derechos[334], dando respuesta a situaciones que justifican cierto reforzamiento de la privacidad y de otros derechos, al propio tiempo que establecen límites a las libertades de expresión e información y a la libertad de empresa entre otros derechos. Como punto de partida, se entiende que las libertades informativas, configuradas como piedra angular sobre la que se asienta una opinión pública libre, esencial en un Estado democrático, no son elemento suficiente para legitimar la intromisión producida, cuando colisionan con la protección de datos o la veracidad de la información[335].

L'étranger", núm. 2, 1996, págs. 385- 424; MEZZANOTTE, M.: *Il diritto all'oblio. Contributo allo studio della privacy storica,* Edizioni Scientifique Italiane, Napoles, 2009.

[332] LETURIA INFANTE, F. J.:" Fundamentos jurídicos del derecho al olvido, ¿un nuevo derecho de origen europeo o una respuesta típica ante colisiones entre ciertos fundamentos?", *Revista Chilena de Derecho*, núm. 1, 2016, pág. 96.

[333] ROLLA, G.: "El difícil equilibrio entre el Derecho a la información y la tutela de la dignidad y la vida privada: breves consideraciones a la luz de la experiencia italiana", *Cuestiones constitucionales*, *Revista Mexicana de Derecho Constitucional*, núm. 7, pág. 165.

[334] LETURIA INFANTE, F. J.*:* art. cit., pág. 97.

[335] Las SSTC 9/2007, 192/1999 y 110/2000, sobre la necesidad de encontrar un equilibrio entre las libertades informativas y los derechos de la personalidad; las SSTC 6/1988, 105/1990,

Entre las posibles aproximaciones al derecho al olvido, desde la perspectiva de los derechos fundamentales, la doctrina y la jurisprudencia han optado por configurarlo como un derecho autónomo o bien construirlo como una proyección de ciertos derechos de la personalidad, en particular, los derechos al honor y a la intimidad o a la vida privada -en la terminología del CEDH-, o bien el derecho a la protección de datos personales[336]. Paralelamente, el derecho al olvido presenta alcances y dinámicas diferentes según el país y la tradición jurídica que se observe[337].

La primera solución ha sido defendida por Simón Castellano, para quien el derecho al olvido sería un derecho fundamental en sí mismo, que encontraría su encaje en el artículo 10.1 CE y en el libre desarrollo de la personalidad[338]. El derecho al olvido se configuraría, así, como un derecho de libertad del individuo, asentándose, de manera parecida a como se derivó el derecho a la

---

240/1992 o 139/2007, respecto a la relevancia pública de los hechos como límite interno a las libertades informativa; y, en concreto, debe destacarse la STC 139/2007, referida al interés público como criterio fundamental para justificar la publicación de la información, a pesar del no consentimiento del titular. *Vid.* LÓPEZ PORTAS, M. B.: "La configuración jurídica del Derecho al olvido en el Derecho Español a tenor de la doctrina del TJUE", *Revista de Derecho Político*, núm. 93, 2015, pág. 154.

[336] MIERES MIERES, L. J.: "El Derecho al olvido digital", *Laboratorio de Alternativas*, 2014, pág. 12. Disponible en Internet: http://www.fundacionalternativas.org/public/storage/laboratorio_documentos_archivos/e0d97e985163d78a27d6d7c23366767a.pdf

[337] Como afirma Leturia, la libertad de expresión y el derecho a la privacidad en Estados Unidos y en Europa difieren lo suficiente como para augurar un mayor desarrollo del derecho al olvido en los países del viejo continente. *Vid.* sobre el desarrollo del derecho al olvido en Francia, Italia y Estados Unidos, LETURIA INFANTE, F. J.: art. cit., págs. 93-96

[338] En el mismo sentido, ORZA LINARES cuando manifiesta que "se abre con enorme fuerza la necesidad de definir otro nuevo conjunto de derechos a incluir en los textos constitucionales, vinculados a lo que empieza a conocerse como la 'sociedad del conocimiento' y que vayan más allá de la mera protección de los datos personales o de una adaptación más o menos forzada de los derechos tradicionales (…) entre otros, de la implantación de un derecho al olvido con la cancelación de datos privados anteriores", *vid.* ORZA LINARES, R. M.: "Derechos Fundamentales e Internet: nuevos problemas, nuevos retos", *Revista de Derecho Constitucional Europeo*, núm. 18, 2012, págs. 275-336, disponible en Internet: http://www.ugr.es/~redce/REDCE18/articulos/10_ORZA.htm#tres

autodeterminación informativa en Alemania, en el libre desarrollo de la personalidad y en la dignidad humana[339].

Sirva para ilustrar esta postura la decisión del Tribunal Constitucional alemán, sentencia de 5 de junio de 1973, en el conocido como caso Lebach[340]. El recurso de amparo pretendía impedir la emisión de un documental de la televisión pública (ZDF) sobre los asesinatos de soldados de Lebach, donde se mencionaba el nombre del recurrente. Los hechos ocurrieron en 1969 y el demandante fue condenado en el proceso penal subsiguiente. La emisión del reportaje se iba a realizar tres años después. Para el Tribunal, tratándose de reportajes sobre delitos graves de actualidad, el interés del público por la información adquiere prevalencia en general respecto de la protección de la personalidad del delincuente. Sin embargo, se debe respetar el principio de proporcionalidad, de ahí que no siempre sea admisible el nombrar, retratar o, simplemente, identificar al delincuente. La protección constitucional de la personalidad no admite que la televisión, más allá de informar sobre cuestiones de actualidad, se ocupe de la persona y la vida privada del autor de un crimen, en forma de documentales y sin límite de tiempo[341].

Por tanto, a juicio del Tribunal, en este caso, la emisión del programa de televisión lesionaba gravemente el libre desarrollo de la personalidad del recurrente, ya que era susceptible de causar un perjuicio adicional al autor del hecho, al identificarlo cuando había sido puesto en libertad o estaba a punto de

---

[339] SIMÓN CASTELLANO, P.: *El régimen constitucional del derecho al olvido*, Tirant lo Blanch, Valencia, 2012, pág. 219.
[340] BVerfGE 35, 202, disponible en http://www.kas.de/wf/doc/kas_16817-544-4-30.pdf
[341] SCHWABE, J.: *Jurisprudencia del Tribunal Constitucional Federal Alemán Extractos de las sentencias más relevantes*, KONRAD-ADENAUER-STIFTUNG e. V, México, 2009, pág. 251. http://www.kas.de/wf/doc/kas_16817-544-4-30.pdf

serlo, y, especialmente, al poner en peligro su reinserción en la sociedad (resocialización). El derecho del afectado "a ser dejado en paz" pone límites al interés informativo de mantener la atención pública sobre el sujeto. En este conflicto, como afirma el Tribunal Constitucional alemán, la frontera temporal entre el reportaje actual lícito y la posterior reiteración ilícita no puede fijarse en meses o años, sino que el criterio decisivo es determinar si la nueva información, en comparación con la noticia que se difundió en su día, constituye un menoscabo nuevo o adicional.

Según Simón Castellano, el bien jurídico que se quiere proteger con el derecho al olvido es más amplio que la protección que se otorga a la vida privada[342], y, en concreto, a la protección de datos de carácter personal, ya que en gran medida lo que se protege es la libertad de desarrollar el propio proyecto vital, sin estar hipotecado por informaciones que no tienen una relevancia pública actual. Así, el derecho al olvido encaja perfectamente con el concepto amplio de "autodeterminación informativa", en la medida en que se defina como el derecho a controlar la divulgación de los datos personales propios, a decidir qué datos van a poder ser tratados por ojos ajenos y a resarcirse de los daños derivados de una difusión de datos realizada sin consentimiento del afectado y que pueda condicionar e hipotecar el futuro del mismo[343].

---

[342] Para Letteron un derecho a ser olvidado de carácter pleno iría más allá que el derecho a la intimidad, pues abarcaría también informaciones públicas que no están cubiertas por la obligación de respeto por la vida privada de las personas. *Vid*. LETTERON, R.: *op. cit.,* pág. 413.

[343] SIMÓN CASTELLANO, P.*: El régimen constitucional…,* pág. 152

Ciertamente la dignidad humana es el fundamento último de los derechos fundamentales consagrados en nuestro texto constitucional[344]. Sin embargo, ello no equivale a ser fuente de nuevos derechos fundamentales. Incluso en el voto particular a la STC 290/2000 del magistrado Jiménez de Parga, que sostenía, frente a la opinión mayoritaria, que la llamada libertad informática era un nuevo derecho fundamental que tenía como "eje vertebrador" el artículo 10.1 CE, con cimientos constitucionales más amplios que los que proporciona el artículo 18.4 CE, no obstante, el magistrado autor del voto, no obstante, era consciente de los inconvenientes que el ordenamiento español presenta para el reconocimiento de nuevos derechos fundamentales. Por consiguiente, partimos de que la dignidad humana y el libre desarrollo de la personalidad, sin perjuicio de ser criterios de interpretación y valores horizontales que atraviesan todo el sistema de libertades, no pueden servir de base para construir un derecho fundamental al olvido autónomo[345].

Frente a esta posición, el derecho al olvido se presenta como un instrumento para reaccionar ante determinados casos de violación del derecho a la intimidad o del derecho al honor. El recuerdo de acontecimientos pasados,

---

[344] PARDO FALCÓN, J.: *op .cit.,* pág. 144.

[345] En este sentido, Mieres afirma que la argumentación de Simón Castellano es audaz y tiene el mérito de afrontar directamente las dificultades de encaje que presenta el derecho al olvido en el molde de los derechos fundamentales específicos. Sin embargo, continúa diciendo que "de acuerdo con la jurisprudencia constitucional, el artículo 10.1 CE no constituye un derecho fundamental en sí mismo, ni es fuente de nuevos derechos fundamentales tácitos. Este precepto constitucional tiene, primeramente, una función interpretativa a la hora de determinar el contenido constitucionalmente declarado de los derechos fundamentales reconocidos y, también cumple la función de dar cobijo a lo que se ha dado en llamar libertades constitucionales, esto es, manifestaciones de un *agere licere* que, por la dimensión de la personalidad concernida, presentan algún grado de resistencia constitucional frente a la restricción por parte de los poderes públicos… Se trata de libertades negativas que exigen de los poderes públicos un deber de abstención, de no interferencia. En cambio el derecho al olvido exige una conducta activa por parte de sus destinatarios: dejar de dar publicidad o corregir cierta información o dato obsoleto". MIERES MIERES, L. J.: *op. cit.*, pág. 12. *Vid.* también REY MARTÍNEZ, F.: *Eutanasia y derechos fundamentales*, Centro de Estudios Políticos y Constitucionales, Madrid, 2008, pág. 87.

cuando estos ya no responden a un interés público vigente, puede ocasionar un daño a la vida privada de terceros[346]. El derecho al olvido protege contra el rescate abusivo de eventos pasados que no deben ser centro de atención y no se inscriben en un enfoque histórico, aunque no proporciona a los individuos el derecho a censurar la información pública legítima.

Desde una perspectiva comparada, la jurisprudencia quebequesa fue pionera en reconocer el derecho al olvido en el año 1889, al considerar que el diario Le Violon, con evidente desacierto, vino a reactivar ciertas acusaciones sobre Odilon Goyette, figura política de la época, cuando había pasado bastante tiempo desde que estas fueron de actualidad, en referencia a hechos que ocurrieron hacía más de diez años, relativos a las relaciones sexuales del señor Goyette con una mujer de mala reputación. El periódico había sido distribuido a personas que no eran suscriptoras, al parecer para socavar la candidatura de Goyette a la Asamblea Legislativa por el distrito electoral de la Prairie[347]. Como señala Simón Castellano, la doctrina que se extrae de esta jurisprudencia es que existe un derecho al olvido que tiene por objeto información que ha sido compartida y conocida por una o más personas con anterioridad, pero que por diferentes circunstancias, como puede ser el mero paso del tiempo, ha perdido actualidad. Resultaría desproporcionado volver a difundir esa información cuando carece de interés público o actualidad, en la medida que mantiene al afectado en la tribuna pública contra su voluntad[348].

---

[346] SIMÓN CASTELLANO, P.: *El reconocimiento del derecho al olvido digital en España y en la Unión Europea*, Bosch, Hospitalet de Llobregat, 2015, pág. 104.

[347] *Idem.* Sentencia del Tribunal Supremo de Quebec, caso Goyette c. Rodier (1889) 20 R. L.108,110

[348] *Ibidem,* pág. 105. Estos supuestos se encuadran en el principio de responsabilidad civil por daños y perjuicios.

Por otra parte, en Estados Unidos, el caso de *Melvin v. Reid*[349], representa un claro ejemplo del derecho al olvido como proyección de los derechos de la personalidad. La demandante, que había sido prostituta, fue acusada de asesinato, en el año 1919 y, finalmente, absuelta. Una vez que hubo rehecho su vida y en esta nueva situación nadie conocía detalles de su pasado, en 1925 se emite la película "El quimono rojo", que relata su vida de prostituta y el juicio en el que se vio envuelta, identificándola con su verdadero nombre. El Tribunal de Apelación de California, en sentencia de 28 de febrero de 1931, estimó la demanda contra la productora de la película, basándose en el derecho a su privacidad y, más específicamente, en el derecho a perseguir y obtener la felicidad que la Constitución de California garantiza y en función del cual, entiende el tribunal, toda persona que vive una vida de rectitud, con independencia de su pasado, tiene ese derecho a una protección frente a ataques innecesarios o agresiones injustificadas contra su libertad, su propiedad, su posición social y su reputación.

En esta resolución se tuvo en cuenta que, a pesar de que los hechos fueron públicos en 1919, el derecho a la privacidad, en conexión con el derecho al honor, debía prevalecer sobre la libertad de expresión, pues tales informaciones carecían de interés público vigente. En tal sentido, el tribunal subrayó la importancia de la capacidad de un individuo para rehabilitarse y puso de manifiesto que el uso innecesario del nombre real de Melvin inhibía este derecho. El tiempo constituiría una expectativa razonable de privacidad,

[349] Sentencia Melvin contra Reid**,** 112 Cal. App. 285, 297, pág. 91 (1931), disponible en Internet: http://itlaw.wikia.com/wiki/Melvin_v._Reid. Esta sentencia fue seguida de una resolución del U.S District Court for the Northem District of California del año 1939, *Mau v. Rio Grande Oil.Inc*, 28 F. Supp.845 (1939).

que permitiría al individuo confiar en que la información personal que una vez fue pública y conocida, se considere, en palabras de Mieres[350], como reservada, y no una *res nullius* publicable en cualquier momento, salvo que concurra un interés público en su difusión. Resultaría razonable no someter a las personas a la divulgación permanente de sus datos publicados en el pasado.

En Europa, años más tarde, la jurisprudencia francesa sería pionera en resolver conflictos jurídicos en torno al derecho al olvido[351]. La Corte de Apelación de París, en su sentencia de 15 de marzo de 1967, en un caso similar al de *Melvin v. Reid*, denegó el derecho al olvido o prescripción del silencio y revocó la condena a la productora de la película *Landru* dirigida por Claude Chabrol y basada en la vida del famoso asesino en serie Henri Desire Landru. Según el órgano jurisdiccional, no se había vulnerado el derecho a vida privada de la demandante, que había sido amante del criminal, ya que los hechos ya habían sido difundidos legalmente y constaban en documentos públicos. La difusión de la información había sido hecha por la propia

[350] MIERES MIERES, L. J.: *op. cit*., pág. 14.

[351] LETURIA INFANTE, F. J.: *op. cit.*, pág. 93. En Italia, el derecho al olvido era ya mencionado en la sentencia de la Corte de Casación del 13 mayo de 1958, nº 1563, conocida como el caso Caruso, el jefe de policía que recibió un disparo después de la caída de fascismo como corresponsable de la elección de las víctimas de las Fosas Ardeatinas. La decisión toca el tema del derecho al olvido (aunque no su desarrollo, ya que consiste, en realidad, en un pronunciamiento sobre la reputación y la dignidad humana) utilizando la frase evocadora "el derecho al privacidad de la deshonra", es decir, un derecho a preservar su dignidad contra los ataques a la verdad, puesto que "el hombre más inmoral tiene el derecho de exigir que los demás no falseen la cantidad los crímenes que cometió, y no aumentar la pesada carga de sus culpas con la adición de hechos no reales". *Vid.* CIAVATTONE, C.: "I diritti della personalità e le nuove tecnologie: il diritto all'oblio e strumenti di tutela" en Jornadas sobre Documento informatico e la prova nel proceso civile: un codice al passo con i tempi?, Roma, 2016, disponible en Internet: http://www.giustizia.lazio.it/appello.it/form_conv_didattico/Relazione_diritto_all_oblio_dott.ssa_Ciavattone.pdf. Cuatro décadas más tarde, el derecho al olvido se reconocía en forma expresa, refiriéndose al "justo interés de cada individuo de no estar indefinidamente expuesto a datos que afectan negativamente su honor o reputación, relativa a la reiterada publicación de una noticia divulgada en el pasado" en sentencia de la Corte de Casación de 9 abril de 1998, nº 3679. LETURIA INFANTE, F. J.: *op. cit.,* pág. 94.

demandante no mucho tiempo antes, publicando sus memorias, y los hechos recogidos en la película figuraban en documentos judiciales accesibles al público.

Será el Tribunal de Instancia Superior de París, en una sentencia de 20 de abril de 1983, el que con mayor claridad afirme que " toda persona que ha estado mezclada en acontecimientos públicos puede, con el paso del tiempo, reivindicar el derecho al olvido; que el recuerdo de esos acontecimientos y el papel que ella haya podido desempeñar en ellos es ilegítimo si no está fundado en las necesidades de la historia o si su naturaleza es tal que puede herir su sensibilidad; (visto) que el derecho al olvido que se impone a todos, incluyendo a los periodistas, debe de la misma manera beneficiar a todos, incluyendo a los condenados que han pagado su deuda con la sociedad y que intentan reintegrarse a esta"[352].

De la jurisprudencia expuesta, puede deducirse que, hasta el siglo XX, el tiempo desempeñaba una expectativa razonable de privacidad. No obstante, las nuevas tecnologías pondrán en duda si nuestro pasado accesible en la red puede formar parte de aquello que no queremos que sea conocido por los demás[353]. En el mismo sentido, el hecho de que Internet pueda provocar que una información ocupe un lugar relevante en los resultados de los motores de búsqueda de manera perenne durante años puede llevar a plantear si el interés público puede ser caduco.

---

[352] SIMÓN CASTELLANO, P.: *El reconocimiento al olvido digital en España…,* pág. 106.
[353] MIERES MIERES, L. J.: *op. cit.*, pág. 15. *Vid.* también, sobre el factor tiempo, MARTÍNEZ CABALLERO, J.: "Como conjugar el derecho al olvido", *Revista jurídica de Castilla la Mancha,* núm. 57, 2015, pág. 158.

Consecuencia de estas reflexiones es el estudio del derecho al olvido en el contexto digital, como una exteriorización del derecho fundamental a la protección de datos en relación con el principio de calidad de los datos que impone límites a la conservación de los mismos más allá del período necesario para cumplir la finalidad del tratamiento. Su reconocimiento en la STJUE de 13 de mayo de 2014 y, sobre todo, su positivización en el Reglamento General de Protección de Datos, han llevado a identificarlo como una manifestación específica del derecho fundamental a la protección de datos.

3. EL DERECHO AL OLVIDO DIGITAL

En la sociedad contemporánea, donde el desarrollo tecnológico ha convertido en realidad material la idea de que la memoria es eterna y universal, es comprensible la imperiosa necesidad de los ciudadanos de hacer invisibles determinadas informaciones personales en la red que con el paso del tiempo pueden producir efectos no deseados, a través del denominado derecho al olvido en Internet.

Para tratar de definir el derecho al olvido digital hay que partir de las características de la red de redes. La perennidad[354] y la descontextualización

[354] La vicepresidenta de la Comisión Europea y ex Comisaria de Justicia Vivianne Reding, el 30 de noviembre de 2010, en la conferencia *Privacy matters-"Why the EU needs new personal data protection rules?"* manifestó: " *Someone once said: God forgives and forgets but Web never does".* http://europa.eu/rapid/press-release_SPEECH-10-700_en.htm. En el mismo sentido se ha pronunciado MAYER-SCHÖNBERGER, quien recalca que con la ayuda de la tecnología y la difusión olvidar se ha convertido en la excepción a la regla, *vid,* MAYER-

de la información y la extrema facilidad para localizarla a través de los motores de búsqueda, con su añadido efecto multiplicador, han sido los retos a los que se ha enfrentado el Derecho al olvido en Internet[355].

Nada tiene que ver el debate sobre el derecho al olvido, como señala Rallo Lombarte[356], con el fin de la memoria, con prescindir del pasado, con el falseamiento de la Historia o con la supuesta instauración de un filtro censor universal al ejercicio del derecho a la información. Por el contrario, esta polémica gira en torno a los riesgos que el uso de Internet produce sobre la reputación, la privacidad, la libertad y la dignidad humana.

Para Mieres[357] el derecho al olvido digital es la respuesta a la amenaza que supone para el libre desarrollo de la personalidad el almacenamiento permanente en Internet de información personal cuya difusión, pasado el tiempo, puede afectar negativamente a la persona, al producirse un desajuste entre lo publicado y la realidad actual. Se trata de garantizar la efectividad del control de las personas sobre las informaciones y datos presentes en la red que se refieren a ellas, que resultan obsoletas y cuya difusión o accesibilidad actual les perjudica.

Para Álvarez Caro, el derecho al olvido podría definirse como el derecho a equivocarse o a que una equivocación pasada no marque y determine la vida de un individuo, que, por definición, no es otra cosa que un proceso evolutivo,

---

SCHÖNBERGER, V.: *Delete: the virtue of forgetting in the digital age*, Princenton University Press, 2009.

[355] *Vid.* SIMÓN CASTELLANO, P.: *EL reconocimiento del derecho al olvido digital*… págs. 60 a 69.

[356] RALLO LOMBARTE, A.: *El derecho al olvido en Internet, Google versus España*, CEPC, Madrid, 2014, págs. 26-27.

[357] MIERES MIERES, L. J.: *op. cit.*, pág. 6.

una secuencia de aciertos y errores. Su ejercicio iría dirigido a eliminar datos de la red que el interesado considere que le perjudican, aunque se ajusten a una realidad pasada[358]. Y, puntualizando aún más, esta autora afirma que se conoce como derecho al olvido a un interés jurídicamente protegido de los ciudadanos que consiste en lograr efectivamente que sus datos personales no sean localizados por los buscadores en la red. No se trata de exigir el borrado de los datos porque estos no son exactos o ciertos, sino porque el titular de los mismos considera que le perjudican y estima, asimismo, que no existe ningún fin que legitime la disponibilidad de dichos datos por parte de terceros[359].

Sobre su ámbito de aplicación, ya no bastaría la protección que proporciona el derecho al olvido como proyección del derecho a la intimidad o el derecho al honor, que exigiría que la información obsoleta lesionara los bienes jurídicos protegidos por estos derechos. El derecho al olvido digital encuentra, en este sentido, su fundamento en el derecho a la protección de datos personales como poder de control sobre la información personal. Este derecho fundamental tiene por objeto un ámbito de protección mucho más amplio pues engloba todo tratamiento de datos que identifique o permita identificar a una persona. A ello ha contribuido la jurisprudencia del Tribunal de Justicia de la Unión Europea, que, en el asunto Lindqvist,[360] interpretó ampliamente el concepto de tratamiento de datos personales como cualquier publicación de datos en línea en cualquiera de sus formas, incluyendo webs, blogs, etc. Todo esto, unido al factor tiempo, puede hacer que el tratamiento de

[358] ÁLVAREZ CARO, M.: *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*, Reus, Madrid, 2015, pág. 68.
[359] *Ibidem*, pág. 71.
[360] Sentencia del Tribunal de Justicia de 6 de noviembre de 2003, asunto C-101/01 – Lindqvist.

datos en Internet resulte inadecuado, no pertinente o excesivo para la finalidad para la que los datos hubiesen sido recabados.

La AEPD fue precursora en la interpretación de que el derecho al olvido se integra dentro del derecho fundamental a la protección de datos[361]. El enfoque inicial que se le dio al derecho al olvido ligado al entorno digital online, vino a acotar su sentido como cancelación de datos[362]. Así, en diversas resoluciones ha venido a proclamar que "ningún ciudadano que no goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a que sus datos de carácter personal circulen por la red sin poder corregir la inclusión de los mismos en un sistema de comunicación universal como Internet. Si requerir el consentimiento individualizado de los ciudadanos para incluir sus datos personales en Internet o exigir mecanismos técnicos que impidieran o filtraran la incorporación inconsentida de datos personales podría suponer una insoportable barrera al libre ejercicio de las libertades de expresión e información a modo de censura previa (lo que resulta constitucionalmente proscrito), no es menos cierto que resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las referidas libertades (por no resultar

---

[361] LÓPEZ PORTAS, M. B.: *op. cit.*, pág. 158. Una aproximación a la actividad de la AEPD en ORZA LINARES, R. M.: "El derecho al olvido en Internet: algunos intentos para su regulación legal", en CORREDOIRA, L. y COTINO HUESO, L. (Dirs).: *Libertad de expresión e información en la Red. Amenazas y protección de los derechos personales*, CEPC, Madrid, 2013, págs. 478 y ss. También en RALLO LOMBARTE, A.: *op. cit*. Del mismo modo alude a la labor de la AEPD, BUISÁN GARCÍA, N.: "El derecho al olvido: el nuevo contenido de un derecho antiguo", *El Cronista del Estado Social y Democrático de derecho*, núm. 46, 2014, pág. 24. La AEPD sigue las interpretaciones realizadas por sus homólogas francesa e italiana, es decir, la *Commision nationale de l'informatique et des libertés* y el *Garante per la Protezione dei Dati Personali*. *Vid.* SIMÓN CASTELLANO, P.: "El encaje constitucional del derecho al olvido digital en perspectiva comparada", *Datos personales.org*, núm. 54, 2012.

[362] *Vid.* la Comunicación de la Comisión Europea de 4 de noviembre de 2010 sobre "Un enfoque global de la protección de datos en la Unión Europea, el Dictamen del Supervisor Europeo de Protección de datos" en RALLO LOMBARTE, A.: *op. cit.,* págs. 36 a 43.

sus datos personales de interés público ni contribuir, en consecuencia, su conocimiento a forjar una opinión pública libre como pilar basilar del Estado democrático) debe gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la red de su información de carácter personal."[363]

En materia de protección de datos, dos son los principios recogidos en la LOPD sobre los que se sustenta el derecho al olvido digital, según el criterio de la AEPD[364]: el principio del consentimiento y el de finalidad o calidad de los datos. El primero es aplicable cuando alguien presta su consentimiento o es él mismo quien publica información que contiene datos personales en la red. En tal caso, el interesado puede revocar su consentimiento y exigir que aquello cuya difusión antes permitió -la divulgación de fotos, videos, comentarios, etc., en Internet- desaparezca de la red. No obstante, con frecuencia el interesado se encuentra con que sus datos personales han sido publicados por terceros sin su consentimiento. En consecuencia, podrá oponerse a su circulación, salvo que tal divulgación suponga el ejercicio de la libertad de información, en cuyo caso el conflicto habrá de resolverse ponderando ambos derechos y aplicando el principio de proporcionalidad. Asimismo, puede ocurrir que el consentimiento sea irrelevante, como cuando se trata de datos personales contenidos en

---

[363] Por todas, la Resolución TD/00266/2007 de la AEPD de 27 de julio de 2007. *Vid.* RALLO LOMBARTE, A: "El derecho al olvido y su protección" *Revista TELOS*, 2010. *Vid.* la comparecencia, en noviembre de 2007, del Director de la AEPD, ante la Comisión Constitucional del Congreso de los Diputados. Disponible en Internet: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2007/notas_prensa/common/11-noviembre/np_281107.pdf.

[364] Cfr. LÓPEZ PORTAS, M. B.: *op. cit.,* págs. 160-161 y SIMÓN CASTELLANO, P.: "El encaje constitucional del derecho al olvido…", art. cit.

fuentes de carácter público, como los diarios y boletines oficiales, de tal manera que las posibilidades de oposición a tales tratamientos son ciertamente reducidas. Por lo tanto, de todo esto se desprende que el principio del consentimiento por sí solo no puede servir de fundamento del derecho al olvido digital.

Es precisamente el segundo de los principios recogidos en la normativa de protección de datos, el principio de calidad de los datos, el que constituye la base sólida sobre la que sustentar el derecho al olvido digital. El articulo 4.5 LOPD determina la obligación de cancelar los datos cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que hubieran sido recabados o registrados.

El conocido popularmente como derecho al olvido digital no es más que una manifestación de los derechos de cancelación y oposición al tratamiento de los datos personales en Internet con el fin de obtener el control sobre los mismos y solicitar en su caso su borrado y no difusión, o, más bien, su no indexación como veremos.

Precisamente una de las principales características de Internet es la proliferación de múltiples prestadores de servicios, lo que implica un incremento de los intercambios de datos. Entre estos, los llamados buscadores o motores de búsqueda son sistemas informáticos que permiten a partir de una o varias palabras clave obtener resultados en forma de enlaces a documentos o páginas web que contienen esas palabras. Sus ventajas son evidentes: son herramientas que ayudan a buscar información en Internet a gran velocidad, en cualquier momento o lugar, de forma anónima y gratuita. No obstante, también interactúan con datos personales con los que comercializar y elaborar perfiles,

que, en ocasiones, pueden aportar resultados descontextualizados, obsoletos e, incluso, perjudiciales para las personas a las que se refieren[365].

El derecho al olvido digital se plantea en la mayoría de los casos en relación con un determinado contenido legal y obsoleto, referido a una persona física, que ha sido publicado en Internet y al que se accede a través de una búsqueda asociada al nombre y apellidos de la persona afectada. Resulta razonable pensar que, pasado el tiempo, el interesado pretenda impedir la difusión o indexación en buscadores de aquella información cuando considere que puede perjudicarle o desea que sea olvidada, aunque su publicación inicial hubiera sido lícita.

En este contexto se plantea la singular problemática de la oposición/cancelación de datos indexados por los motores de búsqueda en Internet. Por ello, es necesario diferenciar entre quien divulga y quien indexa los datos. La AEPD sostenía que frente a quien divulga o mantiene en la red datos personales obsoletos puede ejercerse el derecho de cancelación**,** que implica el bloqueo de los datos para que no resultaran accesibles para los

---

[365] Tene sintetiza los problemas que los motores de búsqueda plantean a la privacidad: agregación (los motores de búsqueda permiten ensamblar informaciones reducidas y elaborar un perfil más o menos completo de una persona), distorsión o inexactitud de la información (que puede llegar a suponer un menoscabo del prestigio o consideración social de una persona), exclusión o incapacidad de una persona para conocer la información recopilada sobre ella y uso de la información disponible para fines distintos a los que motivaron su recopilación. A todo ello se une el *chilling effect* o desincentivo de ciertas búsquedas en una especie de autocensura, cuando el individuo es consciente de que el sistema registra las búsquedas efectuadas desde cada dirección IP. *Vid.* TENE, O.: "What Google Knows: Privacy and Internet Search Engines", *Utha Law Review,* núm.4, 2008, págs.1457-1464, disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1021490. En relación con este tema puede consultarse SOLOVE, D. J.: "I´ve got nothing to hide and other misunderstandings of privacy", *San Diego Law Review*, vol. 44, 2007, págs. 745-772. Disponible en Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565.Desde la perspectiva comparada, algunos tribunales han reconocido la responsabilidad de los buscadores, así, en Francia, la sentencia de la *Cour d'Appel de Paris, Pôle 1*, de 9 de diciembre de 2009, o, en Italia, la sentencia de la Sección cuarta Penal del Tribunal de Milán de 12 de abril de 2010. Cfr. BUISÁN GARCÍA, N.: *op. cit.*, págs. 23-24.

terceros. Por otro lado, frente a los motores de búsqueda que indexan las páginas originales y muestran los enlaces a ellas en su página de resultados, procedía el derecho de oposición al tratamiento de datos, requiriendo del buscador que desindexe la página o páginas que muestran los datos obsoletos. Ambos serían instrumentos de garantía del derecho al olvido[366].

La sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014[367] resuelve una cuestión prejudicial planteada por la Audiencia Nacional sobre la interpretación que debía darse de la Directiva 95/46/CE, conforme al artículo 267 del Tratado de Funcionamiento de la Unión Europea[368].

El objeto del "caso *Google*" persigue aclarar la normativa europea en relación con la actividad de los motores de búsqueda en Internet y la aplicación territorial de la misma, así como el alcance del derecho de cancelación y oposición en este contexto.

Los hechos en los que se fundamenta el proceso administrativo ante la AEPD se remontan a 1998, cuando el periódico La Vanguardia publicó en su edición impresa el anuncio de una subasta de inmuebles por deudas a la

---

[366] Memoria de la AEPD 2011: "es obligado que los responsables de las páginas web y de los motores de búsqueda atiendan las demandas de los ciudadanos cuando ejerzan los derechos que les reconoce la LOPD. Sea el derecho a cancelar sus datos personales cuando han sido publicados sin su consentimiento y sin cobertura legal, o bien el derecho de oponerse a que, aun cuando su publicación originaria fuese legal, sean objeto de tratamientos posteriores que comportan una multiplicación de esa publicidad, como sucede con los buscadores". Disponible en Internet: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common /memorias/2011/Memoria_2011.pdf

[367] STJUE de 13 de mayo 2014, asunto C-131/12-Google Spain y Google.

[368] Auto de la Audiencia Nacional, Sala de lo Contencioso, Sección 1ª, de 27 de febrero de 2012, y petición de decisión prejudicial presentada por la Audiencia Nacional (España) el 9 de marzo de 2010, *Google Spain, S.L., Google Inc./* Agencia de Protección de Datos (AEPD) (Asunto C-131/12).

Seguridad Social[369], donde se mencionaba el nombre y los apellidos del afectado y de su esposa. Posteriormente, esta información se puso a disposición del público en la versión digital. Quince años más tarde, al introducir su nombre en el buscador *Google*, este ofrecía como resultado vínculos al sitio web hemeroteca digital de La Vanguardia que publicaba el citado anuncio, relacionado con un embargo cuya deuda ya estaba saldada[370].

El demandante contactó con la editorial del periódico y con *Google Spain* solicitando la desaparición de dichas informaciones de la red, argumentando que carecían de relevancia actual. La Vanguardia contestó al interesado que no procedía la cancelación de sus datos, dado que la publicación se realizó por orden del Ministerio de Trabajo y Asuntos Sociales. Por su parte, *Google Spain S.L*. lo remitía a la empresa *Google Inc*., con domicilio social en California (EEUU), por entender que ésta era la empresa que presta el servicio de búsqueda en Internet.

Con fecha 5 de marzo de 2010, tuvo entrada en el Registro General de la AEPD la reclamación del afectado, solicitando, entre otras cosas, que se exigiese al responsable de la publicación "*on line*" de La Vanguardia que eliminase o modificase la publicación para que no apareciesen sus datos personales o bien utilizase las herramientas facilitadas por los buscadores para proteger su información personal. También solicitaba que se exigiese a *Google Spain* o *Google Inc*. que eliminase o bien ocultase sus datos, para que no se

[369] Insertado por la Dirección Provincial de la Tesorería de la Seguridad Social de Barcelona, organismo administrativo dependiente de la Secretaría de Estado de la Seguridad Social del Ministerio de Trabajo y Asuntos Sociales.
[370] *Vid* ."¿Según Google sigo siendo deudor y casado?", *El País*, 22 de marzo de 2013.

incluyesen en sus resultados de búsqueda y dejasen de estar ligados a los *links* de La Vanguardia.

En sus alegaciones, *Google Spain* expuso el automatismo y la neutralidad en que consiste el proceso de búsqueda y argumentó que no era ni responsable, ni encargada de la prestación del servicio de búsquedas en Internet. *Google Spain* argumentó que solo representa a *Google Inc*. en el negocio de la venta de espacio publicitario disponible en su página web. Su actividad se limitaría a dichos servicios y, por ello, ni desarrollaría la actividad de buscador ni cabría imputarle ninguna de las actividades ni consecuencias que se derivan de la actividad que ejecuta *Google Inc*. aunque esta empresa fuera la matriz de *Google Spain*. Partiendo de esta premisa, y dado que los servicios de buscador los presta *Google Inc*. desde los Estados Unidos, no resultaría de aplicación ni la Directiva europea de protección de datos, ni la ley española que la aplica. La única vía para conseguir el propósito que perseguía el interesado sería, así, la de acudir a un órgano judicial del domicilio del responsable del sitio web para instar ahí la cancelación de sus datos o la limitación de los efectos de la publicación, de forma que los motores de búsqueda no los indexen.

La AEPD argumentó que la afectación al derecho a la protección de datos solo se da cuando se "*atenta o puede atentar"* al principio de respeto a la dignidad de la persona, a los efectos previstos en el artículo 8 de la Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información[371], y esa

[371] La Resolución de la AEPD nº R/01680/2010 (Procedimiento nº TD/00650/2010) en su fundamento octavo, señala que esta normativa incluye a los buscadores en la definición de servicios de la sociedad de la información. Según el artículo 8 de la citada Ley de Servicios de

afectación debe predicarse de todas y cada una de las garantías que integran el derecho fundamental a la protección de datos personales, entre las que se incluye el derecho de oposición. Por consiguiente, mediante Resolución de 30 de julio de 2010, la AEPD desestimó la reclamación contra el periódico, al considerar que la publicación realizada se había llevado a cabo de forma legalmente justificada, para dar la máxima publicidad a las subastas y conseguir, así, la mayor concurrencia de licitadores.

---

la Sociedad de la Información, “en caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran. Los principios a que alude este apartado son los siguientes: (...)c) El respeto a la dignidad de la persona". Además, abundando en el principio del respeto a la dignidad de la persona, la Resolución de la AEPD hace referencia expresa a la STC 292/2000, que comienza señalando que “la singularidad del derecho a la protección de datos, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no solo a la intimidad en su dimensión constitucionalmente protegida por el artículo 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, FJ 4) como el derecho al honor, citado expresamente en el artículo 18.4 CE, e igualmente, en expresión bien amplia del propio artículo 18.4 CE, al pleno ejercicio de los derechos de la persona”. Reiterando la doctrina que ya había establecido en anteriores sentencias, la STC 292/2000 se refiere a que “el artículo 18.4 de la CE contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad 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". La sentencia hace referencia a continuación al contenido esencial del derecho fundamental a la protección de datos, afirmando que “la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada 'libertad informática' es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención”. Entiende el Alto Tribunal que “el derecho fundamental a la intimidad del artículo 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y el derecho del afectado.” Disponible en Internet: http://www.agpd.es/portalwebAGPD /resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00650-010_Resolucion-de-fecha-30-07-2010_Art-ii-culo-16-LOPD_Recurrida.pdf

En cuanto a la reclamación contra *Google Spain* y contra *Google Inc.*, la AEPD la estimó, al considerar que, al ser gestores de motores de búsqueda, eran responsables y actuaban como intermediarios de la sociedad de la información.

Google se negó a cumplir con la Resolución de la AEPD y recurrió la decisión por la via contencioso-administrativa ante la Audiencia Nacional. En el curso de ese proceso, la Audiencia Nacional consideró necesario preguntar al TJUE tres cuestiones. La primera era la relativa a si un motor de búsqueda como *Google* está sometido al ámbito territorial de aplicación de las normas de protección de datos de la Unión Europea y, por tanto, a la legislación española. La ubicación extraterritorial de los responsables de tratamientos de datos personales que los afectados consideran lesivos es un obstáculo de primer orden a la efectividad del derecho fundamental a la protección de datos, porque, aunque se accede a esos motores de búsqueda desde España y estos acceden también a los proveedores de contenidos radicados en España y captan y suministran información en nuestro país, sin embargo, se niegan a reconocer la jurisdicción de los tribunales españoles y se remiten a los del lugar en que están domiciliados en otros países[372]. En segundo lugar, se preguntaba

[372] Como dice el Auto de la Audiencia Nacional de 27 de febrero de 2012 "(...) sostener que [ante] la indexación de datos procedentes de páginas web situadas en España, en relación con una información publicada en España, en base a una norma legal española, que afecta a datos de un ciudadano español y que fundamentalmente puede tener una repercusión negativa, a juicio del afectado, en su entorno personal y social sito en España (centro de intereses), [este] tenga que defender la tutela de su derecho a la protección de datos en EEUU, por ser el lugar que el gestor del buscador ha elegido para ubicar los medios técnicos, colocaría a los afectados en una situación de especial vulnerabilidad e impediría o dificultaría enormemente la tutela eficaz de este derecho que podría resultar incompatible con el espíritu y finalidad que inspira la Directiva y, sobre todo, con una tutela eficaz de un derecho fundamental contenido en la Carta Europea de Derechos Fundamentales". *Vid.* LUCAS MURILLO DE LA CUEVA, P.: "La distancia y el olvido. A propósito del derecho a la autodeterminación informativa (Comentario al Auto de la Sección Primera de la Audiencia Nacional de 27 de febrero 2012 en

por el concepto de tratamiento de datos personales aplicado a los proveedores de servicios de motores de búsqueda en Internet. Por último, se presentó la cuestión relativa al derecho al olvido, es decir "si los derechos de supresión y bloqueo de los datos, regulados en el artículo 12 b) y el de oposición, regulado en el artículo 14 a) de la Directiva 95/46/CE, comprenden que el interesado pueda dirigirse a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros".

La sentencia del Tribunal de Justicia de la Unión Europea vino precedida por las conclusiones del abogado general *Niilo Jääskineen,* presentadas el 25 de junio de 2013[373]. Más allá de su carácter no vinculante, estas conclusiones son una aportación de primer orden al debate sobre el significado del derecho fundamental a la protección de datos[374]. Tras exponer el marco jurídico aplicable y la jurisprudencia europea sobre la materia, el Abogado General, se pronuncia a favor del sometimiento de *Google* al Derecho Europeo por el hecho de que disponga de establecimientos en la Unión Europea mediante los cuales lleva a cabo la publicidad base de su negocio[375].

---

el recurso 725/2012)", *Revista de Jurisprudencia*, núm.1, 2012. Disponible en Internet: http://www.elderecho.com/tribuna/administrativo/Comentario-Seccion-Primera-Audiencia Nacional_11_475180004.html

[373] Conclusiones del abogado general *Jääskineen,*. Disponible en Internet: http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=ES

[374] LUCAS MURILLO DE LA CUEVA, P: "El derecho al olvido y la sujeción de Google al derecho europeo según el abogado general del Estado", *Revista de Jurisprudencia*, núm. 1, 2014. Disponible en Internet: http://www.elderecho.com/administrativo/derecho_al_olvido-sujecion_de_google-derecho-sujecion-europeo-abogado-general_11_640555005.html

[375] Si el tratamiento de datos personales tiene lugar en el marco de un establecimiento del responsable del mismo y ese establecimiento es un nexo para el servicio con el mercado

Tampoco plantea problemas para el Abogado General la segunda cuestión. En su opinión, el proveedor de servicios de motor de búsqueda lleva a cabo un tratamiento de datos personales y es responsable de ellos a efectos de la Directiva. Ahora bien, en la medida en que sea solamente un intermediario, no debe ser considerado como responsable principal del tratamiento. La puesta a disposición de una herramienta de localización de información no implica control alguno sobre el contenido[376]. Esta condición le corresponde a los proveedores de la información.

Por lo que atañe a la legitimación del tratamiento de datos personales que llevan a cabo los buscadores, en el supuesto de que no exista consentimiento del interesado, para el Abogado General es obvio que la prestación de servicios de motor de búsqueda en Internet persigue, intereses legítimos, concretamente facilitar a los usuarios de Internet el acceso a la información, conseguir que esta información se difunda de modo más efectivo y poner en marcha diversos servicios subsidiarios, como la provisión de

---

publicitario de un Estado miembro, aunque las operaciones técnicas de dicho tratamiento tengan lugar en otro Estado miembro o en países terceros, se da el supuesto previsto en el artículo 4.1 a) de la Directiva. *Vid*. párrafo 67 de las conclusiones.

[376]*Vid*. conclusiones, párrafos 84 a 90. Si el poder de decisión sobre la finalidad y medios del tratamiento de datos es lo que determina al responsable del mismo, como bien explica Brotons, ''un proveedor de servicios de búsqueda otorga una finalidad propia a los datos (personales y no personales) que trata, plenamente desligada de la finalidad que a los mismos datos le otorga el editor de la página web y que coincide ni más ni menos con su finalidad económica: poner al alcance de los usuarios un producto terminado como recurso ordenado de información bajo demanda, a cambio de percibir ingresos por publicidad de los anunciantes(...), para poder cumplir esta finalidad, *Google* define *per se* los medios que emplea para rastrear, localizar, ordenar, cruzar e indexar la información, bien sea diseñando los robots de búsqueda que utiliza, programando un algoritmo informático que mejore la utilidad de los resultados que ofrece o decidiendo en qué servidor del mundo se almacenan las copias ocultas de esta información. Medios propios que, y esto es importante, en muchos casos ningún otro operador económico, editor de página web o usuario final de Internet pueden utilizar" .*Vid.* BROTONS MOLINA, O.: "Caso Google: tratamiento de datos y derecho al olvido. Análisis de las Conclusiones del Abogado General, asunto C-131/12", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 33, 2013, pág. 107-126. Disponible en Internet: https://proview.thomsonreuters.com/launchapp/title/aranz/periodical/106943754/v20130033/document/132462117/anchor/a-VI-BIB_2013_2494

publicidad mediante palabras clave. Estas tres finalidades están relacionadas con los derechos fundamentales a la libertad de información y a la libertad de expresión (art. 11 CDFUE) y la libertad de empresa (art. 16 CDFUE).

Como responsable del tratamiento, el proveedor, siguiendo al Abogado General, debe cumplir los requisitos del principio de calidad de los datos (art. 6 de la Directiva), es decir, los datos personales deben ser adecuados y relevantes, no ser excesivos en relación con los fines para los que se recogen y estar actualizados, no obsoletos, en relación con las finalidades para las que se recogen.

De acuerdo con el criterio del Abogado General, habrán de ponderarse los intereses del responsable del tratamiento o de los terceros a los que sirve el tratamiento y los de los interesados[377]. Sobre la base de este razonamiento, aquel considera que la autoridad nacional de protección de datos no puede requerir a un proveedor de servicios de motor de búsqueda en Internet que retire información de su índice, salvo en los supuestos en que el proveedor de servicios no ha respetado los códigos de exclusión o en los que no se ha dado cumplimiento a una solicitud emanada de la página web relativa a la actualización de la memoria oculta.

Por último, a la pregunta sobre si los derechos de cancelación y oposición sirven de fundamento jurídico para un posible derecho al olvido, el Abogado General responde que el primero se refiere a datos cuyo tratamiento no cumple lo dispuesto en la Directiva, en particular debido al carácter incompleto o inexacto de los datos, lo cual no se deduce del auto de

[377] *Vid.* conclusiones, párrafos 94-96.

planteamiento de la cuestión prejudicial, y el derecho de oposición es de aplicación cuando el interés legítimo del afectado deba prevalecer sobre el que asiste al proveedor del servicio. La finalidad del tratamiento y los intereses a los que sirve, al compararse con los del interesado, serían los criterios que habrían de ponderarse cuando se tratan datos sin el consentimiento del interesado. Una preferencia subjetiva por sí sola no equivale a una razón legítima a los efectos del derecho de oposición. Por consiguiente, aquel llega a la conclusión de que no hay un derecho al olvido que faculte al interesado para restringir o poner fin a la difusión de datos personales que considere lesiva[378], aun siendo consciente de que la propuesta de RGPD reconoce en su artículo 17 el derecho al olvido[379].

A pesar de su brillante argumentación, conviene advertir que, desde el punto de vista constitucional, el Abogado General relativiza el significado del reconocimiento del derecho fundamental a la protección de datos en el artículo 8 de la CDFUE, que no es una mera redundancia del artículo 7 CDFUE, obviando su carácter autónomo. Como consecuencia, centra en el derecho a la vida privada del artículo 8 del CEDH las cuestiones relativas a la protección de datos personales. Por otra parte, es verdad que deja constancia de que los proveedores realizan actividades vinculadas a la libertad de empresa, pero su alegato descansa, especialmente, en la contribución de estos al ejercicio de las libertades de expresión e información, como se pone de relieve cuando enfatiza

[378] Aunque llegara a reconocerse, no tendría carácter absoluto, porque los proveedores no pueden ponerse en la posición del editor de las páginas web fuente y comprobar si la difusión es legal y legítima a los efectos de la Directiva. Sería como abandonar su posición de intermediario y asumir la responsabilidad por el contenido de la página web y cuando fuere necesario censurar su contenido evitando o limitando el acceso a este. *Vid*. párrafo 109 de las conclusiones.

[379] Párrafo 110 de las conclusiones.

que "un proveedor de servicios de motor de búsqueda en Internet ejerce legalmente tanto su libertad de empresa como su libertad de expresión cuando pone a disposición del público herramientas de localización en Internet basadas en un motor de búsqueda"[380]. En este sentido, en su opinión, el reconocimiento del derecho al olvido entrañaría el sacrificio de derechos básicos, como la libertad de expresión e información[381]. Así, equivaldría a una censura del contenido publicado realizado por un tercero[382]. Y lo mismo se puede decir, en su opinión, con respecto al derecho a la información de un usuario de Internet, si su búsqueda de información relativa a una persona física no generara resultados que ofrecieran un reflejo veraz de las páginas webs relevantes, sino una versión "bowdlerizada" de las mismas[383].

El asunto, finalmente, fue resuelto por la STJUE de 13 de mayo de 2014, en el asunto C-131/12, Google Spain, S.L. Google Inc. contra AEPD y Mario Costeja González.

En primer lugar, el Tribunal de Justicia de la Unión Europea entra a examinar la segunda cuestión prejudicial planteada por la Audiencia Nacional, esto es, si la actividad de un motor de búsqueda debe calificarse como

---

[380] Párrafo 132 de las conclusiones.

[381] Sobre el papel de los motores de búsqueda en relación con el derecho de información de los internautas, *vid.* COTINO HUESO L.: "La selección y personalización de las noticias por el usuario de las nuevas tecnologías", en CORREDOIRA, L. y COTINO HUESO, L. (dirs).: *Libertad de expresión e información en la Red. Amenazas y protección de los derechos personales*, CEPC, Madrid, 2013, págs. 41-56.

[382] Este caso, como señala Rallo Lombarte, no confronta directamente derecho al olvido y libertad de información, por cuanto los datos personales impugnados no son objeto de noticia informativa, no tienen relevancia pública ni por razón de la materia, ni del sujeto. Su difusión tiene una finalidad que se agota con ofrecer el máximo conocimiento público de la subasta y, en consecuencia, el día después carecerán de sentido. No cabe oponer un riesgo de censura informativa a datos que no tienen esta naturaleza. *Vid.* RALLO LOMBARTE, A.: *El derecho al olvido en Internet…,* pág. 242.

[383] Conclusiones párrafos 131 a 134. *Vid.* críticas a las conclusiones del Abogado General en LUCAS MURILLO DE LA CUEVA, P: "El derecho al olvido y la sujeción de Google…", art. cit.

tratamiento de datos personales y, tras la respuesta afirmativa[384], si debe o no considerarse responsable del mismo y, en el primer supuesto, el alcance de esta responsabilidad. Para responder, el Tribunal viene a clarificar la actividad que desarrollan los gestores de motores de búsqueda[385]. En efecto, hay que diferenciar el tratamiento de datos personales llevado a cabo por los editores de páginas web del efectuado por los gestores de motores de búsqueda. El primero hace figurar los datos personales en una página de Internet; el segundo desempeña un papel decisivo en la difusión global de dichos datos, cuyos efectos se multiplican y permite la construcción de perfiles de la personalidad. Por consiguiente, un tratamiento de datos personales efectuado por un motor de búsqueda afecta significativamente a los derechos fundamentales de respeto a la vida privada y de protección de datos personales, de modo adicional al que se desprende de la actividad de los editores[386]. El mero interés económico en este tratamiento no justifica tal afección y, por su parte, el interés legítimo de los internautas en tener acceso a la información en cuestión habrá de ser objeto de ponderación, atendiendo, de un lado, a la naturaleza de la información y su carácter sensible para la vida privada de la persona afectada, y, de otro, al interés público en disponer de

[384] "La actividad de un motor de búsqueda como proveedor de contenidos, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de 'tratamiento de datos personales', en el sentido de dicha disposición, cuando esa información contiene datos personales". *Vid.* STJUE de 13 de mayo de 2014, párrafo 21.

[385] STJUE de 13 de mayo de 2014, párrafos 21 a 41 y 62 a 88.

[386] En este sentido, puede consultarse el informe elaborado por el Grupo del articulo 29 sobre la sentencia del Tribunal de Justicia de la Unión Europea con fecha 26 de noviembre de 2014 titulado *Guidelines on the implementation of the Court of Justice of the European Union judgment on " Google Spain and Inc v. AEPD and Mario Costeja González" C-131/12 (WP 225),* punto 4. Disponible en Internet: http://www.dataprotection.ro/servlet/ViewDocument?id=1080

esta información, que puede variar en función del papel que esta persona desempeñe en la vida pública.

Para el Tribunal de Justicia de la Unión Europea, el gestor del motor de búsqueda debe considerarse responsable del tratamiento de datos personales. El hecho de que los editores de páginas web puedan indicar a través de medidas técnicas que determinada información personal sea excluida de los índices automáticos de los motores no modifica la circunstancia de que el gestor determina los fines y los medios de este tratamiento y es responsable del mismo. Por lo tanto, el gestor de un motor de búsqueda puede estar obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona los vínculos a páginas web publicadas por terceros que contienen información relativa a dicha persona, incluso si esta información no se borra previa o simultáneamente de las páginas webs en que han sido publicados y aunque la publicación en dichas páginas sea lícita.

Además, el Alto Tribunal llama la atención acerca de que no podría llevarse a cabo una protección eficaz y completa de los interesados, si estos debieran obtener con carácter previo o en paralelo la eliminación de la información que les afecta de los editores de las páginas web, pues en ocasiones el tratamiento por parte del editor de la página web puede no estar sujeto al Derecho de la Unión, o puede efectuarse con fines exclusivamente periodísticos, que estarían amparados por la excepción del artículo 9 de la Directiva. Por tanto, deja recaer el peso de realizar el borrado de la información y la ponderación en el motor de búsqueda.

En cuanto a la cuestión prejudicial relativa al ámbito de aplicación territorial de la Directiva, la normativa de protección de datos europea exige que, además de realizar un tratamiento de datos personales y de ser responsable del mismo, el gestor del motor de búsqueda tenga un establecimiento en un Estado miembro o bien recurra a medios situados en el territorio de dicho Estado miembro. Para el Tribunal de Justicia de la Unión Europea, *Google Spain* se dedica al ejercicio efectivo y real de una actividad mediante una instalación estable en España, el tratamiento de datos se lleva a cabo en el marco de las actividades de un establecimiento de *Google* y tanto la actividad del gestor del motor de búsqueda como la de la instalación en España, dedicada a la publicidad, están indisolublemente ligadas, puesto que, por un lado, la actividad publicitaria es el medio para que el motor de búsqueda sea económicamente rentable, y, por otro, el motor es el medio por el cual se realiza la actividad publicitaria[387].

El problema era determinar si el prestador de servicios de Internet debía estar sometido a todas las leyes y jurisdicciones de todos los países cuyos servidores alojaran la información a la que los buscadores tuvieran acceso.

El Tribunal determinó que *Google Search* es un buscador a nivel mundial gestionado por *Google Inc*, domiciliada en Estados Unidos, pero entendió también que *Google Search* presta sus servicios en España a través de *Google Spain*. Esta filial gestiona la venta de espacios publicitarios asociada a los patrones de búsqueda introducidos por los internautas con el fin de almacenar

[387] ARENAS RAMIRO, M.: "UNFORGETTABLE: a propósito de la STJUE de 13 de mayo de 2014. caso Costeja *(Google vs AEPD*)", *Teoría y Realidad Constitucional*, núm. 34, 2014, págs. 546-547.

datos de las personas relacionados con la actividad de los clientes de servicios publicitarios que en su día contrataran con *Google Inc*[388]*.*

Por último, en cuanto al reconocimiento del derecho al olvido, el Tribunal interpreta el derecho de supresión y bloqueo en relación con el artículo 6 de la Directiva, relativo al principio de calidad de los datos, de manera que aquellos derechos serán aplicables cuando el tratamiento no se ajuste a las disposiciones de la Directiva, en particular a causa del carácter incompleto o inexacto de los datos, pero también cuando estos sean inadecuados, no pertinentes y excesivos en relación con los fines del tratamiento, no estén actualizados o se conserven durante períodos superiores al necesario, a menos que se imponga su conservación por fines históricos, estadísticos o científicos. Incluso un tratamiento inicialmente lícito de datos exactos puede resultar, con el tiempo, incompatible con la Directiva, cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron.

En congruencia con las consideraciones anteriores, el Tribunal procede a responder a la tercera cuestión prejudicial en el sentido de que los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva, esto es, los derechos de rectificación, supresión, bloqueo y oposición, deben interpretarse en el sentido de que, al analizar los requisitos de aplicación de estas disposiciones, se tendrá que examinar, en particular, si el interesado tiene derecho a que la

[388] No queda claro qué sucede en el caso de que el prestador de servicios de que se trate no tenga oficina comercial en el Estado miembro. No obstante, en razón del principio de eficacia de las garantías de la norma europea, muy posiblemente se admita también la sujeción al Derecho europeo cuando los servicios vayan destinados al continente. *Vid.* 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", en BEL, I. y CORREDOIRA, L.: *Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia*, CEPC, Madrid, 2015, pág. 412.

información personal ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados, obtenida tras una búsqueda efectuada a partir de aquel. La apreciación de la existencia de este derecho no presupone que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado, pero este puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la CDFUE, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados. En tal caso, los derechos citados prevalecen, en principio, no solo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés del público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, se exceptúa el caso de que, por razones concretas, como el papel desempeñado por el interesado en la vida pública, la injerencia en sus derechos fundamentales esté justificada por el interés preponderante del público en tener, a raíz de esta inclusión, acceso a la información de que se trate[389].

La sentencia, sin lugar a dudas, no deja indiferente. En torno a su contenido surgen luces y sombras que han sido puestas de manifiesto por la doctrina. Así, para Cotino Hueso no se percibe la magnitud de la afección a las libertades informativas que se produce al imponer obligaciones a un prestador de servicios de Internet que es esencial para el acceso a la información en el mundo. En su opinión, el interés de los usuarios de Internet en disponer de información no es considerado un contenido de la libertad de información, de

[389] STJUE de 13 de mayo 2014, párrafo 99.

manera que el acceso a la información queda desvalorizado en la ponderación con los derechos a la vida privada y a la protección de datos. De igual modo, este autor sostiene que el Tribunal de Justicia de la Unión Europea tampoco parece haber tenido en cuenta el efecto que produce que el acceso efectivo a la información en Internet, instrumentado esencialmente a través de *Google* –y otros buscadores- quede condicionado a los criterios privados, ya sean los criterios de los afectados por la información que solicitan la retirada masiva de contenidos, ya sea de *Google* a la hora de estimar o no las solicitudes de retirada[390]. A la vista de esta opinión, analizaremos los puntos clave de la sentencia sobre los que han surgido discrepancias[391].

---

[390] COTINO HUESO, L.: "El conflicto entre la libertad de expresión…*", op. cit.,* pág. 415. *Vid.* MARTÍNEZ CABALLERO, J.: *op. cit.,* pág. 174. En términos similares Rodríguez Izquierdo para quien "la comunicación pública a través de Internet las condiciones del canal de transmisión y de los medios o soportes de contenidos inciden, y mucho, en el ejercicio de las libertades informativas, tanto de los receptores como de los comunicadores". Por tanto considera que " la Setencia Google Spain, a diferencia de las conclusiones del Abogado General, resulta demasiado tajante en ese aspecto, pues el papel que el motor de búsqueda tenía en las conclusiones, como garante de la institución de la opinión pública libre, desaparece en la sentencia. La afirmación del motor de búsqueda como titular de intereses económicos, siendo cierta, ignora el papel de intermediarios que tienen estos servicios de la Sociedad de la Información. En tal medida, se les debería tratar de manera afín a los medios de comunicación, ya que no idéntica, y más si se les responsabiliza de la adecuación de los contenidos de terceros que resultan visibles tras su acción indexadora, como al fin y al cabo hace la sentencia". *Vid.* RODRÍGUEZ IZQUIERDO SERRANO, M.: "El tribunal de justicia y los derechos en la sociedad de la información: privacidad y protección de datos frente a libertades informativas", *ReDCE,* núm. 24, 2015, disponible en Internet: http://www.ugr.es/~redce/REDCE24/ReDCEsumario24.htm

[391] ARENAS RAMIRO, M.: "UNFORGETTABLE…", *op. cit.*, págs. 554-557. Por su parte, Murga Fernández enumera los riesgos que lleva aparejado el reconocimiento del derecho al olvido: "El primero de estos riesgos viene a ser la posibilidad de borrar o reescribir la historia a la medida de cada cual, alterando la objetividad de lo ocurrido, modificando su contenido o imposibilitando el acceso a esa información a los demás. En segundo lugar, puede apuntarse que el derecho al olvido podría constituir un obstáculo al normal funcionamiento de los canales de información que necesitan los ciudadanos para desarrollar sus actividades. Asimismo, el derecho al olvido podría tener una incidencia negativa sobre la transparencia que debe acompañar a toda información, ya que a través de su ejercicio se podría llegar a primar el derecho a la protección de datos sobre el derecho a la información. Finalmente, la responsabilidad de los motores de búsqueda en el tratamiento de los datos puede convertirlos en verdaderos jueces a la hora de determinar el alcance del derecho al olvido…", *vid,* MURGA FERNÁNDEZ, J. P.: "La protección de datos y los motores de búsqueda en Internet: cuestiones actuales y perspectivas de futuro acerca del derecho al olvido", *Revista de Derecho Civil,* núm. 4, 2017, pág. 204.

En primer lugar, sobre la cuestión de considerar a *Google* responsable del tratamiento de la información publicada por terceros**,** la sentencia deja relativamente claro que los datos personales que *Google* indexa en una búsqueda por el nombre y los apellidos –por ejemplo de un boletín oficial, un periódico o hemeroteca digital- pueden ser legítimos en origen y no tiene por qué impedirse su acceso por otras vías, pero, puede ser necesario que dicha información desaparezca de los resultados de *Google*. Hay autores que ponen en duda esta conclusión, puesto que comparten la posición del Abogado General de que en esa actividad de indexación *Google* actúa como mero intermediario[392], ajeno a cualquier control efectivo sobre la misma, relativo a comprobar su exactitud o veracidad[393]. En este debate sobre la neutralidad de los buscadores deben tenerse en cuenta dos factores: por un lado, que los gestores de los motores de búsqueda cada vez se relacionan más con los titulares de las páginas webs que publican la información que luego indexan; y, de otro lado, que los gestores de los motores de búsqueda prestan otro tipo de servicios, utilizando a sus propios buscadores para dar la mayor difusión posible a los mismos. De lo cual podría deducirse que la actividad de mera intermediación daría paso a otra mucho más activa y asimilable a la de generación de contenidos[394].

---

[392] Sobre la idea de intermediarios neutrales, *vid.* VAN ALSENOY, B, KUCZERAWY, A y AUSLOOS, J.: "Search engines after Google Spain: internet@liberty or privacy@peril?", *ICRI Research Paper*, núm. 15, 2013, pág. 67.

[393] MARTÍNEZ MARTÍNEZ, R.:"Google es un responsable del tratamiento muy particular. No decide qué hacer con los datos ni puede eliminarlos en origen, solo puede desindexar. Google sí es responsable de los datos de sus usuarios directos y de lo que almacene si falla el robot.txt, o si desaparecida una información en origen, la sigue manteniendo", en "Las costuras de la privacidad", *El País*, 25 de junio de 2013. Disponible en Internet: http://sociedad.elpais.com/sociedad/2013/06/25/actualidad/1372191768_928841.html.

[394] Sobre esto, consúltese BENGHOZI, P, J.: "Les moteurs de recherche: trou noir de la regulation?" en STROWEL, A. et TRIAILLE, J. P. (dirs.): *Google et les nouveaux services en*

Desde la posición que defiende el papel de intermediarios de los buscadores, su responsabilidad debería limitarse a la posibilidad de retirar datos de sus servidores y suprimir los *links* siempre que el responsable de la página web de origen no fuera localizado o técnicamente no pudiera evitar el acceso a dicha información o, incluso, cuando los buscadores tengan conocimiento efectivo de que están realizando enlaces a contenidos nocivos[395].

Situadas en esta perspectiva, el editor de la página web de origen tendría que cumplir solo con sus obligaciones de evitar que la información se disemine sin consentimiento del interesado, realizar una estimación del impacto de sus actuaciones y tomar las medidas adecuadas al efecto, o tratar los menos datos personales posibles, para evitar su perdida, alteración o uso indebido. Comparten la opinión de que a *Google* no se le puede hacer responsable final del olvido Simón Castellano y Guichot Reina[396].

---

ligne. Impact sur l'économie du contenu et questions de propiéte intellectuelle, Larcier, Bruselas, 2008, págs. 83-101. También SARTOR, G. y VIOLA DE AZEVEDO CUNHA, M.: "The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents", *International Journal of Law and Information Technology*, vol. 18, núm. 4, 2010, págs. 356-378.

[395] Sobre la responsabilidad de los motores de búsqueda cuando el editor haya utilizado código de exclusión, cuando se emplea la función de autocompletado de la búsqueda ofrecida por el motor de búsqueda, o en el supuesto de enlaces a páginas que albergan copias de una información declarada judicialmente ilícita, *vid.* MIERES MIERES, L. J.: *op. cit.,* págs. 47- 48. Sobre la reparación de los daños causados por el buscador en relación con la función "autocompletar la búsqueda" en perspectiva comparada SIMÓN CASTELLANO, P.: *El reconocimiento del derecho al olvido digital*…, pág. 51.

[396] En este sentido, Simón Castellano "En contra de lo dictado por el tribunal europeo, (…) considera que la responsabilidad no es únicamente del motor de búsqueda, sino que debería ser compartida con el autor de la información original. Especialmente en el caso de las publicaciones en boletines oficiales", *vid.* "La UE obliga a Google a retirar enlaces con información lesiva", *El País,* 13 de mayo de 2014. Disponible en Internet: http://sociedad.elpais.com/sociedad/2014/05/12/actualidad/1399921965_465484.html. También GUICHOT REINA, E. (coord.): *Derecho de la Comunicación*, Iustel, Madrid, 2013, pág. 223, señala que "resulta altamente cuestionable atribuir a los buscadores la responsabilidad de garantizar la cancelación de datos y no a los responsables de la publicación de la información".

No obstante, también hay razones a favor de la atribución de responsabilidad a los intermediarios y la exigencia de aquella en el lugar de la web fuente, basadas en la mayor capacidad económica del intermediario, en la necesidad de dar solución a los casos en los que la situación geográfica del infractor web fuente dificulta la acción contra él, en definitiva, en la mayor eficacia que tiene actuar sobre el intermediario ante cierto tipos de pretensiones, como impedir el acceso futuro a una determinada información[397]. Así, Vilasau Solana comparte la respuesta del Tribunal de Justicia y considera que *Google* es responsable del tratamiento, basando su posición en que los buscadores permiten una visualización, inmediatez y ubicuidad de la información que sin estos no sería posible, pero, sobre todo, teniendo en cuenta su protagonismo en el actual marco de la sociedad de la información[398].

En mi opinión, la sentencia resuelve un caso concreto, por tanto no se puede extrapolar a otros supuestos. La solución dada en el fallo judicial está llena de matices que habrá que tener en cuenta a la hora de tratar otros litigios en torno al derecho al olvido. Sí me parece adecuado resaltar la postura del Tribunal de Justicia de la Unión Europea que ha destacado el papel que cumplen los buscadores y su impacto en el derecho fundamental a la protección de datos y lo ha explicado distinguiendo expresamente entre la posición de los medios de comunicación en el tratamiento de datos personales con fines periodísticos y la de los motores de búsqueda, que responde a

[397] PAZOS CASTRO, R.: "El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales ¿una relación imposible?", *Indret*, núm. 1, 2015, pág. 28.

[398] VILASAU SOLANA, M.: "El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido (análisis de la STJUE de 13 de mayo de 2014)", *Revista de Internet, Derecho y Política*, núm. 18, 2014, pág. 22.

intereses económicos en el marco de la libertad de empresa. Por tanto, no puedo compartir la opinión de quienes atribuyen al buscador el mismo interés ajeno legítimo que podría alegar el editor de la página, esto es, atender al derecho a obtener información de los internautas. En la medida en que los usuarios suelen buscar información contenida en Internet a través de motores de búsqueda, los servicios del buscador forman parte casi insustituible del proceso de acceso a la información y quedan, por lo tanto protegidos también por el artículo 20.1.a) y d) de la Constitución[399], pero, a mi juicio, esta resolución no afecta al derecho a ser informados de los usuarios de Internet porque la información no desaparece de donde está y solamente se desindexa de las búsquedas de *Google* que se hagan por el nombre y apellidos del afectado. Por lo tanto, rastreándola de otro modo se seguirá encontrando. En definitiva, solo afecta a la forma de búsqueda.

En este sentido, la guía de aplicación práctica del Grupo de Trabajo del artículo 29 contempla la posibilidad de que el individuo pueda considerar que es mejor, dadas las circunstancias del caso, ponerse en contacto primero con la webmaster original para solicitar la supresión de la información o la aplicación de protocolos "sin índices", pero la sentencia no requiere esto. Y, por la misma razón, un individuo puede elegir cómo ejercer sus derechos en relación con los motores de búsqueda seleccionando uno o varios de ellos. Al

[399] *Vid.* MARTÍNEZ OTERO, J. M.: "El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja", *Revista de Derecho Político, UNED,* 2015, págs. 123-124. Abundando en estos argumentos la dimensión investigadora del derecho a la información, afirma Martínez Sospedra, que " la libertad de informar presupone la libertad de obtener información. Por tanto, como no cabe información y mucho menos información veraz, sin previa búsqueda y obtención de la misma se sigue que forma parte del contenido esencial de aquella la libertad de investigar". *Vid.* MARTÍNEZ SOSPEDRA, M.: *Libertades públicas,* vol. I, Fundación Universitaria San Pablo CEU, Valencia, 1993, pág. 259.

hacer una solicitud a uno o varios de los buscadores, el individuo está evaluando el impacto de la aparición de la información controvertida en uno o varios de los motores de búsqueda y, en consecuencia, la decisión sobre los recursos que puedan ser suficientes para disminuir o eliminar ese impacto.

En cualquier caso, hay cuestiones que quedan sin resolver en la sentencia. Ante todo, si el alcance del derecho al olvido digital englobaría también los datos incluidos en las búsquedas que se pueden realizar en las hemerotecas digitales o página fuente. De la misma manera, subsiste el interrogante de qué ocurre cuando la búsqueda en el navegador se efectúa conforme a otros criterios como una palabra injuriosa que da como resultado una lista en la que aparezcan páginas web con el nombre y apellidos del afectado que este considere descontextualizadas, inadecuadas, no pertinentes o excesivas. Tampoco deja resuelta la cuestión de cuánto tiempo debe transcurrir para que *Google* deba atender el derecho al olvido.

En segundo lugar, se le critica al fallo judicial que la obligación concreta de *Google* de eliminar los *links* no consigue el verdadero objetivo. Estos datos dejarían de estar disponibles en territorio europeo, pero la información puede seguir circulando por la red y puede ser indexada por otros buscadores, así como desde fuera del territorio de la Unión Europea[400]. En mi opinión, la

[400] Sobre el ejercicio del derecho al olvido no solo frente a "Google.es", sino frente a "Google.com" consúltese el procedimiento TD/00921/2015 en la memoria anual de la AEPD 2015. El Tribunal de Gran Instancia de Paris, en sentencia de 16 de septiembre de 2014 declaró contraria al derecho europeo la interpretación según la cual Google solo estaría obligada a desindexar los enlaces en las extensiones nacionales allí donde residiera el afectado y condenó a *Google* por no retirar enlaces del buscador general ".com". Sobre las críticas a esta resolución vid. GARCÍA MEXÍA, P.: " Olvido en Internet: mejor una mentira en el aire que una verdad en el cajón" en el blog *la Ley en la red,* 2014. Disponible en Internet: http://abcblogs.abc.es/ley-red/public/post/olvido-en-internet-mejor-una-mentira-al-aire-que-una-verdad-en-el-cajon-15898.asp/

sentencia no está reconociendo un derecho al olvido en Internet, sino que da respuesta a unas preguntas en torno a un litigio concreto, lo que explica que en ella se demande borrar los enlaces, pero no la información.

La información, efectivamente, no desaparece de donde está y, simplemente, buscándola de otro modo se seguirá encontrando. En estas condiciones, pensamos que resulta exagerado hablar de censura. Por el contrario, el Tribunal viene a interpretar los derechos de cancelación y oposición de manera lógica en el conflicto entre libertad de empresa y derecho fundamental a la protección de datos, conforme al sentido que se deriva de uno de los principios que informan este derecho, como es el de calidad de los datos. En esta línea, afirma la sentencia que "un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron".

No cabe duda de que en el asunto *Google Spain*, el anuncio de la subasta era veraz pero no era una información exacta porque inducía al error de considerar vigente un embargo que ya estaba cancelado con el consiguiente perjuicio para el afectado, ya que, ante una búsqueda por su nombre en *Google,* se daba de él la imagen de que podía ser una persona insolvente. En consecuencia, mediante el ejercicio de estos derechos se le garantiza al perjudicado que en las búsquedas realizadas por su nombre -en un determinado buscador- no se ofrezcan resultados obsoletos, fuera de la actualidad y que pugnen con el principio de calidad de los datos. Y como los derechos fundamentales no son absolutos, y este caso no es una excepción, el interés público de la información vendría a imponer límites.

Para Álvarez Caro, considerando que solo *Google* debe proceder al borrado de los datos, no tiene mucho sentido justificar el borrado alegando que carece de interés público mientras se permita que tales datos permanezcan en la web de origen o estén accesibles a través de otros buscadores de Internet. Si no tiene interés público, debería carecer de dicho interés para todos los buscadores y la única manera de asegurar la no indexación por ningún buscador es la toma de medidas simultáneas o previas por parte del editor web, incorporando los protocolos de exclusión[401]. Sin embargo, a mi juicio, esta solución es técnicamente imposible, pues no se pueden eliminar todas las copias que puedan existir de los datos. De ahí que la sentencia haya delimitado el derecho al olvido digital, teniendo en cuenta los condicionantes impuestos por la realidad.

En tercer lugar, se reprocha que la aplicación práctica de la sentencia, esto es, el deber de ponderar los derechos en conflicto, recae sobre el motor de búsqueda, en este caso *Google,* lo cual excede de sus competencias. En su lugar, Piñar Mañas sostuvo que debería realizarla el editor[402] y, en su caso, los tribunales. Se ha dicho del conflictivo derecho al olvido que se trata de "un falso derecho a juzgar por un falso tribunal"[403].

Ciertamente, la ponderación debe situarse en el marco señalado por el Tribunal de Justicia de la Unión Europea, pero este no determina criterios

---

[401] ÁLVAREZ CARO, M.: *op. cit.*, pág. 124.

[402] Piñar Mañas afirma que "la cuestión es hasta qué punto *Google* es responsable de la información y hasta qué punto puede convertirse, ahora sí, en una especie de censor. Habría sido mucho más preciso exigir que fuera el editor el que tomara medidas para no indexar la información", en " Defiendo la privacidad. No me he pasado al enemigo", *El País*, 8 de junio de 2014. Disponible en Internet: http://sociedad.elpais.com/sociedad/2014/06/08/actualidad/1402249205_539753.html

[403] COTINO HUESO, L.: "El conflicto entre las libertades…", *op. cit.,* pág. 406.

claros que la orienten[404]. A mi juicio, son dos las pautas que marca la sentencia ante futuros conflictos entre el derecho fundamental a la protección de datos y las libertades informativas: el interés público actual y el paso del tiempo. En este sentido De Terwangne afirma que "el valor informativo de un caso inclina la balanza a favor del derecho a difundir a costa del derecho al olvido. Y en cuanto deja de tener valor la noticia, la balanza se inclina en la otra dirección"[405]. Por su parte, Boix Palop ha planteado la posibilidad de que el paso del tiempo opere en sentido inverso, dotando de interés público a informaciones que inicialmente no la tenían o que dejaron de tenerlo, y que por ello fueron objeto del derecho al olvido. En estos supuestos, el derecho al olvido hurtaría del conocimiento general informaciones que podrían resultar importantes[406].

Hay quien sostiene que el comportamiento racional del buscador, para precaverse frente a la amenaza de eventuales responsabilidades ante la autoridad de protección de datos, puede ser acceder en caso de duda al borrado de los vínculos que haya solicitado el interesado[407]. En cualquier caso,

---

[404] MIERES MIERES, L. J.: *op. cit.,* pág. 45.

[405] DE TERWANGNE, C.: "Privacidad en Internet y derecho a ser olvidado/derecho al olvido", *IDP:* r*evista de Internet, derecho y política*, núm. 13, 2012, pág. 56.

[406] 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*, núm. 38, 2015, pág. 32.

[407] MIERES MIERES, L. J.: *op. cit*., pág. 45. *Vid.* Van Alsenoy, Kuczerawy y Ausloos advierten del riesgo de sobrecumplimiento de la normativa eliminando más vínculos de los necesarios para proteger el derecho. VAN ALSENOY, B. KUCZERAWY, A. y AUSLOOS, J.: *op. cit.* Martínez Caballero da cuenta de que según el Informe de Transparencia de Google del año 2012 se realizaron 42.327 solicitudes de datos sobre 68.249 usuarios, de donde deduce que un juez no puede dictar ese número de sentencias en un año examinando el fondo del asunto. *Vid.* MARTÍNEZ CABALLERO, J.: *op. cit.*, págs. 170-171. Por su parte Martínez Martínez, ilustra la conclusión de que cualquier petición a Google de borrar búsquedas será aceptada con el caso Bayarri, *vid.* MARTÍNEZ MARTÍNEZ, R.: "Aplicar el derecho al olvido", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 36, 2014. Disponible en Internet: http://www.unir.net/derecho/revista/noticias/la-anonimizacion-de-las-sentencias-del-tribunal-contitucional/549201456751/.

entiendo que si el buscador se excediera en sus atribuciones operarían los mecanismos de garantía propios del Estado de Derecho, esto es, la agencia de protección de datos y los tribunales.

A pesar de todas las cuestiones que deja abierta la sentencia, mi valoración sobre el pronunciamiento del Tribunal de Justicia de la Unión Europea es positiva, pues pone termino a la situación de desprotección generada por la negativa de la empresa *Google* a someterse a la normativa europea y española sobre la materia, estableciendo que el derecho fundamental a la protección de datos prevalece sobre la libertad de empresa, esto es, el mero interés económico del gestor del motor de búsqueda, salvo que el interesado tenga relevancia pública y el acceso a la información esté justificado por el interés público actual. Por lo tanto, lo decisivo de la sentencia es que toca cuestiones concluyentes para la efectividad del derecho fundamental a la protección de datos personales en Internet[408].

La Sala de lo Contencioso de la Audiencia Nacional, Sección Primera, en su sentencia de 29 de diciembre de 2014, ha resuelto finalmente el caso Mario Costeja integrando los argumentos de la STJUE de 13 de mayo de 2014.

De conformidad con una nota de prensa publicada por la AEPD en 2016[409], en el caso de los procedimientos de tutela por el denominado derecho al olvido frente a buscadores, desde la sentencia del Tribunal de Justicia de la

---

[408] Buisán García considera la sentencia un hito que contribuirá a regular, jurídicamente, la actividad de Internet. Según sus palabras "pronunciamientos así empiezan a ser imprescindibles no solo para tratar de ordenar la ilimitada potencialidad comunicadora de la red sino, sobre todo, para garantizar los derechos de los ciudadanos en dicha nueva realidad virtual". *Vid*. BUISÁN GARCÍA, N.: *op. cit.*, pág. 35.

[409] Nota de prensa disponible en Internet: http://www.agpd.es/portalwebAGPD/revista_prensa prensa/2016/notas_prensa/news /2016_06_20-ides-idphp.php

Unión Europea de 2014, la Agencia ha dictado 371 resoluciones, en las que se ha estimado la petición en 157 ocasiones y desestimado en 82. En 131 casos la petición se ha inadmitido, ya que los reclamantes no se habían dirigido con anterioridad al buscador solicitando la cancelación de los datos tal y como exige la legislación. En cuanto a las sentencias de la Audiencia Nacional recaídas en los recursos interpuestos contra resoluciones de la AEPD, del total de 201 sentencias dictadas en 2015, un 76% confirmaron los criterios de la Agencia en cuanto al fondo del asunto. A esta doctrina de la Audiencia hay que añadir la Sentencia del Tribunal Supremo de la Sala de lo Civil de 15 de octubre de 2015, sobre la obligación de los editores de adoptar medidas para evitar la indexación de informaciones por parte de los buscadores cuando las noticias sean ya obsoletas y haya sido solicitado por los afectados[410].

La regulación del derecho al olvido en el ámbito europeo ha sido fruto de la tramitación de la propuesta de Reglamento de la Comisión Europea presentada el 25 de enero de 2012[411], aprobada finalmente con modificaciones por el Parlamento Europeo y publicada en el Diario Oficial de la Unión Europea

[410] Memoria anual de la AEPD 2015.

[411] Se regulaba separadamente el derecho de rectificación en el artículo 16 y el derecho de oposición en el artículo 19. El artículo 17 establecía el derecho del interesado al olvido y de supresión. Asimismo elaboraba y especificaba el derecho de supresión que se establece en el artículo 12, letra b), de la Directiva 95/46/CE y establecía las condiciones del derecho al olvido, incluida la obligación del responsable del tratamiento que haya difundido los datos personales de informar a los terceros sobre la solicitud del interesado de suprimir todos los enlaces a los datos personales, copias o réplicas de los mismos. También integraba el derecho a que se restringiera el tratamiento en determinados casos, evitando la ambigüedad del término "bloqueo". Disponible en Internet: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf.El Parlamento Europeo, en Resolución de 12 de marzo de 2014, rechazó la denominación de derecho al olvido y la sustituye por derecho a la supresión. Disponible en Internet: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF. Sobre este particular, el derecho al olvido durante la tramitación de la propuesta del Reglamento vid, MORENO MARÍN, M. D.: "El derecho al olvido en el marco del nuevo Reglamento General de Protección de Datos" en BUENO DE MATA, F (dir/coord.): *Fodertics 6.0 Los nuevos retos del derecho ante la era digital*, Comares, Granada, 2017, págs. 380-382.

el 4 de mayo de 2016. Indudablemente, también ha influido en su reconocimiento y alcance la resolución por el Tribunal de Justicia de la Unión Europea de las cuestiones prejudiciales sobre la interpretación que había de darse a la Directiva 95/46/CE en el asunto Google contra Mario Costeja[412]. Desde el punto de vista normativo, la cuestión que debía resolver el legislador europeo era definir el derecho al olvido como una manifestación de la facultad de cancelación del derecho fundamental a la protección de datos o como un derecho más amplio, como la facultad de impedir que terceros recuerden sucesos veraces que en su día revistieron notoriedad pública[413]. Finalmente, este derecho se ha configurado en el Reglamento como una consecuencia del derecho al borrado (el borrado conduce al olvido) y como una obligación del responsable que ha hecho públicos los datos que han de ser borrados de comunicar el mismo a los demás responsables a los que se hayan podido ceder[414].

Regulado en el artículo 17 del RGPD, como expusimos al principio de este capítulo, el derecho al olvido se podrá ejercer contra todo responsable del tratamiento que determine los fines y los medios del mismo, sea persona física o jurídica. La práctica del derecho al olvido se concreta jurídicamente en el

---

[412] Aunque la sentencia se formula sobre la base de la anterior normativa, el Tribunal de Justicia de la Unión Europea interpreta no solo la Directiva, sino que afirma que el derecho de los interesados dimana de la Carta de derechos fundamentales de la Unión Europea, en concreto de los derechos a la intimidad y el derecho de protección de datos (arts. 7 y 8). En este sentido COTINO HUESO, L: "El conflicto…", *op. cit.,* pág. 408.

[413] Los países de tradición juridica del *common law* son más reacios al reconocimiento al derecho al olvido. La jurisprudencia estadounidense se ha decantado por esta solución. Como ha señalado Touriño en Estados Unidos "el debate del derecho al olvido es un tema resuelto y zanjado, por haber entendido el poder judicial estadounidense de manera reiterada que tratar de impedir la libre disposición de resultados de los buscadores chocaría frontalmente con los valores constitucionales" consagrados en la Primera Enmienda. TOURIÑO, A.: *El derecho al olvido y a la intimidad en Internet*, Catarata, Madrid, 2013, pág. 42.

[414] AEPD Memoria anual 2015, pág. 75.

ejercicio del derecho de supresión contra el responsable del tratamiento de los datos personales cuando por aplicación del principio de calidad estos no sean ya necesarios para los fines para los que fueron recogidos o tratados o si el tratamiento incumple de otro modo el Reglamento. De igual manera, el afectado tendrá derecho a que se supriman y dejen de tratarse sus datos personales cuando revoque el consentimiento o se oponga al tratamiento. En el primer caso, este derecho es pertinente si el interesado dió su consentimiento siendo menor de edad y sin ser plenamente consciente de los riesgos que implica el tratamiento y más tarde, alcanzada la madurez, quiere suprimir tales datos personales en Internet[415].

En particular, el derecho al olvido en el contexto de Internet se podrá ejercer contra todo prestador de servicios de la sociedad de información. Si se ejerce frente al responsable de la publicación original y este ha hecho públicos los datos, el Reglamento[416] le impone la obligación de indicar a los responsables que estén tratando tales datos personales que supriman todo enlace a ellos o las copias o réplicas de tales datos, por lo cual debe tomar las medidas técnicas necesarias para informar de la solicitud de supresión del interesado.

Desde el punto de vista de las nuevas tecnologías, la cuestión relativa a las herramientas a través de las cuales se llevaría efecto el derecho de supresión u olvido es objeto de debate. Cabría acudir, por ejemplo, al empleo de protocolos de exclusión (robot.txt)[417]. Esta etiqueta, colocada en un

[415] *Vid*. considerando 65 RGPD.
[416] Artículo 17.2 RGPD.
[417] Sentencia de la Sala de lo Civil del Tribunal Supremo de 15 de octubre de 2015.

determinado contenido, evita la indexación por los buscadores. Junto a esta solución, estaría la tecnología *vanish,* que consiste en programar los contenidos digitales para su autoeliminación pasado un determinado período de tiempo, lo que, por otra parte, supone un obstáculo para la investigación histórica. Otra alternativa sería la solución intermedia, es decir, programar la aparición de la etiqueta que impide la indexación, de modo que no se eliminase el contenido, pero que a partir de un plazo razonable dejara de estar disponible en los buscadores de Internet. Esta opción podría operar en sentido bidireccional, eliminando la posibilidad de indexación pasados unos años de la publicación, y devolviéndola tras otro plazo de tiempo mayor con la intención de facilitar la investigación histórica. Por último, los responsables de medios digitales han propuesto el derecho al actualizado o rectificado respecto a ciertas noticias relacionadas con actuaciones policiales o judiciales, que supondría la obligación del medio de completar las noticias del pasado con enlaces a noticias relacionadas más recientes que reflejan cómo termina el procedimiento o actuación judicial[418].

En definitiva, el artículo 17.2 del RGPD contiene una obligación de conducta por parte del responsable principal, más que una obligación de resultado.

En el caso de que los datos sean tratados lícitamente por el responsable, el afectado debe tener derecho a oponerse al tratamiento. Ello dará lugar a una ponderación, debiendo demostrar el responsable que sus

[418] MARTÍNEZ OTERO, J, M.: *op. cit.*, págs. 136-137. El autor pone como ejemplo la edición de 2014 del Libro de estilo del Diario El País donde ya se prevé específicamente la problemática del derecho al olvido.

intereses legítimos deben prevalecer sobre los derechos y libertades fundamentales del interesado[419]. A mi juicio, y a la vista de la sentencia del Tribunal de Justicia de la Unión Europea, esta circunstancia no impedirá que, aunque no proceda el derecho de oposición frente al responsable de la información, pueda obtener la supresión o, más bien, la no indexación frente al motor de búsqueda. En este sentido, Troncoso Reigada apunta que el Reglamento construye el derecho al olvido en Internet sobre las obligaciones del responsable principal de la *webmaster* que ha hecho público los datos[420], frente a la postura de la AEPD, que había defendido que el derecho al olvido en Internet debía girar en torno al derecho de oposición ejercido sobre los motores de búsqueda, considerados estos como responsables de sus propios tratamientos.

Por el contrario, para Cotino Hueso de la sentencia del Tribunal de Justicia de la Unión Europea debe extraerse que ahora *Google* no podrá considerarse como un "tercero", sino también "responsable" del tratamiento de datos, un segundo responsable si se quiere, a partir de la información que rastrea y capta de Internet entre los datos introducidos por los "iniciales" o primeros responsables de datos. Para este autor, el Reglamento habrá de partir de que el interesado puede perfectamente dirigirse solo a *Google,* esto es, no

---

[419] *Vid.* considerando 69 RGPD.

[420] TRONCOSO REIGADA, A.: "Las redes sociales a la luz de la Propuesta de Reglamento general de Protección de Datos Personales", *Revista de Internet, Derecho y Política*, Universitat Oberta de Catalunya, núm. 16, 2013, pág. 33. En el mismo sentido Martínez Caballero, para quien "el sujeto directamente obligado por el derecho al olvido es quien ha tratado y hecho público en alguna página de Internet los datos personales que el afectado quiere suprimir, Las otras páginas o servicios que multiplican la publicidad de esos datos al mantener copias o enlaces a ellos no serían los destinatarios de manera autónoma sino que estarían obligados a suprimir esas copias o enlaces, si la fuente primera de la divulgación los ha bloqueado previamente… Como es palpable, el Tribunal de Justicia de la Unión Europea no ha compartido y tenido en cuenta esta consideración a la hora de dictar sentencia en el caso *Google Spain*". *Vid.* MARTÍNEZ CABALLERO, J.: *op. cit.,* pág. 163.

reclamar la supresión de la información en origen del editor de la web que contiene los datos personales indexados por *Google*. De igual modo, el tratamiento de datos del editor o responsable original puede ser legítimo, pero ello no significa que también lo sea el de *Google*[421].

Por último, como todos los derechos fundamentales, el derecho al olvido digital también está sujeto a límites. La retención ulterior de los datos personales será lícita cuando responda al ejercicio de las libertades de expresión e información, al cumplimiento de una obligación legal o de una obligación realizada en interés público o en el ejercicio de los poderes públicos conferidos al responsable del tratamiento, a razones de interés público en el ámbito de la salud pública, a fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o a la formulación, el ejercicio o la defensa de reclamaciones.

El Reglamento no establece los criterios para determinar cuándo la libertad de expresión e información prevalecen sobre el derecho de supresión o derecho al olvido. A la vista de la jurisprudencia del Tribunal de Justicia de la Unión Europea, puede deducirse que el derecho al olvido digital cederá frente a las libertades informativas cuando la conservación, divulgación o publicación de los datos personales sea necesaria para la finalidad perseguida, debido a la relevancia pública actual de la información o del personaje, y, en todo caso, habrá que atender al juicio de proporcionalidad. El Reglamento ha previsto en el artículo 85 que los Estados miembros puedan establecer excepciones, entre otras materias, a los derechos de los titulares de los datos cuando sea

[421] COTINO HUESO, L.: "El conflicto entre las libertades de expresión…", *op. cit.,* págs. 408-409.

necesario para conciliar el derecho de protección de datos personales con las libertades de expresión e información[422].

Por tanto, el derecho al olvido está regulado por el Reglamento y limitado por las libertades de expresión e información. Cada Estado podrá establecer el contenido de este derecho, si bien su nivel de protección no podrá ser inferior al que se derive de la Carta, según la interpretación del Tribunal de Justicia de la Unión Europea. Así, en la sentencia de 26 de febrero de 2013, asunto C-617/10, caso Akerberg Fransson*,* el Tribunal de Justicia de la Unión Europea estableció el grado de vinculación a los derechos fundamentales de la

[422] Artículo 85. 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." *Vid.* también el considerando 153: "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".

Carta que es exigible a los Estados de acuerdo con su artículo 53, cuando actúan dentro del ámbito del Derecho de la Unión Europea, dictando que "en una situación en la que la acción de los Estados miembros no esté totalmente determinada por el Derecho de la Unión, las autoridades y tribunales nacionales siguen estando facultados para aplicar estándares nacionales de protección de los derechos fundamentales, siempre que esa aplicación no afecte al nivel de protección previsto por la Carta, según su interpretación por el Tribunal de Justicia, ni a la primacía, la unidad y la efectividad del Derecho de la Unión (véase, en este sentido, la sentencia de 26 de febrero de 2013, *Melloni*, C-399/11, apartado 60)"[423].

Por el contrario, la norma comunitaria precisa los motivos de interés público en el ámbito de la salud pública por los cuales el derecho fundamental a la protección de datos debe ceder, entre los que se encuentran el supuesto de que el tratamiento sea necesario para fines de medicina preventiva o laboral o para la protección contra riesgos sanitarios transfronterizos graves o de que sea imprescindible para garantizar altos niveles de calidad y seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios[424]. Lo mismo ocurre cuando el tratamiento responda a fines de investigación histórica, estadística y científica, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dichos tratamientos. No obstante, la apreciación de estos supuestos estará sujeta al principio de proporcionalidad mediante el empleo de garantías adecuadas, que exigirán que se disponga de medidas técnicas y organizativas, tales como la

[423] Apartado 29 de la STJUE de 26 de febrero de 2013, asunto C-617/10, Akerberg Fransson.
[424] Artículo 9.h) e .i) y párrafo 3 RGPD.

seudonimización, para asegurar el respeto al principio de minimización de los datos personales o, incluso, la sustitución, siempre que sea posible, por un tratamiento ulterior que no permita o ya no permita la identificación de los interesados[425].

Por último, hay que añadir que a la cuestión de la configuración de los límites concretos al ejercicio del derecho al olvido digital la contribución que han hecho las resoluciones de la AEPD, que, como ha resaltado Simón Castellano, han resultado fundamentales para la protección de la dignidad humana, el libre desarrollo de la personalidad y la tutela de los datos personales en el contexto digital, a la par que no han tutelado intereses meramente particulares, ni limitado las libertades informativas[426].

[425] Artículo 89 RGPD.
[426] SIMÓN CASTELLANO, P.: *El reconocimiento*…, pág. 221.

Capítulo tercero

EL DERECHO AL OLVIDO DIGITAL DEL PASADO PENAL

1. EL PASADO PENAL: REPERCUSIONES PARA LOS DERECHOS DE LA VIDA PRIVADA.1.1. Antecedentes penales. 1.2. Indultos. 1.3. La publicidad de las resoluciones judiciales. **2. EL DIFÍCIL EQUILIBRIO ENTRE EL DERECHO AL OLVIDO DIGITAL DEL PASADO PENAL Y OTROS DERECHOS Y PRINCIPIOS CONSTITUCIONALES EN LA JURISPRUDENCIA DEL TRIBUNAL SUPREMO.** 2.1. El derecho al olvido digital y las libertades informativas. 2.2. El derecho al olvido digital y el principio de transparencia.

1. EL PASADO PENAL: REPERCUSIONES PARA LOS DERECHOS DE LA VIDA PRIVADA.

Está fuera de toda duda que la transparencia de los poderes públicos y la protección de los datos personales son dos pilares esenciales para la configuración de las actuales sociedades de la información como verdaderas sociedades democráticas en las que, al tiempo que se fomenta el control eficaz de la actuación de los gobernantes y la participación de la ciudadanía en los asuntos públicos, se protegen y se respetan de manera adecuada los derechos y las libertades de los individuos, en particular los relacionados con la esfera personal y el libre desarrollo de la personalidad[427].

Por otra parte, en la tradición jurídica europea es esencial para la garantía de la dignidad humana la necesidad de olvidar el pasado penal. Ahora bien, la sociedad se ha limitado a regular determinadas situaciones en las que el mero transcurso del tiempo conlleva la caducidad de sus efectos jurídicos. Como señala Rallo Lombarte, "hoy por hoy sigue viva la convicción social de que resulta intrínseco a la garantía de la dignidad humana *olvidar* en determinados ámbitos -especialmente sensible resulta el criminal-. Por ello, lejos de conceptualizar y regular un derecho autónomo al olvido, la sociedad se ha limitado a identificar y normar concretas y heterogéneas situaciones en las que el paso del tiempo aboca a la caducidad y olvido de sus efectos jurídicos"[428].

---

[427] RODRÍGUEZ ÀLVAREZ, J. L.: *op. cit.*, pág. 53.
[428] *Vid.* RALLO LOMBARTE, A.: *El derecho al olvido en Internet, Google versus…,* pág. 24.

En la doctrina francesa, el derecho al olvido tiene su fundamento jurídico en instituciones como la amnistía, la prescripción de antecedentes penales o la disociación de los datos que contienen las sentencias judiciales[429]. A continuación, vamos a analizar la situación del derecho al olvido del pasado penal en el ordenamiento jurídico español, desde la triple perspectiva que se apunta.

1.1. Antecedentes penales.

A lo largo de largo de la historia, la aparición de ciertas modalidades de "derecho al olvido" ha ido unida a la progresiva juridificación, inicialmente tácita, del valor de la dignidad humana. Así, ya el 22 de febrero de 1813, las Cortes de Cádiz, al tiempo que abolieron la Inquisición, decretaron la desaparición de los sambenitos que obligatoriamente permanecían colgados y etiquetados en las iglesias, para que perdurase la infamia caída sobre los condenados y sus familias[430]. La figura de la cancelación de antecedentes penales obedece a la misma finalidad de permitir a la persona su rehabilitación social y jurídica y de evitar que cargue toda su vida con la marca que imprime la comisión de un delito. Sin embargo, en la red no hay "amnesia". Para las personas aludidas en noticias y sentencias, la red puede convertirse, de hecho, en un Registro de condenas de eficacia perpetua, que obliga a las personas a soportar durante toda su vida el desvalor social que conlleva su implicación en un delito. El

[429] SIMÓN CASTELLANO, P.: "El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos", en CORREDOIRA, L. y COTINO HUESO, L. (dirs).: *Libertad de expresión e información en la Red. Amenazas y protección de los derechos personales*, CEPC, Madrid, 2013, pág. 453.

[430] SÁNCHEZ SAUS, R.: "El derecho al olvido", *Diario de Sevilla*, 15 de mayo de 2014, disponible en http://www.diariodesevilla.es/opinion/articulos/derecho-olvido_0_807219443.html

hecho de poseer antecedentes penales puede comportar importantes consecuencias para el futuro laboral de la persona y para el ejercicio de sus derechos cívicos o familiares, constituyendo una "pena invisible" que debe sumarse a la pena impuesta[431].

En la normativa española actual, las personas condenadas por la comisión de delitos y que han extinguido la responsabilidad penal, cuando haya transcurrido un determinado plazo sin haber vuelto a delinquir, y una vez satisfecha su responsabilidad civil, tienen derecho a obtener del Ministerio de Justicia, de oficio o a instancia de parte, la cancelación de sus antecedentes penales[432]. Asimismo, aunque no se haya llevado a cabo la cancelación, los jueces y tribunales no tendrán en cuenta dichos antecedentes a la hora de apreciar la agravante de reincidencia[433]. Por tanto, los antecedentes penales no pueden desplegar sus efectos *sine die.* Estas previsiones legislativas son una garantía del derecho al olvido frente a los poderes públicos en el ejercicio del *ius puniendi*.

---

[431] JACOBS, J. B. y LARRAURI, E.: "¿Son las sentencias públicas? ¿Son los antecedentes penales privados? Una comparación de la cultura jurídica de Estados Unidos y España", *Indret,* 2010, pág. 3. Como recuerda Muñoz Conde en el prólogo a un libro de Grosso Galván: " 'A nadie le gusta llevar su pasado escrito en la frente', dice uno de los personajes de un film de John Ford, menos que a nadie al delincuente, porque ello, además lo marca como a una res, lo distingue y lo aparta, a veces como a un apestado, de los demás miembros de la comunidad", en GROSSO GALVÁN, M.: *Los antecedentes penales: rehabilitación y control social*, Bosch, Barcelona, 1983.

[432] Artículo 136 Código Penal.

[433] *Vid.* también artículo 19 del Real Decreto 95/2009 de 6 de febrero, sobre el sistema de registros administrativos de apoyo a la Administración de justicia. Los antecedentes penales, a diferencia de los antecedentes policiales, sí son tenidos en cuenta por el Juez en los juicios penales celebrados contra el afectado por la comisión posterior de otro delito, e influyen en la tramitación de otros procedimientos como puede ser la solicitud de la nacionalidad.

Los antecedentes penales o antecedentes judiciales son datos personales de los sujetos condenados por sentencia judicial firme, que están recogidos en el Registro Central de Penados y Rebeldes[434].

Dado que los datos obrantes en este registro son especialmente sensibles, no es un registro público al que cualquier persona pueda acudir a consultar tal información y existe una especial protección, de forma que solo el interesado o los órganos judiciales, el Ministerio Fiscal y la policía judicial, así como determinados miembros de las Fuerzas y Cuerpos de Seguridad del

[434] Sobre la evolución de la marca penal, física en un primer momento y a través de los antecedentes después, *vid.* GROSSO GALVÁN, M.: *op. cit.*, págs. 14-16. El Registro Central de Penados y Rebeldes se regula por el Real Decreto 95/2009, de 6 de febrero, sobre el sistema de registros administrativos de apoyo a la Administración de justicia. Conforme al artículo 8 de este Real Decreto, la información de carácter general contenida en los Registros integrados en el sistema abarcará los siguientes datos: a) datos identificativos b) Órgano judicial que acuerda la resolución c) Los datos personales identificativos de la víctima, d) la condición de menor de edad de la víctima cuando se trate de delitos contra la libertad e indemnidad sexuales. El artículo 9 del Real Decreto regula la información contenida en la inscripción de sentencias firmes: "Cuando se trate de sentencias firmes que impongan penas o medidas de seguridad a personas físicas mayores de edad, penas a personas jurídicas o consecuencias accesorias a entes sin personalidad se inscribirán, además, los siguientes datos: a) Fecha de la sentencia que imponga la pena o medida de seguridad. b) Fecha de firmeza de la sentencia y fecha de efectos del requerimiento del cumplimiento. c) Órgano judicial sentenciador. d) Condición de reincidente y/o reo habitual del condenado en su caso. e) Órgano judicial de ejecución de la sentencia, en su caso. f) Número y año de la ejecutoria. g) Delito o delitos y precepto penal aplicado. h) Pena o penas principales y accesorias, medida de seguridad y su duración y cuantía de la multa con referencia a su duración y cuota diaria o multa proporcional. i) Fecha de comisión del delito. j) Participación como autor o cómplice y grado de ejecución. k) Sustitución de las penas o medidas de seguridad, en su caso. l) Suspensión de la ejecución de las penas o medidas de seguridad, en su caso, fecha de notificación, así como plazo por el que se concede la suspensión. m) Prórroga del auto de suspensión de las penas. n) Fecha de la revocación del auto de suspensión de las penas o medidas de seguridad. ñ) Fecha de la remisión definitiva de la pena, cumplimiento efectivo de la misma o prescripción. o) Fecha del cese de la medida de seguridad. p) Expulsión y fecha de la misma, cuando se acuerde como sustitución de la pena o medida de seguridad. q) Cumplimiento. r) Acumulación de penas. s) Responsabilidad civil derivada de la infracción penal. t) Resoluciones judiciales que se pronuncien sobre el traslado de la pena de acuerdo con el artículo 130.2 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal". Conforme al artículo 2.3.d) de la LOPD, los tratamientos de datos personales derivados del Registro Civil y del Registro Central de penados y rebeldes, se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta LOPD. En concreto por las normas de seguridad y conforme al artículo 26 Real Decreto 95/2009 sobre el sistema de registros administrativos de apoyo a la Administración de justicia: "De conformidad con lo dispuesto en el artículo 18.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, los interesados podrán recabar la tutela de la Agencia Española de Protección de Datos en relación con el ejercicio de sus derechos de acceso, rectificación o cancelación".

Estado, pueden consultar los datos registrados[435]. Tampoco serán públicos los antecedentes una vez cancelados porque solo tendrán acceso a los mismos los jueces y tribunales españoles y cuando resulten necesarios para la elaboración de estadísticas[436].

Esta regulación es una manifestación del artículo 25.2 CE, que establece el principio constitucional general relativo a la orientación de las penas, según el cual "las penas privativas de libertad y las medidas de seguridad estarán orientadas hacia la reeducación y la reinserción social". Así, el Tribunal Constitucional en su sentencia 174/1996[437], declaró que "no han de perpetuarse en el tiempo los efectos de conductas pasadas que ya no existen para el mundo del Derecho. Si, como es el caso, quien fuera condenado otrora ha obtenido la rehabilitación,… rehabilitación que extingue de modo definitivo todos los efectos de la pena (…), no se puede tomar en consideración su condena (…). Otra solución chocaría frontalmente con el artículo 25.2 CE. y con la orientación que atribuye a las penas, cuya finalidad trascendente es la reinserción social"[438]. Lo cual confirma el carácter reservado de los antecedentes penales.

---

[435] Así, las unidades de Intervención de Armas y Explosivos de la Guardia Civil o las unidades del Cuerpo Nacional de Policía responsables. *Vid*. Artículos 5, 6 y 7 del Real Decreto 95/2009, sobre el sistema de registros administrativos de apoyo a la Administración de justicia.

[436] Artículo 25 del Real Decreto 95/2009, sobre el sistema de registros administrativos de apoyo a la Administración de justicia. En el ámbito de la cooperación judicial en la Unión Europea téngase en cuenta la Ley Orgánica 7/2014, de 12 de noviembre de intercambio de información de antecedentes penales y consideración de resoluciones judiciales penales en la Unión Europea.

[437] STC 174/1996, FJ 3.

[438] Sobre la idea de reinserción social, el artículo 73 de la Ley Orgánica General Penitenciaria dispone: "1. El condenado que haya cumplido su pena y el que de algún otro modo haya extinguido su responsabilidad penal deben ser plenamente reintegrados en el ejercicio de sus derechos como ciudadanos. 2. Los antecedentes no podrán ser en ningún caso motivo de discriminación social o jurídica." *Vid*. LUZÓN CANOVAS, M.: "Antecedentes Penales", pág. 23, disponible en Internet: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga

Del mismo modo, la normativa sobre los antecedentes penales se inspira en la protección de los derechos fundamentales a la intimidad y a la protección de datos personales, que encuentra su fundamento en el respeto a la dignidad humana, el libre desarrollo de la personalidad y en la reinserción social[439]. Nuestro Tribunal Constitucional constata, así, la confidencialidad de los antecedentes penales en la STC 144/1999, al afirmar que "la información relativa a un aspecto tan sensible de la vida de un individuo como son sus antecedentes penales, que indudablemente afectan a su integridad moral, debe estar a recaudo de una publicidad indebida y no consentida por el afectado, y, aun en el caso de que una norma de rango legal autorice a determinados sujetos el acceso a la misma, con o sin el consentimiento del afectado, ese acceso solo está justificado si responde a alguna de las finalidades que explican la existencia del archivo o registro en el que estén contenidas; fines que deberán coincidir con alguna de las limitaciones constitucionalmente impuestas a la esfera íntima del individuo y su familia. Así pues, si el acceso no se realiza con estricta observancia de las normas que lo regulan, se vulnera el derecho a la intimidad. Y se vulnera ese derecho en la medida en que aquel archivo o registro se puede convertir en una fuente de información sobre la vida de una persona o su familia, menoscabando la confidencialidad de esa información" (FJ 8).

En esta sentencia, el Tribunal Constitucional examina el régimen de los antecedentes penales a propósito de un recurso de amparo contra actos de la

---

/Ponencia%20Luz%C3%B3n%20C%C3%A1novas,%20Mar%C3%ADa.pdf?idFile=2ab36b02-6023-49a0-bd19-8fb338837685

[439] En cuanto al impacto en otros derechos fundamentales *vid,* sobre el principio de igualdad la STEDH de 7 de noviembre de 2013, caso E.B. y otros contra Austria.

Administración Pública que tuvieron lugar durante un proceso electoral. El recurrente había sido condenado, como autor de un delito de injurias graves, a la pena de un mes y un día de arresto mayor, con la accesoria de suspensión del derecho de sufragio durante el tiempo de la pena principal. Confirmada la sentencia en casación, la condena le fue notificada cuando ya había sido proclamado candidato para las elecciones locales y autonómicas. El ofendido por las injurias instó a la Junta Electoral a que lo declarara inelegible. Esta, previa obtención de los datos del Registro Central de Penados y Rebeldes, lo excluyó como candidato.

El recurso de amparo se fundamentaba, entre otros preceptos, en la vulneración del artículo 18.1 CE, pues la Junta Electoral de Zona había obtenido la información del Registro Central de Penados y Rebeldes, es decir, fuera de los cauces establecidos, tratándose de un archivo cuyo acceso estaba restringido a quien no fuera el propio interesado o la jurisdicción penal. Lo interesante de esta resolución estriba en que, a pesar de que se resuelve sobre la base de una concepción subjetiva del derecho a la intimidad, reconoce que nos encontramos ante un tratamiento automatizado de una categoría especial de datos sometido a fuertes limitaciones, "que obligan a una interpretación restrictiva y rigurosa de los términos en los que esa información puede divulgarse o transmitirse, incluso (y quizá, sobre todo) entre distintos órganos del Estado"[440].

[440] Como señala Álvarez-Cienfuegos, "la definición de lo que constituye 'la intimidad personal y familiar' se nos revela cada vez más amplia y más precisa, más rica de contenido y más próxima al ciudadano, amparando esferas de la personalidad hasta ahora desconocidas. Nace, por tanto, una nueva sensibilidad hacia espacios de la intimidad que aparecen vedados para la curiosidad ajena y reservados a lo que configura la construcción de la propia vida privada". *Vid.* ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M.: "El registro de penados y rebeldes y la intimidad de

A tal efecto, el Tribunal Constitucional se remite, por la vía de la interpretación de los derechos fundamentales (art.10.2 CE), al artículo 6 del Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, de 28 de enero de 1981, que dispone que "los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condena penales"[441].

Llevando a cabo una actualización de la normativa anterior, la LOPD preceptúa que los datos de carácter personal relativos a la comisión de infracciones penales o administrativas solo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras[442]. Y el artículo 10 del Reglamento General de Protección de datos reitera que solo podrá llevarse a cabo el tratamiento de esta clase de datos bajo la supervisión de las autoridades públicas o cuando lo

---

los ciudadanos (Comentario a la sentencia 144/1999, de 22 de julio", *Actualidad Jurídica Aranzadi*, núm. 409, 1999.

[441] Y en términos similares se pronuncia el artículo 8.5 de la Directiva 95/46/CE : "El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, solo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, solo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos."

[442] Artículo 7.5 LOPD. Por su parte, el artículo 22.2 LOPD dispone: "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad". *Vid*. artículo 10 del Proyecto de Ley Orgánica de 24 de noviembre de 2017 sobre el tratamiento de datos de naturaleza penal.

autorice el Derecho de la Unión o de los Estados miembros y siempre con las garantías adecuadas para los derechos y libertades de los interesados. El registro completo de condenas penales, en concreto, solo podrá llevarse bajo el control de las autoridades públicas.

Desde la perspectiva del derecho fundamental a la protección de datos, el análisis llevado a cabo por el Tribunal Constitucional en esta sentencia se centra en el carácter confidencial de los datos, pero se tienen en cuenta algunos de los principios inspiradores de la autodeterminación informativa. Así, se resolvió, evidentemente, una cuestión de procedimiento, esto es, que la petición por teléfono del historial penal del recurrente de amparo por el Presidente de la Junta Electoral y su remisión por fax por el Registro de Penados y Rebeldes, sobre quien pesa el deber inexcusable de proteger la confidencialidad de la información contenida en él, se hizo al margen de lo que establece la normativa. En efecto, las certificaciones de antecedentes penales solo pueden solicitarse por el interesado o por los órganos judiciales u otros poderes públicos cuando así lo disponga una norma con rango legal, dada la naturaleza de los datos contenidos en el referido Registro[443].

En definitiva, lo que subyace en el supuesto resuelto por el Tribunal Constitucional es una cesión de datos sensibles entre Administraciones Publicas, al haberse dispuesto de los datos obrantes en el Registro de Penados y Rebeldes sobre el demandante de amparo sin su conocimiento, ni su consentimiento. En tal sentido, el principio de calidad de los datos adquiere relevancia y el acceso a la información debe estar sometido "al estricto

[443] En la actualidad, los artículos 16 y 17 del Real Decreto 95/2009 de 6 de febrero, sobre el sistema de registros administrativos de apoyo a la Administración de justicia.

escrutinio del fin que lo legitime, que no puede ser otro que la realización efectiva de los límites constitucionales al derecho a la intimidad del artículo 18.1 CE". Siendo el acceso por un poder público a la hoja histórica penal de un ciudadano una limitación de su derecho a la intimidad, no solo es del todo inexcusable que una Ley lo permita, sino que, además, esa Ley debe establecer explícitamente tanto el límite de que se trate cuanto los términos en los que ese límite puede hacerse valer, y lo cierto es que ninguna normativa atribuía tal competencia a la Junta Electoral de Zona[444].

A mayor abundamiento, el propósito de la obtención del historial penal por parte de la Junta Electoral, a juicio del Tribunal Constitucional, era inadecuado porque no se podía justificar con el pretexto de velar por la "pulcritud" del proceso electoral, y a la vez resultaba innecesario, pues la causa de la incapacidad electoral del recurrente en amparo debía buscarse en la sentencia firme condenatoria, por lo que hubiera bastado con el testimonio de la ejecutoria para hacer valer la suspensión del derecho de sufragio. Por consiguiente, la finalidad pretendida no superaba, en la ponderación con el derecho a la protección de datos como garante de la intimidad, los dos primeros requisitos establecidos por el principio de proporcionalidad.

En cualquier caso, a título anecdótico, la estimación parcial del recurso de amparo por la vulneración del derecho a la intimidad en este caso no supuso la alteración de los resultados electorales, como pretendía el recurrente.

---

[444] "Aun cuando su presidente sea un juez, este (…) al solicitar dicha hoja a aquel Registro, en modo alguno actúa en el ejercicio de sus funciones jurisdiccionales y al eventual amparo del artículo 118 C.P. (de 1973), pues en ese caso obra únicamente como Presidente de un órgano administrativo como lo es la Junta Electoral (STC 197/1988), al que ninguna norma habilita para acceder a aquella información. Si esto es así, la Junta Electoral de Zona habría infringido el artículo 18.1, en relación con su apartado 4º, CE" (STC 144/1999, FJ 8).

Sobre la base de las consideraciones anteriores, el hecho de que el Registro de Penados y Rebeldes no sea público no implica que no se puedan divulgar los antecedentes penales, pues a esta información se puede llegar por otros medios, como, por ejemplo, la publicidad procesal. En este sentido, en ocasiones la difusión de la información sobre los antecedentes penales se traduce en un conflicto entre el derecho al honor, a la intimidad y a la protección de datos personales del afectado y el principio de transparencia judicial y las libertades informativas, como ocurrió en el caso objeto de la STC 46/2002.

El litigio se remonta a octubre de 1990, a propósito de la publicación de un artículo en la sección de Tribunales del diario El País, bajo el título: "Los escritos anónimos no pueden considerarse falsos", donde el periodista se hacía eco de una sentencia del Tribunal Supremo que absolvía al demandante de amparo de un delito continuado de falsedad en documento privado, por el que había sido condenado por la Audiencia Provincial. El recurso de amparo se fundamentaba en la vulneración de los derechos fundamentales al honor y a la intimidad (art. 18.1 CE), pues se mencionaban el nombre y los apellidos del demandado junto al comentario de que "tenía antecedentes penales por hurto y en el caso de haber sido condenado, hubiese tenido que ingresar en prisión".

Para el recurrente en amparo, la revelación de los antecedentes penales, en este caso, contribuía únicamente a su descrédito, resultando además, que aquellos se encontraban ya cancelados, e, incluso aunque no lo hubiesen estado, carecía de relevancia pública. Sin poner en duda que la sentencia del Tribunal Supremo tuviera carácter noticiable, al establecer una

doctrina novedosa en relación con un tipo penal, esto no era igualmente predicable de la persona que resultaba afectada por la información.

La sentencia del Tribunal Constitucional recoge en el fundamento jurídico quinto la doctrina, antes expuesta, sobre la confidencialidad de esta clase de datos, en el sentido de que la divulgación de los antecedentes penales de una persona puede constituir una intromisión ilegítima en el derecho al honor del afectado, e, incluso, que la información relativa a un aspecto tan sensible de la vida de un individuo, según las circunstancias de esa información, puede llegar a lesionar su intimidad en la medida en que puedan convertirse en una fuente de información sobre su vida privada o la de su familia. No obstante, no se hace ninguna referencia al derecho fundamental a la protección de datos personales.

De hecho, el núcleo de la argumentación del Tribunal Constitucional gira en torno a si el ejercicio de las libertades informativas, en este supuesto, cumple con los requisitos de veracidad e interés público de la información.

El Tribunal Constitucional advierte que el objeto del artículo era la información sobre una concreta sentencia del Tribunal Supremo. Según su criterio, la difusión de una sentencia puede suponer por su propio contenido un desprestigio en la consideración de la persona afectada por la información. Ello obliga a comprobar si el medio de comunicación actuó con la debida diligencia, en su máxima intensidad. El dato de que el recurrente de amparo tenía antecedentes penales por hurto resulta del texto de la sentencia. Y aunque es cierto que tal información era inexacta, pues los antecedentes estaban ya cancelados, no podía exigírsele mayor diligencia al periodista, tratándose además de un dato que no cabía calificar de superfluo, porque terminaba por

perfilar los efectos que la sentencia del Tribunal Supremo habría de producir y que no se produjeron debido a su carácter absolutorio.

En relación con el interés público de la información, el Tribunal Constitucional parte de que lo que se difunde es un dato que ya se ha hecho público por las sentencias de las que procede y descarta que la publicación de algo que es oficialmente público pudiera afectar a la intimidad o constituir cualquier otra clase de injerencia ilegítima. Adicionalmente, para el Tribunal Constitucional, la información sobre los antecedentes penales del demandante, servía a un fin informativo lícito, como es, el de resaltar los efectos de la sentencia en ese caso concreto, en contraste con lo que en él hubiera podido significar un fallo condenatorio, y, consecuentemente, completar la información sobre dicha resolución, con lo que, a juicio del Tribunal Constitucional, no podía negarse su trascendencia pública.

A la vista de este pronunciamiento es preciso hacer algunas consideraciones. En primer término, se diferencia acertadamente en el fundamento cuarto de la sentencia, en el conjunto de la información difundida, cuál es el derecho ejercido por el autor de la noticia controvertida. En el artículo en sí, al limitarse este a informar sobre el contenido de la sentencia del Tribunal Supremo, transcribiendo literalmente alguno de sus pasajes esenciales, así como a exponer los hechos que desencadenaron el proceso penal en el que aquélla recayó, sin añadir juicios de valor, su contenido habría de enmarcarse en el ejercicio del derecho a comunicar libremente información del artículo 20.1.d) CE. Sin embargo, en relación con el comentario que se desliza en el artículo periodístico sobre las consecuencias que se hubieran podido derivar para el demandante de amparo de sus antecedentes penales por hurto, si no

hubiera sido absolutoria la sentencia del Tribunal Supremo, el Tribunal Constitucional entiende que, al emitirlo, no se relata un hecho, sino que se expresa una opinión sobre lo que hubiera pasado de haber sido condenatoria la sentencia que se comenta. Tal opinión, a juicio del Tribunal Constitucional, "por más que pueda resultar inexacta, carece de toda virtualidad lesiva, tanto desde la perspectiva del honor como de la intimidad: ni constituye una injuria ni, al no relatar hecho alguno, desvela nada que pudiera pertenecer a la esfera íntima". Como resultado, el recurso de amparo se resuelve sobre la base del conflicto entre los derechos al honor y a la intimidad frente a la libertad de información.

En segundo término, el Tribunal Constitucional recuerda que en el citado conflicto, para que la libertad de información pueda prevalecer sobre los citados derechos, la información tiene que ser veraz y noticiable, es decir, relevante para la formación de la opinión pública. El primer requisito parece haber quedado acreditado al haber desplegado el profesional de la información la diligencia debida y al tratarse de una fuente de información fidedigna, como lo es una sentencia del Tribunal Supremo.

Es en lo que afecta al carácter noticioso de la información donde la argumentación del Tribunal no resulta convincente, en el sentido de que no tiene en cuenta su propia doctrina acerca del carácter sensible de la información sobre los antecedentes penales de una persona, que obligaría a una interpretación restrictiva y rigurosa de los términos en los que esa información puede divulgarse. A ello cabe añadir que tampoco se tiene en cuenta la condición de persona privada del demandante de amparo.

Para completar estas observaciones, conviene tener en cuenta que, si bien el Tribunal Constitucional se remite a la STC 144/1999, no hay ninguna

referencia expresa al derecho fundamental a la protección de datos en esta resolución. Desde esta perspectiva, creo que hubiera encajado mejor la pretensión del demandante de amparo en el sentido de haber enfocado el recurso hacía el tratamiento de datos personales hecho por un profesional de la información. Conviene recordar que dato personal es cualquier información concerniente a personas físicas identificadas o identificables. El derecho fundamental a la protección de datos protege también los datos públicos.

En fin, la información publicada, a nuestro juicio, carecía de relevancia pública por tratarse de un dato sensible, relativo a una persona privada, empleado para fines distintos de aquel que legitimó su obtención. El tratamiento de datos, que era inicialmente lícito no obstante el transcurso del tiempo (habían transcurrido más de 10 años desde que ocurrieron los hechos) hace en este caso que los datos sean inadecuados, no pertinentes o excesivos en relación con la finalidad informativa para la que se han empleado, pues ofrecían un perfil de la persona que, además, afectaba a su reputación. De hecho, a nuestro juicio, habría procedido ejercer el derecho de oposición respecto al periódico.

La sentencia del Tribunal Constitucional parte del principio de que el artículo periodístico era una plasmación objetiva de una resolución judicial previa, que gozaba del principio de publicidad ex artículo 120 CE. Sin embargo el empleo de los datos personales (el nombre y apellidos, ya que por entonces no se usaba la anonimización) y su conexión con los antecedentes penales con el objeto de informar al público de que el delito de falsedad en documento privado mediante anónimos podría haber implicado la pena de prisión resulta

desproporcionado en relación con el derecho fundamental a la protección de datos del afectado porque perjudica su reputación.

Para el diario El País, defendiendo que la información gozaba de interés público, el interesado podría haber ejercitado contra el medio de comunicación el derecho de rectificación al tratarse de un dato inexacto, cosa que no hizo. Este modo de proceder me parece lógico porque el derecho de rectificación supone la posibilidad que tiene el aludido por una información que considere errónea de corregirla, difundiendo en el mismo espacio su versión de los hechos. En este caso, el mencionado rechazaba la divulgación de su pasado penal porque le perjudicaba, por lo tanto no iba a colaborar aún más en difundirlo. En fin, el tema no era si el dato era o no exacto, sino si el dato en sí, vistas las circunstancias del caso, era susceptible de ser publicado.

No es esta la única ocasión en que el Tribunal Constitucional analiza el conflicto entre los derechos al honor y a la intimidad y las libertades informativas al hilo de la divulgación de antecedentes penales. Así, la STC 52/2002 se refiere a un caso en el que el Tribunal Constitucional, al contrario del supuesto anterior, hizo prevalecer el derecho al honor. En el asunto, el diario Las Palmas daba cuenta de una información sobre las investigaciones llevadas a cabo por las Fuerzas y Cuerpos de Seguridad del Estado para determinar la identidad del sospechoso que había dado muerte a dos tripulantes del ferry “Ciudad de Palma”, indicando que dos de las tres personas que habían sido objeto principalmente de las pesquisas iniciales habían sido descartadas. En el texto de la noticia se dedicaban los dos primeros párrafos al interesado en el proceso, descartándose su participación en los mencionados acontecimientos, y, concretamente en el segundo, se afirmaba “que tiene

antecedentes penales por una violación acaecida hace 12 años, habiendo sido objeto en otra ocasión de un arresto menor". La Sala de lo Civil del Tribunal Supremo consideró en su sentencia, frente al criterio mantenido por la Audiencia Provincial y el Juzgado de Primera Instancia, que la divulgación de tales datos, al margen de su no veracidad, suponía una intromisión ilegítima en el honor del afectado[445].

Los demandantes de amparo —la periodista autora de la información controvertida, el director del medio de comunicación y la empresa editora— invocaron frente a la resolución judicial impugnada la vulneración del derecho a comunicar libremente información, al entender que un texto periodístico ha de ser considerado en su conjunto, destacándose que en el artículo había sido descartada la participación del afectado en el doble crimen, de modo que, lejos de ser lesiva para su honor, el núcleo de la información había servido para eliminar la sombra que gravitaba sobre la reputación del afectado.

Argumentaban, además, que en el presente caso no hubo vejación, injuria o insulto, sino, solamente, revelación de antecedentes penales y policiales, tomados de una fuente de máxima fiabilidad, como era la Jefatura Superior de Policía. Aun cuando se admitía que la autora de la información había incurrido en confusión entre antecedentes penales y policiales[446], a su juicio, no podía imputársele menosprecio por la verdad o falsedad de lo comunicado, como consecuencia de la confusión en la que incurrió, ni tacharse de innecesaria la divulgación de aquellos antecedentes, que no tenía un

---

[445] La condena de la Sala Civil del Tribunal Supremo se basaba en que la divulgación de la información sobre los antecedentes penales del demandante en el proceso *a quo*, por una violación acaecida hace doce años, era innecesaria.

[446] La Jefatura Superior de Policía certificó, no que tuviera antecedentes penales, sino que había sido puesto a disposición judicial.

propósito difamatorio, y constituía una referencia accesoria, que dejaba indemne el contenido esencial de la información.

Frente a esta postura, el afectado consideró que la atribución de antecedentes penales implicaba por sí misma la condena mediante sentencia firme por la comisión de hechos delictivos, circunstancia que no debía difundirse, por los perjuicios que socialmente representaba, máxime si no eran ciertos dichos antecedentes[447] y su publicación carecía de relevancia pública. Para aquel, la divulgación de este dato no solo resultaba innecesaria, sino que tenía la virtualidad de que, al mismo tiempo que lo colocaba fuera de toda sospecha, lo convertía inmediatamente en culpable de un delito de violación. Por su parte el Ministerio Fiscal se opuso también a la pretensión de los demandantes de amparo por la falta de relevancia pública del artículo periodístico, porque no solo divulgaba la identidad de una persona, cuya participación en la comisión del delito había sido descartada, sino que además proporcionaba datos sobre la misma, como el de tener antecedentes penales y haber estado sujeto al cumplimiento de una pena de arresto mayor, que, con independencia de su veracidad, se pueden considerar socialmente denigrantes.

El Tribunal Constitucional vuelve a reiterar aquí su doctrina según la cual la divulgación de los antecedentes penales de una persona puede dañar la reputación del afectado por la información, en cuanto conlleva un desmerecimiento en la consideración ajena, quedando de este modo menoscabado su honor, y paralelamente puede llegar a lesionar su intimidad,

[447] Lo cual se acredita con la certificación del Registro Central de Penados y Rebeldes que se acompaña a las alegaciones, así como testimonio emitido por el Juzgado de procedencia del sobreseimiento definitivo de su inculpación por un presunto delito de violación.

en la medida en que puede convertirse en una fuente de información sobre la vida privada de una persona o su familia.

A la vista de las circunstancias concurrentes en este caso, recuerda el máximo intérprete de la Constitución que el requisito de que la información publicada sea veraz para encontrar cobertura en el ejercicio del derecho a comunicar libremente información no supone la exigencia de una rigurosa y total exactitud en el contenido de la información. Para poder apreciar si la diligencia empleada por el informador es suficiente, a efectos de entender cumplido el requisito constitucional de la veracidad, deben tenerse en cuenta diversos criterios. En primer lugar, el nivel de diligencia exigible adquiere su máxima intensidad cuando la noticia que se divulga puede suponer por su propio contenido un descrédito en la consideración de la persona a la que la información se refiere. De igual modo deben ser criterios que deben ponderarse, el respeto a la presunción de inocencia, la trascendencia de la información, la condición pública o privada de la persona cuyo honor queda afectado o cuál sea el objeto de la información, es decir, si el medio asume los hechos divulgados como propios o son la transmisión neutra de manifestaciones de otro. Finalmente, otras circunstancias pueden contribuir a perfilar el comportamiento debido del informador en la búsqueda de la verdad, como el carácter noticioso de los hechos, la fuente de la noticia y las posibilidades efectivas de contrastarla. Apreciada, por todo ello, la falta de veracidad de la información, el Tribunal Constitucional se centra posteriormente en la cuestión de la relevancia pública de la noticia.

A diferencia del recurso de amparo resuelto por la STC 46/2002, en este supuesto el Tribunal pone de manifiesto que el articulo era el resultado de una

elaboración propia de la periodista autora del mismo, no un reflejo objetivo del texto de una resolución judicial. Lo narrado sobre los antecedentes penales era innecesario en relación con la finalidad informativa sobre los sucesos en que pudo verse implicado el afectado[448], máxime si se tiene en cuenta la profunda afectación que la divulgación de tales datos habría de suponer para el honor y la consideración social de la persona afectada.

Esta solución es, en nuestra opinión, congruente con la consideración de los antecedentes penales como datos sensibles aunque la sentencia no trata del derecho fundamental a la protección de datos personales. Este derecho debió prevalecer en este caso sobre la libertad de información porque los datos eran innecesarios o superfluos para los fines para los que se emplearon. No se puede exigir a una persona que no ostente la consideración de personaje público que soporte la revelación de datos personales que puedan desacreditarla, más aún cuando ha transcurrido un lapso de tiempo considerable desde la comisión de los hechos.

Frente a esta línea jurisprudencial que tiene en cuenta la confidencialidad de los antecedentes penales, la publicidad de estos se concibe en algunos Estados[449] como un medio de prevención de los delitos y de alertar

---

[448] La finalidad informativa del motivo por el que la policía había inicialmente investigado al afectado no queda demostrada según el Tribunal Constitucional, ya que en ningún momento se conectan los supuestos antecedentes penales con el hecho de que, entre otras personas, se centrasen en aquel en un principio las pesquisas policiales, ni en la noticia se aportan datos sobre tal conexión, siendo, por el contrario, su condición de indigente y sus características personales, supuestamente comunes a las del autor de las muertes a bordo del ferry, el motivo por el que fue inicialmente una de las personas investigadas, como se desprende tanto del titular de la información dedicado al demandado en el proceso *a quo* como del texto de la noticia (STC 46/2002, FJ 8).

[449] Sobre la cultura jurídica del *Common Law* en Estados Unidos y en el Reino Unido, *vid.* SIMÓN CASTELLANO, P.: *El reconocimiento del olvido digital*…, *op. cit.*, págs. 112-116. También en relación con Estados Unidos *vid.* JACOBS, J. B. y LARRAURI, E.: "¿Son las sentencias públicas?..., *op. cit.*, 2010.

a las personas físicas y jurídicas de los riesgos de una posible reincidencia. Como se puede suponer, para los potenciales delincuentes, el hecho de saber que serán rechazados y que se les negarán oportunidades de trabajo, podría disuadirlos de cometer ilícitos. Del mismo modo, la opinión pública apoya estas medidas, en relación con determinados delitos, pues se considera que pueden ser útiles o pueden contribuir a la seguridad pública[450]. En España, los antecedentes penales se solicitan en ocasiones por diversos organismos públicos y privados como requisito para poder presentarse a oposiciones, contratos laborales, para la solicitud de visados o la concesión de licencias o para el acceso y ejercicio de determinadas profesiones y actividades, especialmente cuando implican el contacto habitual con menores[451].

El tema del impacto que sobre los derechos fundamentales pueda tener la publicidad de los antecedentes penales planteó el debate sobre la constitucionalidad de la Ley de Castilla-La Mancha 5/2001, de 17 de mayo, de Prevención de Malos Tratos y de Protección a las Mujeres Maltratadas[452], que, en su artículo 11.d) prevé que el Gobierno de esta Comunidad remita a las Cortes de dicha Comunidad Autónoma, al menos con carácter anual, un informe en el que preceptivamente se contengan los procedimientos penales iniciados sobre violencia doméstica con indicación de su número, la clase de procedimiento penal, el delito o falta imputado y la intervención de la

[450] Registro Central para la protección de las víctimas de la violencia doméstica. Real Decreto 513/2005, de 9 de mayo.

[451] Real Decreto 1110/2015, de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales. Recoge los datos relativos a la identidad y perfil genético (ADN) de las personas condenadas por los delitos objeto del mismo.

[452] Sobre las críticas a la ley *vid.* JACOBS, J. B. y LARRAURI, E.:“ Son las sentencias públicas…", *op. cit.,* pág. 18, nota 57. También la prensa se hizo eco de la polémica ley: Disponible en Internet: https://elpais.com/diario/2001/05/18/sociedad/990136807_850215.html http://www.abc.es/hemeroteca/historico-17-05-2001/abc/Ultima/castilla-la-mancha-aprobo-una-ley-sobre-violencia-domestica-que-incluye-la-publicidad-de-las-sentencias_31444.html

Administración regional en dichos procedimientos, así como la reproducción de las sentencias condenatorias firmes sobre violencia doméstica cuando se cuente con el consentimiento de la víctima, y en el caso de que esta no pudiere prestarlo, con el consentimiento de las personas perjudicadas.

El propósito de divulgar las sentencias firmes en este tipo de delitos, según se desprende de la exposición de motivos de esta ley, es que la acción de la justicia contribuya a crear un clima social de rechazo a la violencia doméstica que se combate. Pero, además, "los poderes públicos son responsables de que no se arroje un manto de silencio sobre el crimen para que no se juzgue, o sobre la propia condena para que no se conozca". Para salvar el conflicto entre esta norma y el derecho fundamental a la protección de datos personales, la Ley prevé en su Disposición adicional única que "los datos personales de todo tipo que figuren en el Informe al que se refiere el artículo 11 de esta Ley no podrán ser incluidos en fichero, ni ser tratados, ni cedidos en los términos que para estos conceptos establece el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, cuyos preceptos deberán ser siempre respetados en aplicación de esta Ley"[453].

El primer Informe presentado por el Gobierno a las Cortes de la Comunidad de Castilla la Mancha incluía 18 de las 41 sentencias condenatorias firmes dictadas entre mayo y diciembre del 2001[454]. La Agencia Española de Protección de Datos archivó el expediente sancionador al considerar que la publicación de estas sentencias se hacía en un soporte físico

[453] En similares términos se pronuncia el artículo 15.2 de la Ley de Violencia de Genero de Cantabria.
[454] https://elpais.com/diario/2002/05/29/sociedad/1022623205_850215.html

no susceptible de tratamiento automatizado posterior y, por lo tanto, quedaba al margen de la LOPD[455].

En otros casos la publicidad de las condenas penales ha buscado respaldo en la libertad de información o en la necesidad de dar a conocer al público en general la actividad en la lucha contra la tortura y otros tratos vejatorios de la dignidad humana. En tales términos se pronunció la Sentencia del Tribunal Supremo de 26 de junio de 2008[456], en torno a la difusión en la página web de la Asociación contra la tortura de un listado de nombres de policías, guardias civiles y políticos implicados en actuaciones relativas a torturas, adjuntándose, junto al nombre del funcionario, su situación en relación con la denuncia por tortura (investigación, condenado, absuelto), el lugar de los hechos, la fecha y la identificación del caso. La Asociación, que tenía por objeto la denuncia ante la opinión pública y Tribunales de los casos de maltrato, vejaciones o tortura, obtenía los datos, bien de los propios órganos jurisdiccionales que les facilitaban las sentencias a petición de la Asociación, o bien del hecho de ser la Asociación acusación particular en algunos juicios.

En el caso examinado, el Director de la Policía presentó una queja ante la AEPD por infracción de la LOPD. La AEPD confirmó que la información publicada en la página web constituía un fichero de datos personales, además de que la totalidad de los datos no procedían de fuentes accesibles al público, como lo eran las sentencias penales. Por otra parte, los datos de carácter personal relativos a la comisión de infracciones penales o administrativas, de

[455] ROIG, A.: "Derecho Público y Tecnologías de la información y la comunicación", *Revista catalana de dret public*, núm. 35, 2007, pág. 10. Sobre las resoluciones de la AEPD respecto a la publicidad en una web de las condenas penales, *vid.* JACOBS, J. B. y LARRAURI, E.: *op. cit.*, págs. 18 y 19.

[456] Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de 26 de junio de 2008.

acuerdo con la normativa de protección de datos, solo podían ser incluidos en ficheros de las Administraciones Públicas[457]. Por lo tanto, multó a la Asociación y ordenó retirar tal información de la página web[458].

En relación con los datos extraídos de sentencias y resoluciones judiciales, la Asociación sostenía, básicamente, que las sentencias penales y los medios de comunicación eran de acceso público, y la publicación de la identidad de las personas declaradas culpables de tortura era difusión de datos públicos protegida por la libertad de expresión. La publicación de la lista en la página web, que a su juicio no constituía un tratamiento de datos, era, además, necesaria para la satisfacción de los fines de la Asociación, así como también para el interés general de organismos nacionales e internacionales en la lucha contra la tortura.

El Tribunal Supremo apoyó los argumentos de la AEPD, y señaló que los nombres de los previamente acusados y condenados penalmente son datos personales, pues el derecho fundamental a la protección de datos personales no se refiere solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos, entre los que lógicamente han de considerarse todos los relativos a sometimiento a denuncias o a causas penales cuando aún no ha recaído sentencia debidamente publicada.

Por otra parte, tal como expresa la sentencia, el derecho fundamental a la protección de datos también alcanza a aquellos datos personales públicos, que, por el hecho de serlo, no escapan al poder de disposición del afectado.

---

[457] Artículo 7.5 LOPD.
[458] Resoluciones del Director de la Agencia de Protección de Datos de fecha 4 de septiembre y 3 de octubre de 2000.

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. Expresa la sentencia que "en tal sentido es importante tener en cuenta la trascendencia que en la valoración social se hace de la imputación de conductas delictivas, que dan lugar a los llamados juicios paralelos y que pueden o no terminar en pronunciamientos condenatorios, que sin ninguna duda inciden en la consideración que pueda tenerse de un determinado funcionario público y más si lo que se le imputan son hechos tan execrables como los que pudieran dar lugar a condena por delitos contra los derechos humanos". Por tanto, solo las Administraciones Públicas competentes pueden disponer de un fichero que contenga datos relativos a la comisión de infracciones penales.

La LOPD establece que publicar esta información en una página web, constituye tratamiento de datos, prohibido a no ser que la persona consienta.

Según quedó acreditado en el asunto, la información no provenía de fuentes accesibles al público. De acuerdo con el Tribunal Supremo, "no es que se esté negando su acceso a las sentencias que, efectivamente, son públicas, sino al tratamiento y creación que solo corresponde a las Administraciones públicas". Así pues, aquel no encuentra justificado que, al amparo de la libertad de información, la Asociación pueda llevar a cabo un tratamiento de datos personales que es ilegítimo, pues está reservado a la Administración, confeccionando un fichero para dar publicidad por Internet a datos sensibles de

las personas[459]. Las concretas conductas sancionadas nada tienen que ver ni con la libertad de expresión, ni con el derecho a la información, en relación con la tortura y a la denuncia de tan execrable práctica. Lo que se estaba sancionando en esta resolución era, por un lado un tratamiento de datos contrario a la norma, y, por otro, una cesión de tales datos. Por consiguiente, en modo alguno tales conductas podían estar amparadas en los artículo 20.1.a) y d) y 20. 2 CE, ni la prohibición de su publicación podía reputarse censura previa.

Finalmente, a las reflexiones anteriores también hay que sumar la jurisprudencia del Tribunal Europeo de Derechos Humanos, que ha tomado en consideración los antecedentes penales y su incidencia en el derecho al respeto a la vida privada.

En la sentencia de 4 de diciembre de 2008, caso S y Marper contra Reino Unido, el Tribunal resolvió si la conservación de las huellas dactilares y los datos de ADN de los demandantes, que fueron sospechosos pero no condenados, se justificaba al amparo del artículo 8.2 Convenio Europeo de Derechos Humanos. Los datos fueron almacenados sobre la base de una Ley que autorizaba su conservación ilimitada en el tiempo, si bien el primer demandante había sido absuelto de un delito de robo y la causa por acoso a su pareja del segundo demandado se había archivado definitivamente.

Particularmente preocupante es para el Tribunal Europeo de Derechos Humanos el riesgo de estigmatización[460]. Así, conforme al párrafo 122: "[s]in

[459] Para alcanzar esta conclusión, el Tribunal Supremo se apoya en la STC 144/1999.

[460] En el mismo sentido, por la conservación en los registros policiales de sus huellas dactilares después de ser absuelto del delito de robo de libros, la STEDH de 18 de abril de 2013, asunto MK contra Francia, párrafo 42. Por su parte, la STEDH de 18 de septiembre de 2014, caso

duda la conservación de datos privados sobre los demandantes no equivale a expresar sospechas. Sin embargo, la impresión que tienen los interesados de no ser considerados inocentes se ve reforzada por el hecho de que los datos que les conciernen se conservan indefinidamente, al igual que los relativos a las personas condenadas, mientras que los que afectan a los individuos que no han sido nunca sospechosos de un delito han de ser destruidos". Por ello concluyó el Tribunal Europeo de Derechos Humanos que la conservación de estos datos constituía una lesión desproporcionada del derecho de los demandantes al respeto de su vida privada y no podía considerarse necesaria en una sociedad democrática.

El tema de la especial gravedad de los delitos sexuales contra menores dio lugar a la demanda de un ciudadano ante el Tribunal Europeo de Derechos Humanos contra Francia, relativa a la incorporación de sus datos personales en un registro de condenados por delitos sexuales, tras haber cumplido ya la pena. El Fichero Judicial Nacional automatizado de Autores de Delitos sexuales (FIJAIS), creado en 2004, dependía del Ministerio de Justicia francés. Este registro tenía como fin prevenir la reincidencia en los delitos sexuales, facilitar la identificación de sus autores y localizarlos rápidamente y en todo momento. Para el Tribunal Europeo de Derechos Humanos, en la Sentencia de 17 de diciembre de 2009, caso Bouchacourt contra Francia, la obligación para las personas condenadas por un delito sexual de indicar a la policía su nombre, fecha de nacimiento, domicilio o cambio de dirección, afectaba a su derecho al

---

Brunet contra Francia, a propósito de la solicitud de la eliminación en un registro policial de sospechosos de los datos de un denunciado por malos tratos a su pareja tras quedar el asunto archivado, el Tribunal resolvió que el mantenimiento durante veinte años de tales datos era una medida desproporcionada con el derecho al respeto a la vida privada.

respeto de la vida privada. Además, la conservación de los datos durante un plazo especialmente largo planteaba un problema. No obstante, en el proceso quedó constatado que el demandante tenía la posibilidad de solicitar la cancelación de la inscripción, cuando dejara de producir sus efectos la decisión que la originó. En estas condiciones, el Tribunal estimó que el plazo de conservación de los datos no era desproporcionado respecto a la finalidad que perseguía el registro. En conclusión, estimó que la inscripción en el FIJAIS, tal y como le había sido aplicada al demandante, mantenía un justo equilibrio entre los intereses privados y públicos concurrentes y que el Estado demandado no se había excedido en su margen de apreciación sobre la materia, por lo que no hubo violación del artículo 8 del Convenio.

Pero quizás la resolución que resume mejor la doctrina del Tribunal Europeo de Derechos Humanos sobre la necesidad de olvidar los antecedentes penales sea la STEDH de 13 de noviembre de 2012, asunto MM contra Reino Unido, que plantea la cuestión de si los datos relativos a los antecedentes penales de la demandante almacenados en los registros formaban parte de su "vida privada". La demandante había sido arrestada por secuestro de menores en abril de 2000[461]. La Fiscalía observó que no era exigible en este caso el inicio de un proceso penal pero, en su lugar, se le dio una advertencia policial. Las advertencias de la policía están destinadas a ser utilizadas como una respuesta proporcionada cuando la persona presenta un nivel bajo de delincuencia y ha reconocido el delito. Si bien la advertencia policial no se

[461] En abril de 2000, la novia del hijo de la demandante deseaba irse de Irlanda del Norte con su nieto de diez meses y regresar a Australia a raíz de su separación del hijo de la demandante. Con la intención de forzar a su hijo y su novia a limar sus diferencias y con la esperanza de que su nieto no regresara a Australia, la demandante desapareció con su nieto el 19 de abril del mismo año sin el permiso de los padres. La policía fue avisada y el niño fue devuelto ileso en la mañana del 21 de abril.

clasifica técnicamente como una condena penal, la policía retiene los datos para futuras referencias y los puede tener en cuenta un juez si la persona es condenada por un delito en el futuro.

Seis años más tarde, la demandante recibió una oferta de empleo como trabajadora social y la empresa contactó con el registro de antecedentes penales. Sin embargo, poco después, la empresa retiró la oferta. La demandante reclamó ante el registro de antecedentes penales, el cual le contestó lo siguiente: "En el caso, de que alguien esté de acuerdo con una advertencia policial, está aceptando que ha sido culpable del delito. Esta información está impresa en el formulario que firmó el 17 de noviembre de 2000. Lamentablemente no hay forma de cambiar esto. El plazo de cancelación de la advertencia era de 5 años si el acusado no había sido condenado por ningún otro delito. Sin embargo, tras el asesinato de las colegialas en Soham y el posterior Informe Bichard, la política de cancelación se modificó en relación con todos los casos en que la parte perjudicada es un niño. La política actual es que todas las condenas y advertencias, donde la parte perjudicada es un niño, se mantienen en el sistema de registro de por vida".

En este contexto, los datos en cuestión constituyen "datos personales sensibles" y se identifican como una categoría especial de datos en el marco del Convenio de Protección de Datos del Consejo de Europa. El Tribunal Europeo de Derechos Humanos, subraya que, aunque los datos contenidos en el registro penal son, en cierto sentido, información pública, su almacenamiento sistemático implicaba que se pudieran revelar mucho tiempo después de los hechos, cuando todos, salvo la persona afectada, posiblemente los hubieran olvidado. Así pues, cuando la condena o la medida penal es lejana en el

tiempo, viene a formar parte de la vida privada de una persona, que debe ser respetada[462].

1.2. Indultos.

En el marco de las repercusiones que sobre los derechos de la vida privada tiene el pasado penal, es preciso mencionar la situación de los indultados a los que el Estado exime de cumplir la pena, pero cuyos datos personales nunca se borran del diario oficial en el que, con motivo de la concesión de un indulto, se insertaron. Y es que, según la LOPD, tienen la consideración de fuentes de acceso público, entre otros, los Diarios y los Boletines oficiales[463].

---

[462] STEDH MM contra Reino Unido, de 13 de noviembre de 2012, párrafo 188.

[463] Artículo 3.j LOPD. Por su parte en cuanto a la publicación electrónica, el artículo 11 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos dispone que la publicación de los diarios o boletines oficiales en las sedes electrónicas correspondientes, tendrán los mismos efectos que los atribuidos a la edición impresa. Y, en referencia específica al Boletín Oficial del Estado, la Ley dispone que su publicación electrónica "tendrá carácter oficial y auténtico en las condiciones y con las garantías que se determinen reglamentariamente, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables". En desarrollo de esta Ley, el Real Decreto 181/2008, de 8 de febrero, de ordenación del diario oficial "Boletín Oficial del Estado", responde al objetivo principal "de que la difusión de las normas jurídicas a través de las nuevas redes electrónicas (y muy especialmente por la red 'Internet') sitúa la publicación normativa en un plano de accesibilidad y propagación muy superior a todo lo hasta ahora conocido". De ahí la relevancia de conferir a los textos normativos así publicados el carácter oficial y auténtico que durante siglos ha tenido, en exclusiva, su impresión en papel como reconoce su artículo 3. Dispone su artículo 14 que "los ciudadanos tendrán acceso libre y gratuito a la edición electrónica del Boletín Oficial del Estado". Dicho acceso comprenderá la posibilidad de búsqueda y consulta del contenido del diario, así como la posibilidad de archivo e impresión, tanto del diario completo como de cada una de las disposiciones, actos o anuncios que lo componen. Como señala el fundamento jurídico primero de la sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección Primera), de 11 de noviembre de 2013, "deben tenerse en cuenta los principios de publicidad y accesibilidad a las decisiones del poder público y de transparencia administrativa, esenciales en un Estado democrático de Derecho, y que las disposiciones, actos o anuncios que se publican en el BOE, y que pueden contener datos de carácter personal, son aquellas que las normas reguladoras de cada procedimiento han estimado que deben recibir tal difusión oficial, por concurrir razones jurídicas o de interés público".

En estos casos, por tanto, entran en juego distintos intereses, como el derecho al honor, a la intimidad y a la protección de datos de carácter personal del indultado, por una parte, y, la transparencia de la información en aras a la protección de la democracia por parte de los ciudadanos en general, por otro.

Bajo la denominación genérica de derecho o prerrogativa de gracia se integran instituciones de diferente naturaleza, como son, la amnistía[464] y el indulto. Como dice Aguado Renedo, "mientras este se proyecta sobre las penas, la amnistía lo hace sobre el acto ilícito, operando sobre él como si nunca hubiere existido, incluso con efectos retroactivos sobre las penas ya purgadas"[465].

La naturaleza de los indultos supone una excepción al principio de separación de poderes, en tanto que el poder ejecutivo ejerce de forma discrecional una prerrogativa de gracia con la que deja sin efecto la ejecución de una resolución judicial. Con el ejercicio del derecho de gracia, un poder diferente al judicial, obligado a cumplir las sentencias firmes, tiene la facultad de dispensar de tal cumplimiento, en situaciones concretas, a individuos determinados y de excepcionar la misión de hacer ejecutar lo juzgado[466].

La Constitución no ha dispuesto que corresponda al poder ejecutivo la facultad de indultar. Es la aún hoy vigente Ley de Indulto de 18 de junio de 1870, la que atribuye materialmente la decisión de indultar -o de no hacerlo- al Consejo de Ministros. Como acertadamente explica Diez- Picazo, "como hija de

---

[464] SIMÓN CASTELLANO, P.: *El reconocimiento del olvido digital*…, pág. 116.

[465] AGUADO RENEDO, C.: "La clemencia vinculada por el derecho", *Revista de Derecho Político*, núm. 74, 2009, pág. 337.

[466] FLIQUETE LLISO, E. F.: "El indulto un enfoque jurídico constitucional", Universidad Miguel Hernández, Elche, 2015, pág. 446, disponible en Internet: http://dspace.umh.es/bitstream/11000/1953/1/TD%20Fliquete%20Lliso%2C%20Enrique%20Fco.pdf. *Vid.* GARCÍA MAHAMUT, R.: *El indulto un análisis jurídico-constitucional*, Marcial Pons, Barcelona, 2004.

su tiempo, la Ley de Indulto refleja la concepción tradicional del derecho de gracia como algo de índole ejecutiva. Pero la Constitución no dice que el derecho de gracia deba corresponder necesaria e íntegramente al Poder Ejecutivo, esto es, al Gobierno. No hay que infravalorar que el derecho de gracia esté regulado no en el Título IV relativo al Gobierno, sino en el Título II relativo a la Corona. Ciertamente, cuando el apartado i) del artículo 62 CE encomienda al Rey 'ejercer el derecho de gracia con arreglo a la ley, que no podrá autorizar indultos generales', nadie entiende que la decisión material de indultar o no indultar corresponda al monarca, pues ello resultaría incompatible con la idea misma de monarquía parlamentaria. Pero del mencionado precepto constitucional se desprenden dos relevantes consecuencias: por un lado, debe existir una regulación legal del derecho de gracia, de manera que el Gobierno no tendría una potestad de indultar si no existiese una ley reguladora de las formas y los límites a que debe ajustarse el indulto; y, por otro lado, la Constitución no sería obstáculo a una regulación legal del indulto notablemente distinta de la actual, en la que el papel del Gobierno en la decisión se viera más constreñido"[467].

Lo cierto es que como ha señalado el máximo intérprete de la Constitución "la figura del indulto permite compatibilizar las exigencias de la justicia formal con las de la justicia material del caso. Ahora bien, el indulto, en cuanto figura del derecho de gracia, corresponde decidirlo al Poder Ejecutivo concediéndolo el Rey, sin que esas decisiones sean fiscalizables

[467] Voto particular concurrente del Magistrado Luis María Díez-Picazo Giménez, a la sentencia del Tribunal Supremo (Sala de lo Contencioso-Administrativo, Pleno), de 20 de noviembre de 2013.

sustancialmente por parte de los órganos jurisdiccionales, incluyendo el Tribunal Constitucional"[468].

Para Aguado Renedo, el concepto del beneficio de la gracia, como una interferencia permitida *ex Constitutione* en la ejecución de lo juzgado, hace que la misma haya de ser entendida como una facultad de uso ponderado, si no claramente restringido a los casos objetivamente necesarios, debiendo quedar excluido radicalmente el abuso de tal institución. Discrecionalidad no es arbitrariedad y, por ello, no cabe explicar la gracia como la renuncia al *ius puniendi* estatal sin más. Ciertamente, se da tal renuncia en la concesión del beneficio, pero ello es solo la descripción de la gracia, no su justificación, y, so pena de entender que en un Estado de Derecho cabe el ejercicio de una competencia de modo absolutamente libérrimo e ilimitado, ha de poder exigirse el uso correcto de la misma[469].

Este instrumento repercute, no solo en la esfera jurídica del indultado, sino también en la confianza que la sociedad tiene depositada en el Estado de Derecho, pues supone una intromisión en el derecho fundamental a la tutela judicial efectiva, que presupone la legítima expectativa de que se dicte una resolución judicial y ésta se ejecute. La peculiar naturaleza de los indultos exige unos cauces de publicidad de los mismos, como mecanismos de control

[468] ATC 360/1990, FJ 5.

[469]AGUADO RENEDO, C.:" El derecho de gracia. El indulto", disponible en Internet: http://0-www.iustel.com.fama.us.es/v2/c.asp. Precisamente a la necesidad de impedir la arbitrariedad mediante un mayor control jurisdiccional de los indultos así como imponer al gobierno la obligación de motivar su concesión responde la Proposición de ley de reforma de la Ley del Indulto, presentada por el grupo parlamentario socialista en septiembre de 2016. *Vid.* Proposición de ley disponible en Internet: http://www.congreso.es/public_oficiales/L12/CONG/BOCG/B/BOCG-12-B-20-1.PDF

público de la potestad discrecional del Gobierno de concederlos[470]. De conformidad con el artículo 15.1 de la Ley 19/2013, de 9 de diciembre, de Transparencia y Buen Gobierno "si la información incluyese datos especialmente protegidos a los que se refiere el apartado 3 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, o datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de Ley". Por lo tanto, en principio, no cabría ponderación alguna entre derechos para resolver el conflicto en el caso de indultos ya que, en aras del principio de transparencia, y por imperativo legal, procedería la publicación de este tipo de datos. Sin embargo, el derecho al olvido tropieza con esta necesidad de transparencia.

Este conflicto se planteó en la sentencia del Tribunal Supremo de 17 de noviembre de 2010, en el que se suscitó una posible responsabilidad patrimonial del Estado sobre la base de la publicación de un indulto por parte del Ministerio de Justicia, en el que el nombre y apellidos del indultado coincidían con el del recurrente, abogado en ejercicio. Este, al introducir su nombre y dos apellidos en diversos buscadores de Internet, obtenía como resultado la referencia a un BOE en el que se hacía constar la existencia de un Real Decreto por el que se indultaba de un delito contra la salud pública. Para el demandante, el Ministerio de Justicia era el responsable de una publicación que no contenía suficientes datos identificadores (además del nombre y dos

[470] SANCHO LÓPEZ, M.: “Consideraciones procesales del ejercicio del derecho al olvido: examen de jurisprudencia reciente y del nuevo marco legal", *Revista Aranzadi de Derecho y nuevas tecnologías*, núm. 41, 2016, pág. 11.

apellidos, el DNI y la fotografía del indultado) y que había servido a distintos buscadores para incluirla en sus portales, y ello había lesionado su prestigio personal y profesional como abogado en el ejercicio normal de su actividad y en el crecimiento de su despacho.

Partiendo de que la publicación de los indultos es un imperativo legal (art. 30 de la Ley del Indulto) que no puede dejarse de cumplir, el Tribunal Supremo afirma en este caso que no puede trasladarse al Ministerio de Justicia, y en consecuencia al Estado, el resultado de las actividades de los buscadores de Internet. Además, pone en duda las repercusiones que sobre la vida privada pueda tener la divulgación de un indulto en Internet. Para la sentencia, "nos movemos ante meras especulaciones cuando afirmamos que la simple publicación del indulto en el BOE desencadena una efectiva publicidad negativa en la persona del recurrente como abogado con una efectiva pérdida de ingresos". En consecuencia, aunque el Tribunal Supremo aprecia que en ocasiones esa publicidad pueda llevar a la consecuencia desgraciada de que una o varias personas coincidan en nombres y apellidos con el reo indultado, y pese a que esa circunstancia pueda trascender al conocimiento público de un modo más o menos intenso por la publicación en el BOE del Real Decreto de indulto y por el hecho de que esas publicaciones aparezcan en los resultados de los buscadores de Internet, esto constituye un daño que el perjudicado por ese hecho está obligado a soportar[471].

La responsabilidad del BOE a la hora de publicar los edictos fue tratada por la AEPD desde su inmunidad como fuente de acceso público y desde su

[471] Sentencia del Tribunal Supremo (Sala de lo Contencioso-Administrativo), de 17 de noviembre de 2010, FJ 4.

consideración como responsable del tratamiento de estos datos personales[472]. La primera posición, esto es, la exoneración de responsabilidad en la cancelación de datos relativos a indultos publicados tanto en formato papel como digital (ni eliminación de datos identificativos, ni sustitución por iniciales), estaba fundada en la consideración del BOE como fuente de acceso público en la que el indulto concedido se inserta por imperativo legal. Ahora bien, sobre la base de la doctrina del Tribunal Europeo de Derechos Humanos expuesta en la sentencia de 6 de noviembre de 2003, caso *Lindqvist,* y recogida por la jurisprudencia española, la AEPD entendió que la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, constituye un "tratamiento total o parcialmente automatizado de datos personales" en el sentido del artículo 3, apartado 1, de la Directiva 95/46[473].

Esto llevó a la AEPD a considerar que el BOE, al publicar datos personales en su página web, está realizando un tratamiento de datos total o parcialmente automatizado y, en consecuencia, aunque por imperativo legal debiera publicar determinados actos administrativos, está sometido a la legislación sobre protección de datos[474]. Por lo tanto, si bien no procedería un derecho de cancelación ante el BOE (eliminando o anonimizando los datos) por

---

[472] R/602/2004, de 4 de noviembre, R/2553/2010, de 20 de diciembre y R/1777/2012, de 13 de julio. *Vid.* RALLO LOMBARTE, A.: *El derecho al olvido en Internet, Google versus…,* págs. 96-100.

[473] Sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1ª), de 20 de abril de 2009.

[474] Como pone de manifiesto Guichot Reina, la AEPD ha admitido que la puesta a disposición en la edición digital de los diarios oficiales supone una injerencia en el derecho a la protección de datos con un notable riesgo lesivo, dada la facilidad de localización de la información y el carácter de fuente de acceso público de los diarios oficiales. GUICHOT REINA, E.: "La publicidad de los datos personales en Internet por parte de las Administraciones Publicas y el derecho al olvido", *Revista Española de Derecho Administrativo*, núm. 154, 2012, pág. 137.

la obligación legal que exige la publicación de los Reales Decretos de indulto, sí sería razonable un derecho de oposición a que los datos personales del indultado sean objeto de un tratamiento que, en sí mismo, es lícito, cuando concurra un motivo legítimo y fundado, en una situación personal concreta *ex* artículo 6.4 LOPD, obstaculizando su cesión para el tratamiento por los buscadores generalistas, al permitir su edición electrónica su rastreo ilimitado por los motores de búsqueda de Internet. Este derecho quedaría satisfecho con el empleo del comando "robots.txt", que permite crear un fichero negativo con contenidos que los motores de búsqueda no podrán rastrear. No obstante no será hasta casi un año y medio después de la sentencia del Tribunal de Justicia de la Unión Europea caso Google Spain, cuando se producirá la recepción de esta doctrina de la AEPD por la jurisprudencia del Tribunal Supremo.

1.3. La publicidad de las resoluciones judiciales.

La Constitución reconoce el derecho a un juicio público en su artículo 24.2 y, como no podía ser menos, el Tribunal Constitucional se ha hecho eco de esta garantía[475]. Además el artículo 120.1 CE prevé la publicidad de las actuaciones judiciales. Como ha reconocido el Tribunal Constitucional el principio de publicidad en el ámbito judicial tiene una doble finalidad: el control público de la justicia y asegurar la confianza en los Tribunales. Esto es, por un lado, proteger a las partes de una justicia sustraída a la supervisión pública, y, por otro, mantener la confianza de la sociedad en los Tribunales, constituyendo

[475] STC 30/1982.

en ambos sentidos tal principio una de las bases del debido proceso y uno de los pilares del Estado de Derecho[476].

En el mismo sentido se pronuncia el artículo 6.1 del Convenio Europeo de Derechos Humanos, habiendo señalado al respecto el Tribunal Europeo de Derechos Humanos que "la publicidad del procedimiento de los órganos judiciales, protege a las partes contra una justicia secreta que escape al control público; por lo que constituye uno de los medios de preservar la confianza en los Jueces y Tribunales"[477].

La Constitución establece asimismo en el artículo 120.3, que las sentencias serán siempre motivadas y se pronunciarán en audiencia pública. Este precepto es, por una parte manifestación del principio de legitimación funcional del poder judicial, el cual está sometido al imperio de la ley como expresión de la voluntad popular, y, por otra, es igualmente reflejo del derecho del justiciable y del interés legítimo de la sociedad en general a conocer las razones de la decisión judicial, es decir, a comprobar que la solución dada al caso es consecuencia de la interpretación y aplicación del derecho, y no fruto de la arbitrariedad. En particular, respecto a la referencia a que las sentencias se tengan que pronunciar en audiencia pública, la jurisprudencia española, recogiendo la doctrina del Tribunal Europeo de Derechos Humanos, considera que no debe seguirse una interpretación literal de dicho artículo, en el sentido de entender que equivale a la lectura pública de la sentencia. El Tribunal Europeo de Derechos Humanos permite que la publicidad se alcance con otros

[476] STC 96/1987, FJ 2.
[477] SSTEDH de 8 de diciembre de 1983, caso Pretto contra Italia, y caso Axen contra la República Federal Alemana.

medios, como puede ser el depósito de la sentencia en un registro público o su publicación en una relación oficial[478].

En tal sentido, de los artículos 235 bis y 266 de nuestra Ley Orgánica del Poder Judicial -en adelante LOPJ- se extrae que las sentencias, una vez extendidas y firmadas por el juez o por todos los Magistrados que las hubieren dictado, serán depositadas en la Oficina judicial y se permitirá a cualquier interesado el acceso al texto de las mismas[479]. No obstante, el acceso al texto de las sentencias, o a determinados extremos de las mismas, solo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contuvieran[480] y podrá quedar restringido cuando el mismo pudiera afectar al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o

---

[478] SSTEDH de 8 de diciembre de 1983, caso Pretto contra Italia, y de 22 de febrero de 1984, caso Sutter contra Suiza.

[479] El concepto de interesado es muy restringido, al atribuirse tal condición tan solo a quien manifiesta y acredita al menos "prima facie" ante el órgano judicial una conexión de carácter concreto y singular bien con el objeto mismo del proceso, bien con alguno de los actos procesales a través de los que aquel se ha desarrollado y que están documentados en autos. *Vid.* ORENES RUIZ, J. C.: "Publicidad de sentencias, Internet y protección de datos de carácter persona", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 30, 2012, pág. 1.

[480] Artículo 235 bis, introducido por Ley Orgánica 7/2015, de 21 de julio de reforma de la LOPJ. No obstante la Ley Orgánica 10/2015, de 10 de septiembre de reforma de la LOPJ ha añadido el artículo 235 ter en orden a posibilitar el acceso público a través del BOE a los datos personales contenidos en los fallos de las sentencias firmes condenatorias por delito de defraudación tributaria. Sobre el anteproyecto de esta norma se pronunciaron el Consejo General del Poder Judicial y el Consejo fiscal en sendos informes de 11 y 15 de mayo de 2015. Su encaje constitucional se fundamenta en los artículos 120 CE y 31.1 CE. Según el preámbulo de la norma "el bien jurídico protegido en estos casos ha sido elevado a rango constitucional en el artículo 31 CE, lo que resulta relevante a la hora de realizar esa ponderación en este ámbito, pues no cabe olvidar que el deber constitucional de contribuir al sostenimiento de los gastos públicos tiene como reverso el derecho del conjunto de la sociedad a exigir el cumplimiento de las obligaciones tributarias, así como al control de la actividad de todos los poderes públicos dirigida a la lucha contra el fraude fiscal, concreción en este ámbito del principio general de transparencia que debe informar la actividad pública y muy especialmente la actuación judicial". Sobre la valoración crítica de esta disposición vid, RAMOS PRIETO, J.: " El nuevo instrumento en la lucha contra el fraude fiscal: la publicación de los datos personales de las sentencias condenatorias por determinados delitos contra la Hacienda Pública" en COLOMER HERNÁNDEZ, I. (dir.): *Cesión de datos* personales *y evidencias entre procesos penales y procedimientos administrativos sancionadores y tributarios,* Aranzadi, Cizur Menor, 2017, págs. 695-713.

perjudicados, cuando proceda, así como, con carácter general, para evitar que las sentencias puedan ser usadas con fines contrarios a las Leyes. En consecuencia el principio de publicidad de las sentencias no es ilimitado y de él no puede derivarse el acceso indiscriminado e íntegro al texto las resoluciones judiciales en todos los casos.

Sobre la base de las consideraciones anteriores, la LOPD no considera a las sentencias como fuentes accesibles al público. La doctrina de la AEPD es reiterada en este sentido y ha sido confirmada por los Tribunales: sin perjuicio del principio de publicidad de las sentencias de la LOPJ, las resoluciones judiciales no pueden ser consideradas como fuente accesible al público puesto que el artículo 3.j de la LOPD hay que interpretarlo literalmente. Dicho artículo recoge un *númerus clausus* de las fuentes que pueden calificarse como accesibles al público, lo que se remarca con el empleo del término "exclusivamente" que se anuda a las concretas fuentes que enumera[481].

El Tribunal Europeo de Derechos Humanos, en sentencia de 6 de octubre de 2009, condenó a España[482] por no anonimizar la sentencia de un Juzgado de Primera Instancia que permitía asociar la identidad del demandante con los datos de salud, concretamente con la enfermedad de SIDA, lo cual no estaba justificado por ningún motivo imperioso y suponía una violación del derecho a la vida privada consagrado en el artículo 8 del CEDH.

En esta dirección, el artículo 7 del Reglamento del Consejo General del Poder Judicial 1/2005, de 15 de septiembre, sobre los aspectos accesorios de las actuaciones judiciales, se remite a la normativa de protección de datos y, en

[481] Resoluciones AEPD 337/2009 y 1135/2009. *Vid.* ORENES RUIZ, J. C.: art. cit.
[482] STEDH de 6 de octubre de 2009, caso CC contra España.

particular, establece "que en el tratamiento y difusión de las resoluciones judiciales se cumplirá lo dispuesto en la legislación en materia de protección de datos personales y en los artículos 234 y 266 de la LOPJ[483]. Salvo lo dispuesto en dichos artículos, no se facilitarán por los órganos jurisdiccionales copias de las resoluciones judiciales a los fines de difusión pública regulados en el presente artículo, sin perjuicio del derecho a acceder en las condiciones que se establezcan, a la información jurídica de que disponga el Centro de Documentación Judicial del Consejo General del Poder Judicial. Todo ello sin perjuicio de las competencias atribuidas a los Gabinetes de Comunicación del Tribunal Supremo, Audiencia Nacional y Tribunales Superiores de Justicia, previstas en el Reglamento de los Órganos de Gobierno de Tribunales".

El Centro de Documentación Judicial del CGPJ (CENDOJ) es el órgano competente para la publicación oficial de las sentencias y otras resoluciones que se determinen del Tribunal Supremo y del resto de órganos judiciales. El

---

[483] Artículo 234 LOPJ: "1. Los Letrados de la Administración de Justicia y funcionarios competentes de la Oficina judicial facilitarán a los interesados cuanta información soliciten sobre el estado de las actuaciones judiciales, que podrán examinar y conocer, salvo que sean o hubieren sido declaradas secretas o reservadas conforme a la ley. 2. Las partes y cualquier persona que acredite un interés legítimo y directo tendrán derecho a obtener, en la forma dispuesta en las leyes procesales y, en su caso, en la Ley 18/2011, de 5 de, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, copias simples de los escritos y documentos que consten en los autos, no declarados secretos ni reservados. También tendrán derecho a que se les expidan los testimonios y certificados en los casos y a través del cauce establecido en las leyes procesales". Incluso, el Real Decreto 65/2015, de 27 de noviembre, sobre comunicaciones electrónicas de la administración de justicia en el ámbito territorial del Ministerio de justicia y regulador del sistema Lexnet, prevé en el artículo 7.3 que "lo dispuesto en este real decreto se aplicará observando y garantizando la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio del Poder Judicial". Artículo 266 LOPJ: "1. Las sentencias, una vez extendidas y firmadas por el juez o por todos los Magistrados que las hubieren dictado, serán depositadas en la Oficina judicial y se permitirá a cualquier interesado el acceso al texto de las mismas. El acceso al texto de las sentencias, o a determinados extremos de las mismas, podrá quedar restringido cuando el mismo pudiera afectar al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda, así como, con carácter general, para evitar que las sentencias puedan ser usadas con fines contrarios a las Leyes. 2. Los secretarios pondrán en los autos certificación literal de la sentencia."

CENDOJ intenta compaginar el libre acceso de los ciudadanos a la misma, configurada como un auténtico servicio público, con el derecho a la protección de los datos de carácter personal. Así, la jurisprudencia que publica en Internet, de modo libre y gratuito, aparece vaciada de datos personales. Del mismo modo sucede con las sentencias que las editoriales jurídicas adquieren para elaborar las bases de datos de jurisprudencia y cuyos datos aparecen disociados[484].

Sobre la base de las consideraciones anteriores, el alcance de la publicidad de las sentencias del Tribunal Constitucional plantea un posible conflicto con el derecho fundamental a la protección de datos personales, lo que ha requerido su posicionamiento, en el que ha dejado clara su postura contraria al criterio de establecer restricciones a su publicidad, al afirmar la importancia de dar la máxima difusión a las sentencias del Tribunal Constitucional en su integridad.

En la STC 114/2006[485], el recurrente había solicitado que cuando se procediera a llevar a cabo la publicación e inserción de la sentencia, en Internet y en el BOE electrónico, se incluyeran únicamente sus iniciales, así como las de su ex esposa y demás personas que pudieran constar en la resolución, alegando motivos de seguridad personal, prestigio y dignidad personal y familiar. Esta petición, sobre la que el Tribunal ya había tenido ocasión de pronunciarse[486], sirve al máximo intérprete de la Carta Magna para afirmar su

---

[484] *Vid.* ORENES RUIZ, J. C.: *op. cit.*, pág. 2.
[485] STC 114/2006. *Vid.* RAMOS GONZÁLEZ, S., MILÁ RAFAEL, R., GIL SALDAÑA, M. A. y SALVADOR CORDECH, P.: "Las sentencias del Tribunal Constitucional deben publicarse íntegras: Comentario a la sentencia del Tribunal Constitucional, Sala Primera, 114/2006, de 5 de abril de 2006 (MP: Pablo Pérez Tremps). Recurso de amparo 24-2002 (BOE núm. 110, de 9 de mayo de 2006)", *Indret: Revista para el Análisis del Derecho*, núm. 3, 2006.
[486] ATC 516/2004, FJ 5.

absoluta independencia de los demás órganos constitucionales, estando sometido únicamente a la Constitución y a su Ley Orgánica[487]. A partir de esta base, afirma que, de acuerdo con el principio general recogido en el artículo 120 CE, conforme al que las actuaciones judiciales serán públicas, con las excepciones que prevean la leyes de procedimiento y las sentencias serán siempre motivadas, y, más específicamente, de conformidad con la previsión contemplada en el artículo 164 CE de que "las sentencias del Tribunal Constitucional se publicarán en el Boletín Oficial del Estado con los votos particulares, se confirma la exigencia constitucional de dar la máxima difusión y publicidad a la doctrina constitucional emanada de las resoluciones del Tribunal Constitucional.

El mandato enunciado, para la sentencia anterior, se concreta, desde una perspectiva formal, no solo en la publicación integra en soporte papel de determinadas resoluciones en el Boletín Oficial, sino también en la obligación material de dar la mayor accesibilidad y difusión pública, por cualquier medio, al contenido de todas aquellas resoluciones jurisdiccionales del Tribunal Constitucional que incorporen doctrina constitucional, con independencia de su naturaleza y del proceso en que se dicten. El razonamiento que fundamenta esta decisión está en la función específica que cumple la jurisprudencia constitucional, siendo el Tribunal Constitucional el supremo intérprete de los preceptos y principios de nuestra Carta Magna, lo que hace imprescindible la

[487] Artículos 86.2 y 99.2 Ley Orgánica del Tribunal Constitucional -en adelante LOTC-. De acuerdo con el artículo 80 LOTC: “Se aplicarán, con carácter supletorio de la presente Ley, los preceptos de la Ley Orgánica del Poder Judicial y de la Ley de Enjuiciamiento Civil, en materia de (...) publicidad y forma de los actos (...)”.

máxima divulgación de la doctrina constitucional que proviene de sus resoluciones.

La garantía efectiva de la vinculación a la Constitución de todos los ciudadanos y de todos los poderes públicos (art. 9.1 CE) -en particular de los órganos judiciales (art. 5.1 LOPJ)- exige como *prius* un conocimiento inobjetable de la doctrina constitucional que al Tribunal Constitucional corresponde preservar y promover con cuantos medios obren a su alcance[488]. Y, más taxativamente, la completa identificación de quienes han sido parte en el proceso permite asegurar el imparcial ejercicio de la jurisdicción constitucional y el derecho de todos a ser informados de las circunstancias, también las personales, de los casos que por su trascendencia acceden a ella, lo cual descartaría anonimizar las resoluciones, suprimiendo los datos identificativos de las partes o sustituyéndolos por sus iniciales.

Por lo demás, el Tribunal Constitucional recordó en la STC 114/2006 que este principio de publicidad íntegra de las sentencias es, además, aplicado por otros tribunales, en particular por el TEDH y el TJUE[489].

No faltan quienes han puesto en duda la solidez de este razonamiento para apoyar la supresión de determinados datos identificativos de las partes

[488] RALLO LOMBARTE, A: *El derecho al olvido en Internet, Google versus...*, pág. 80.

[489] Así, el artículo 33 del Reglamento de Procedimiento del Tribunal Europeo de Derechos Humanos, de 14 de noviembre de 2016, establece el principio de publicidad de los documentos del Tribunal y, en particular, respecto de las decisiones y resoluciones, establece que son accesibles al público. Asimismo, su artículo 63 recoge el principio de publicidad de las actuaciones judiciales: "La audiencia es pública, a menos que, conforme al apartado 2º del presente artículo, el Tribunal decida lo contrario por razón de las circunstancias excepcionales del caso". En el mismo sentido, el principio de publicidad rige también en la jurisdicción del Tribunal de Justicia de la Unión Europea. Así, el artículo 117 del Reglamento de Procedimiento del TJUE, de 4 de marzo de 2015, señala que: "La sentencia contendrá: g) la designación de las partes". Además, el artículo 35.3 establece que el Secretario se encargará de las publicaciones del Tribunal General, en particular de la Recopilación de la Jurisprudencia, y de la difusión en Internet de documentos relativos al Tribunal General. Disponible en Internet: http://www.echr.coe.int/Documents/Rules_Court_ENG.pdf y en http://eur-lex.europa.eu/legal conent/ES/TXT/PDF/?uri=-CELEX:32015Q0423(01)&from=ES

(nombre y apellidos) en las resoluciones del Tribunal Constitucional. Opinión que comparto, pues, como señala Rallo Lombarte[490], resulta difícil imaginar que por dichos motivos pudiera verse cuestionada la imparcialidad del Tribunal o dificultado el conocimiento fehaciente de la doctrina emanada de sus resoluciones, máxime cuando los órganos judiciales, y, en particular, el Tribunal Supremo ven compiladas sus resoluciones para conocimiento general anonimizando las mismas.

De todas formas, el principio enjuiciado no es tan absoluto como parece a primera vista y puede ceder, a partir de la ponderación de circunstancias concurrentes en el caso, debidamente acreditadas, por resultar prevalentes otros intereses constitucionales. A este respecto, el Tribunal Constitucional ha procedido a omitir puntualmente la identificación de determinadas personas que aparecían mencionadas en sus resoluciones en garantía del derecho a la intimidad, de los derechos de quienes requieran un especial deber de tutela y del anonimato de determinadas víctimas y perjudicados, así como, con carácter general, para evitar que las sentencias puedan ser usadas con fines contrarios a las leyes[491]. Así, en la STC 127/2003, el Tribunal Constitucional prescinde de los datos identificativos de la recurrente de amparo, que era menor de edad y había sido víctima de un delito sexual, reconociendo la vulneración de su derecho a la intimidad por parte del reportaje periodístico que permitía su completa identificación, que frustraba además, la finalidad de la decisión judicial de celebrar el juicio a puerta cerrada.

---

[490] RALLO LOMBARTE, A.: *El derecho al olvido en Internet, Google versus…,* pág. 82

[491] Como resulta del articulo 266.1 LOPJ, aplicable al Tribunal Constitucional de conformidad con el artículo 80 LOTC. Son supuestos de anonimización las SSTC 7/1994, 114/1997, 288/2000, 124/2002, 185/2002, 221/2002, 94/2003, 144/2003, y 30/2005.

La reforma de la Ley Orgánica del Tribunal Constitucional, mediante la Ley Orgánica 6/2007, de 24 de mayo, dio nueva redacción a su artículo 86, apartados segundo y tercero, ubicado en el Titulo VII de la LOTC, denominado "De las disposiciones comunes sobre procedimiento". Conforme al último apartado de dicho artículo en su redacción actual, "… el Tribunal podrá disponer que las sentencias y demás resoluciones dictadas sean objeto de publicación a través de otros medios, y adoptará, en su caso, las medidas que estime pertinentes para la protección de los derechos reconocidos en el artículo 18.4 de la Constitución".

La doctrina constitucional contenida en la STC 114/2006, donde se establece la competencia exclusiva y excluyente del Tribunal Constitucional para determinar las posibles limitaciones a la publicidad de sus resoluciones, se ha extendido en la jurisprudencia de los órganos judiciales. Así, la Audiencia Nacional, en sentencia de 11 de noviembre de 2013, resolvió sobre el derecho a la cancelación de datos personales, en cuanto a la publicación de una sentencia del Tribunal Constitucional en la página web del BOE.

La controversia suscitada en el caso anterior, a decir verdad, era sustancialmente idéntica a la planteada y resuelta por la misma Sala y Sección de la Audiencia Nacional en la sentencia de 30 de octubre de 2013[492], donde el mismo recurrente ejercitaba la misma pretensión de tutela respecto de la misma sentencia del Tribunal Constitucional, solo que referida a la página web del Tribunal Constitucional.

[492] Sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1ª), de 19 de julio de 2013, y sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1ª), de 30 de octubre de 2013.

El recurrente remitió un escrito al BOE manifestando la oposición al tratamiento de sus datos personales y en su defecto, pidiendo el bloqueo de dichos datos. Según su argumentación, la localización de esa información personal a través de motores de búsqueda, como Google, le estaba acarreando consecuencias negativas en su intimidad, honor y privacidad. Solicitaba aquel, concretamente, la cancelación de los datos personales que se contenían en los enlaces web de aquellas páginas y su sustitución por iniciales, es decir, anonimizar los datos personales aparecidos en dicha sentencia en tal página web del BOE o, en su defecto, la inclusión de las disposiciones mencionadas en el fichero robots.txt para evitar que esa información personal pudiera ser indexada, puesto que el citado fichero deja inalterable la publicación en el BOE, pero impide que esa concreta publicación del BOE aparezca en los buscadores de Internet.

En el supuesto que nos ocupa, la Audiencia Nacional sostiene que el Tribunal Constitucional, como intérprete supremo de la Constitución, ha ponderado la eventual prevalencia de los derechos fundamentales y garantías constitucionales, en concreto el derecho fundamental a la protección de datos personales, con los que pudiera entrar en conflicto la decisión jurisdiccional de otorgar máxima difusión y publicidad al contenido íntegro de una sentencia, incluyendo los datos personales de identificación del demandante, y que sobre la base de la jurisprudencia de aquel, ha decidido en ejercicio de su función jurisdiccional otorgar prevalencia a la difusión y publicidad de su resolución jurisdiccional.

A partir de la entrada en vigor del Acuerdo del Pleno del Tribunal Constitucional de 23 de julio de 2015, que regula la exclusión de los datos de

identidad personal en la publicación de las resoluciones jurisdiccionales, este es el criterio general cuando se trate de menores y personas que requieran un especial deber de tutela, de las víctimas de delitos de cuya difusión se deriven especiales perjuicios y de las personas que no estén constituidas en parte en el proceso constitucional. En los demás casos, la exigencia constitucional de publicidad de sus resoluciones (artículo 164 CE), en lo relativo a los datos de identidad y situación personal de las partes intervinientes en el proceso, podrá ser excepcionada por el Tribunal Constitucional de oficio o a instancia de parte, a partir de la ponderación de circunstancias debidamente acreditadas concurrentes en el caso,[493]. En este último supuesto, "si una parte estimase necesario que en un asunto sometido al conocimiento del Tribunal no se divulgue públicamente su identidad o situación personal, deberá solicitarlo en el momento de formular la demanda o en el de su personación, exponiendo los motivos de su petición. El Tribunal accederá a la petición cuando, a partir de la ponderación de circunstancias debidamente acreditadas concurrentes en el caso, la estime justificada por resultar prevalente el derecho a la intimidad u otros intereses constitucionales". Y entre estos no cabe duda que el Tribunal Constitucional habrá de tener en cuenta el derecho fundamental a la protección de datos[494].

---

[493] BOE núm. 178, de 27 de julio de 2015, disponible en Internet: https://www.boe.es/buscar/pdf/2015/BOE-A-2015-8372-consolidado.pdf

[494] Se pregunta Ricard Martínez, ¿qué impacto producirá en la esfera de derechos de un sujeto la publicación de sentencias que no afectando a su intimidad se refieran a aspectos como su capacidad económica, su ideología, o simplemente puedan desmerecerle en la consideración ajena? Ciertamente el recurrente ya sabe a qué se expone, pero ¿le disuadirá precisamente el riesgo de ser identificado e indexado a la hora de presentar un recurso? ¿Deberíamos sumar ahora la pena de buscador a la pena de telediario? Para este autor, una interpretación excesivamente generosa del conflicto que genera la publicidad procesal de las sentencias del Tribunal Constitucional podría sin duda afectar a la configuración constitucional de sus procedimientos. Sin embargo, una noción estricta que atienda exclusivamente a los tres

2. EL DIFÍCIL EQUILIBRIO ENTRE EL DERECHO AL OLVIDO DIGITAL DEL PASADO PENAL Y OTROS BIENES Y DERECHOS CONSTITUCIONALES EN LA JURISPRUDENCIA DEL TRIBUNAL SUPREMO.

El flujo masivo de información personal en Internet obliga a evitar la banalización de las amenazas que genera en el individuo e invita a reforzar la vigencia del derecho fundamental a la protección de datos[495]. Los datos personales en formato digital permiten su almacenamiento de forma ilimitada y su puesta a disposición de cualquiera a través de los buscadores en Internet *sine die*. Siendo la protección de datos un derecho fundamental, el tratamiento de datos personales que implica el volcado de esta información en Internet debe justificarse en la tutela de otros bienes o derechos constitucionales.

El avance tecnológico, y en particular Internet, han dificultado el control sobre la difusión de las condenas penales, que encuentra en el derecho fundamental a la protección de datos un límite más idóneo que el que representan los tradicionales derechos al honor y a la intimidad. No obstante, si en los conflictos honor-información o intimidad-expresión existen pautas hermenéuticas consolidadas que posibilitan su resolución, el litigio entre protección de datos y medios de comunicación adolece todavía de una bisoñez que se traduce en una enorme dificultad para trasladar al entorno informativo

---

supuestos arriba enumerados y solo considere como valor preferente la intimidad puede repercutir significativamente sobre la esfera vital de los recurrentes. Si además, esta rigidez no viene acompañada de políticas de no indexación por los buscadores, los abogados que asistan al recurrente deben incorporar a su arsenal de conocimientos un curso acelerado sobre derecho al olvido. MARTÍNEZ MARTÍNEZ, R.: "La anonimización de las sentencias del tribunal constitucional", *Unir Revista*, 2015, disponible en Internet: http://www.unir.net/derecho/revista/noticias/la-anonimizacion-de-las-sentencias-del-tribunal-contitucional/549201456751/

[495] RALLO LOMBARTE, A.: *op. cit.,* pág. 27.

los principios y derechos propios de la protección de datos (calidad, consentimiento, acceso, cancelación, rectificación, oposición, etc.)[496]

Los motores de búsqueda facilitan el acceso a la información sobre el pasado penal a través de métodos de indexación. El Tribunal de Justicia de la Unión Europea, como se examinó anteriormente, ha ponderado los intereses en juego, por un lado el del internauta que lucha por su derecho al respeto a su vida privada, fundamento último del derecho fundamental a la protección de datos, y los motores de búsqueda, que defienden sus intereses económicos, resolviendo en favor del primero y obligando a los segundos a desindexar la información de carácter personal. No obstante, las dificultades de aquellos que quieren poner en marcha el derecho al olvido digital son mayores cuando los datos están contenidos en fuentes accesibles al público porque han sido publicados por terceros sin su consentimiento, amparados en la libertad de información, o cuando su consentimiento es irrelevante, por tratarse de datos que resultan de Diarios y Boletines Oficiales.

Si el derecho al olvido digital es un derecho en construcción en general, más aún lo es en el ámbito objeto de nuestro interés. Por ello vamos a tratar de acercarnos a su contenido a través de los pronunciamientos jurisprudenciales del Tribunal Supremo, la máxima instancia judicial que, como garante natural de la protección de los derechos fundamentales, ha tratado de perfilar a día de hoy sus dimensiones en el ordenamiento jurídico español.

---

[496] RALLO LOMBARTE, A.: "El derecho al olvido en el tiempo de Internet. La experiencia española", pág. 160. Disponible en Internet: http://repositori.uji.es/xmlui/bitstream/handle/10234/122643/ID66654.pdf?sequence%20=1

2.1 El derecho al olvido digital y las libertades informativas.

Como regla general en la normativa actual de protección de datos, no será preciso el consentimiento del interesado para el tratamiento de sus datos personales cuando el mismo sea manifestación del ejercicio de las libertades de expresión e información. Tal principio debe ponerse en relación con el artículo 20 CE, sin perjuicio de que tal actividad deberá respetar en todo caso el principio de calidad de los datos[497].

De este modo cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, el tratamiento de los datos personales no requiere el consentimiento previo del interesado, siempre que no se vulneren los derechos y libertades fundamentales del mismo[498]. Y entre las fuentes accesibles al público se encuentran los medios de comunicación (art. 3.j LOPD).

La problemática que plantea la conciliación del derecho al olvido digital y las libertades informativas a través de los medios de comunicación *on line* ha sido resuelta a favor de las segundas. La comunicación social no puede entenderse a día de hoy sin Internet; los contenidos digitales forman ya parte de nuestra realidad cotidiana. La Red ha fortalecido universalmente la formación de la opinión pública libre[499]. Podemos decir que las libertades de

[497] Artículo 4 LOPD.
[498] Artículo 6.2 LOPD.
[499] En este sentido, la preferencia de la libertad de información sobre el derecho a la protección de datos personales es también una consecuencia lógica de la libertad ideológica, del valor del pluralismo político y, en definitiva, del principio democrático. *Vid.* TRONCOSO REIGADA, A.: *La protección de datos personales. En busca*…, pág. 210.

expresión y de información amparan la intangibilidad de los datos personales en los medios de comunicación *on line.*

La digitalización de la prensa escrita, en particular, en su sección de hemeroteca, ha provocado su indexación por los motores de búsqueda de Internet, lo que ha facilitado el acceso a informaciones del pasado que, en ocasiones, lesionan los derechos de la personalidad de las personas afectadas. Ciertamente, en el caso de la publicidad de las condenas penales, el soporte divulgativo suele ser un medio de comunicación, cuya difusión queda amparada por la libertad de información, al pretender contribuir a la formación de una opinión publica libre en una sociedad democrática, lo que hace que estemos ante un tratamiento de datos personales lícito y amparado en el artículo 20 CE.

El tema de la divulgación indiscriminada del pasado penal por los buscadores de Internet a propósito de las hemerotecas digitales fue abordado por la Sentencia de la Sala de lo Civil del Tribunal Supremo de 15 octubre de 2015.

En 1985, la policía procedió a la detención del hermano del entonces alcalde de una gran ciudad española, por un presunto delito de tráfico de drogas. El diario El País se hizo eco de la noticia ampliamente, acompañándola de los datos sobre la identidad personal, profesional y del estado de salud de otros detenidos, entre los que se encontraban dos mujeres que eran hermanas. En particular, se aludía al "síndrome de abstinencia" del que estaban siendo tratadas las dos hermanas, que, tras su detención, fueron ingresadas en un centro penitenciario.

Estas personas fueron condenadas en su día por un delito de contrabando y, posteriormente, superaron su adicción a las drogas y desarrollaron normalmente su vida familiar y profesional.

Desde noviembre de 2007 era posible el acceso público, general y gratuito a la hemeroteca digital del diario El País. La página web en la que se encontraba recogida la noticia no contenía ningún código ni instrucción que impidiera que los motores de búsqueda indexaran las palabras contenidas en el código fuente, incluyendo las relativas a los datos personales de las personas afectadas, y las almacenaran en sus bases de datos para permitir búsquedas mediante la utilización de esa información personal, como palabras clave[500]. De este modo, cuando se introducía el nombre y los apellidos de una de las afectadas el enlace a la web de la hemeroteca digital de El País que contenía la noticia aparecía como primer resultado en *Google* y *Yahoo.* Cuando se hacía con el nombre y los apellidos de la otra afectada, aparecía en primer lugar en la lista de resultados de *Google* y en tercer lugar en la lista de resultados de *Yahoo.*

A diferencia del asunto resuelto por la sentencia del Tribunal de Justicia de la Unión Europea en el caso Google, las demandantes se dirigieron contra el editor de la página web[501], y no contra los gestores de los motores de

---

[500] Es más, estos datos personales aparecían como palabras clave en la cabecera de dicho código fuente, con lo cual se resaltaba su relevancia y se facilitaba que en los espacios de publicidad “on line” que contenía la página web apareciera publicidad relacionada con ellas, puesto que se trataba del texto marcado como contexto para escoger la publicidad "on line".

[501] Las interesadas ejercitaron sendas oposiciones contra Google Spain, Prisacom y El País. Prisacom denegó la petición aduciendo que El País era responsable solo de la edición digital, indexada por Google Search y obtenida en la lista de resultados de este motor de búsqueda a partir de la consulta por sus nombres. El 3 de agosto de 2009 (TD/1436/2009 y TD/1437/2009), las afectadas solicitaron la tutela de la AEPD contra El País y Google Spain, al no haber atendido su derecho de oposición. La AEPD estimó la tutela solicitada frente a El País -no frente a Google Spain- instándola a que considerase la posibilidad de limitar la indexación de

búsqueda, solicitando a Ediciones El País que cesara en el tratamiento de sus datos personales o que lo sustituyera por las iniciales de sus nombres y apellidos, y que adoptara las medidas tecnológicas necesarias para que la página web no fuera indexada por los motores de búsqueda de Internet.

Ediciones El País rechazó tal pretensión alegando que su conducta estaba amparada en el ejercicio de la libertad de información, pues la noticia se contenía en la hemeroteca digital como cualquier otra, que no podía proceder al borrado o modificación del artículo, pues ello equivaldría a la retirada de los archivos existentes en las hemerotecas, y, asimismo, que no podía adoptar medida alguna para evitar que los buscadores en Internet indexaran la noticia.

A la pregunta, "¿para qué sirve entonces la cancelación de los antecedentes penales si la noticia siempre saldrá a través de los buscadores?", la resolución judicial responde que volver a publicar una noticia de 1985, que ya formaba parte de la esfera privada de las interesadas, suponía una vulneración de los derechos al honor y a la intimidad de las afectadas, porque se refería a hechos que carecían de interés general y no eran noticiables debido al tiempo transcurrido, al hacer referencia al pasado de personas que ya habían superado sus problemas de drogodependencia y, en su momento, fueron enjuiciadas y condenadas por ello. Además, el hecho de que dicha noticia fuera accesible poniendo sus nombres y apellidos en *Google* suponía un menoscabo de su reputación, afectando a su vida personal y profesional (eran médica y abogada).

---

tales datos personales en la noticia relacionada. *Vid*. RALLO LOMBARTE, A.: art. cit., pág. 162,.y DI PIZZO CHIACCHIO, A.: “Efectos en la jurisprudencia del Tribunal Supremo de la doctrina sentada en el caso 'Google Spain': la interpretación de la responsabilidad de los gestores de motores de búsqueda en la implementación del derecho al olvido digital", *RJC,* núm. 4, 2016, pág. 81.

En relación con el derecho al olvido, la sentencia expone que "(…) tras su rehabilitación tanto personal como legal, su pasado siempre las va a acechar, no teniendo así derecho al olvido, viéndose condenadas "*ad eternum*" a que la sociedad las continúe juzgando y valorando por hechos de febrero de 1985".

En fin, para el Juzgado de Primera Instancia[502], la difusión de la noticia por Ediciones El País suponía una vulneración de los derechos al honor, a la intimidad y a la protección de datos personales, porque suponía la divulgación de unos antecedentes penales que estas personas ya tenían cancelados[503]. No podía justificarse que quedaran afectados tales derechos en aras de la libertad de información porque faltaba la veracidad de la información, el interés público de la noticia y, además, no se trataba de personajes púbicos.

Lo más interesante de este pronunciamiento es que la resolución judicial distinguió entre la finalidad informativa[504], que se obtuvo cuando se publicó la noticia en los años ochenta, y la finalidad mercantilista de incremento de ingresos publicitarios a través del volcado de la hemeroteca en soporte digital. Faltaba la finalidad periodística en la inclusión de la noticia en la hemeroteca digital del diario. Por esto, condenó a Ediciones El País a cesar en su difusión,

---

[502] Juzgado de Primera Instancia núm. 21 de Barcelona, dictó sentencia de 4 de octubre de 2012.

[503] La sentencia puso de manifiesto que en el año 2007, las circunstancias habían cambiado porque las afectadas, que fueron condenadas en su día por un delito de contrabando, tenían cancelados sus antecedentes penales. Al no haberse implementado por ediciones El País los elementos de control necesarios, el artículo había alcanzado en el año 2007 una difusión total y absoluta.

[504] El artículo periodístico controvertido estaba amparado por el derecho a la libertad de información, pues nadie discutía la veracidad de los sucesos divulgados en el año 1985 ni su relevancia pública, además de no haberse utilizado en su redacción expresiones injuriosas, ni inadecuadas.

mediante la inclusión del comando *NO INDEX*, aunque no impidió que la noticia siguiera en la hemeroteca digital del periódico.

En la segunda instancia, la Audiencia Provincial de Barcelona, no solo desestimó el recurso de apelación interpuesto por Ediciones El País, sino que le impuso una condena más rigurosa, al obligarle a cesar en el uso de los datos personales en el código fuente de la página web que contenía la noticia y en la propia página web, sin que pudieran constar ni los nombres, ni los apellidos, ni las iniciales de los afectados.

El Tribunal Supremo, al entrar a resolver el recurso de casación correspondiente, empieza delimitando el objeto del mismo, que era el tratamiento de los datos personales que llevó a cabo el editor de la página web como consecuencia de la digitalización de una noticia, con determinadas características técnicas que permitían su indexación y aparición en los resultados de los buscadores de Internet, de modo que perjudicaban al honor y la intimidad de las personas afectadas.

Según los argumentos de Ediciones El País en el recurso, estaríamos ante un tratamiento de datos personales con fines periodísticos amparado en la libertad de información. El carácter privado del medio de comunicación y la utilización de la publicidad como fuente de ingresos no impedía que su actuación pudiera tutelarse al amparo del artículo 20 CE[505]. Los hechos recogidos en la noticia, posteriormente incluida en la hemeroteca digital, fueron veraces y tenían interés público, pues lo tienen las informaciones relativas a la

[505] STJUE de 16 de diciembre de 2008, caso Satakunnan Markkinapörssi y Satamedia, asunto C-73/07, párrafos 56 a 61. En particular, el párrafo 59 dispone: "el hecho de que se publiquen datos personales con ánimo de lucro no excluye a priori que pueda considerarse una actividad 'exclusivamente con fines periodísticos'".

comisión de delitos y la averiguación y detención de sus autores. Alegó, también Ediciones El País que la expresión de los nombres y apellidos de los implicados en hechos delictivos estaría amparada por la libertad de información, según la jurisprudencia del Tribunal Constitucional. Por consiguiente, a su juicio, el transcurso del tiempo no convertía la noticia en inveraz ni en carente de interés público.

El Tribunal Supremo, en su sentencia de 15 de octubre de 2015, parte de la premisa de que el editor de una página web en la que se incluyen datos personales realiza un tratamiento de datos, como se deduce de la STJUE del caso Lindqvist [506], y de que, como tal, es responsable del mismo, conforme a la STJUE del caso Google[507]. En consecuencia, Ediciones el País debió respetar el principio de calidad de los datos, conforme al cual los datos personales objeto de tratamiento automatizado han de ser exactos (art. 6.1.e de la Directiva 95/46/CE y 4.3 LOPD), adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se hayan obtenido (art. 6.1.d de la Directiva 95/46/CE y 4.1 LOPD).

El problema no era que el tratamiento de los datos personales fuera inveraz, como afirmaba el Juzgado de Primera Instancia, sino, como aclara el Tribunal Supremo, que podía "no ser adecuado a la finalidad con la que los datos personales fueron recogidos y tratados inicialmente. El factor tiempo tiene una importancia fundamental en esta cuestión, puesto que el tratamiento de los datos personales debe cumplir con los principios de calidad de datos no solo en el momento en que son recogidos e inicialmente tratados, sino durante

[506] STJUE de 6 de noviembre de 2003, caso Lindqvist, asunto C-101/01, párrafo 25.
[507] STJUE de 13 de mayo de 2014, caso Google Spain S.L contra Agencia Española de Protección de Datos, asunto C-131/12, párrafo 26.

todo el tiempo en que se produce ese tratamiento. Un tratamiento que inicialmente pudo ser adecuado a la finalidad que lo justificaba puede devenir con el transcurso del tiempo inadecuado para esa finalidad, y el daño que cause en derechos de la personalidad como el honor y la intimidad, desproporcionado en relación al derecho que ampara el tratamiento de datos."[508]

De este modo, el Tribunal Supremo lleva a cabo una ponderación de los derechos en conflicto. Citando la jurisprudencia del TEDH[509], aborda la cuestión de la distinción entre la función informadora que llevan a cabo los medios de comunicación en una sociedad democrática cuando difunden noticias actuales y la función que juegan cuando gestionan y publican una hemeroteca digital. Para el Tribunal Supremo, ambas funciones son distintas y deben tratarse de modo diferente.

Como recoge la sentencia del Tribunal Europeo de Derechos Humanos, el Tribunal Supremo ha considerado que, mientras que la actividad de los medios de comunicación cuando transmiten noticias de actualidad es la función principal de la prensa en una democracia (la de actuar como un "perro guardián", en palabras de ese Tribunal), el mantenimiento y puesta a disposición del público de las hemerotecas digitales, con archivos que contienen noticias que ya se han publicado, ha de considerarse como una función secundaria, en la que el margen de apreciación de que disponen los Estados para lograr el equilibrio entre derechos es mayor, puesto que el

[508]Sentencia de la Sala de lo Civil del Tribunal Supremo de 15 de octubre de 2015, FJ 6.3.
[509] STEDH de 10 de marzo de 2009, caso Times Newpapers Ltd contra Reino Unido, párrafo 45; STEDH de 16 de julio de 2003, caso Wegrzynowski y Smolczewski contra Polonia, párrafo 59, y STEDH de 5 de mayo de 2011, caso Equipo Editorial de Pravoye Delo y Shtekel contra Ucrania, párrafo 63.

ejercicio de la libertad de información puede considerarse menos intenso. El riesgo de provocar daños en el derecho al respeto de la vida privada que representa el contenido y las comunicaciones en Internet es sin duda mayor que el que se deriva de la prensa escrita.

Por consiguiente, según el Tribunal Supremo, el tratamiento de los datos personales realizado por los motores de búsqueda generalistas que provoque que, cuando se utilicen como palabras clave el nombre y los apellidos de los afectados, aparezcan como resultados destacados los vínculos a las páginas de la hemeroteca digital que en su día fueron noticia, irá perdiendo su justificación a medida que transcurra el tiempo, si las personas implicadas carecen de relevancia pública y los hechos vinculados a esas personas carecen de interés histórico.

En el caso de autos, la publicidad general y permanente de la implicación de las demandantes en sucesos ocurridos hacía más de veinte años supuso un daño desproporcionado para su honor, al vincular sus datos personales con unos hechos que afectaban seriamente a su reputación y a su intimidad, puesto que hacían pública la drogodependencia que habían padecido en el pasado. El tratamiento de esos datos personales podía ser veraz, pero el paso del tiempo lo había transformado en inadecuado, no pertinente y excesivo para la finalidad del mismo.

Avanzando un paso más en relación con lo aclarado por el Tribunal de Justicia de la Unión Europa en la Sentencia del caso Google, nuestro Tribunal Supremo viene a perfilar el llamado derecho al olvido digital, definiéndolo como una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento, que garantiza que, cuando el afectado no tenga la

consideración de personaje público, pueda oponerse al tratamiento de sus datos personales, dirigiéndose, como en este caso, contra el editor de la página web que gestione la hemeroteca digital, el cual estará obligado a utilizar “protocolos de exclusión” para evitar que las noticias antiguas pueden ser indexadas por buscadores generalistas cuando la información carezca de interés público. Tal medida es el resultado de ponderar el derecho de cancelación que la normativa de protección de datos atribuye a los afectados por un tratamiento de datos personales que no reúna los requisitos de calidad con la libertad de información que ampara a las hemerotecas digitales en Internet.

Ahora bien, lo que deja claro la sentencia es que los editores de la página web no están obligados a modificar la noticia de la hemeroteca, ya que las hemerotecas digitales gozan de la protección de la libertad de información, al satisfacer un interés público en el acceso a la información y estar protegidas por el artículo 20 de la Constitución y el artículo 10 del Convenio de Derechos Humanos. El llamado "derecho al olvido digital" no puede suponer una censura retrospectiva de las informaciones correctamente publicadas en su día.

Tampoco están aquellos obligados a adoptar medidas técnicas tendentes a desindexar los datos de carácter personal de sus buscadores internos. Como dice la sentencia, "el riesgo para los derechos de la personalidad de las personas afectadas por la información guardada en la hemeroteca digital no radica tanto en que la información sea accesible a través del motor de búsqueda interno del sitio web en que se encuentra alojada, pues se trata de una búsqueda comparable a la que efectuaban quienes acudían a las viejas hemerotecas en papel, como en la multiplicación de la publicidad que

generan los motores de búsqueda de Internet, y en la posibilidad de que mediante una simple consulta utilizando los datos personales, cualquier internauta pueda obtener un perfil completo de la persona afectada en el que aparezcan informaciones obsoletas sobre hechos ya remotos en la trayectoria vital del afectado, con un grave potencial dañoso para su honor y su intimidad, que tengan un efecto distorsionador de la percepción que de esta persona tengan los demás conciudadanos y le estigmatice. Es por eso que esa información debe resultar invisible para la audiencia general de los usuarios de los motores de búsqueda, pero no para la audiencia más activa en la búsqueda de información, que debe tener la posibilidad de acceder a las noticias en su integridad a través del sitio web de la hemeroteca digital".

La sentencia crea, por tanto, una enorme diferencia entre la obtención de información específica acudiendo al buscador de una hemeroteca digital y la averiguación de un perfil completo que cualquiera pueda obtener en un buscador de Internet con tan solo introducir el nombre de una persona. La supresión de la primera posibilidad "supone un daño desproporcionado para la libertad de información que ampara a las hemerotecas digitales".

El derecho al olvido digital no ampara en ningún caso que cada uno construya su pasado a su medida. No permite reescribir las noticias, ni impedir de modo absoluto que en una búsqueda específica en la hemeroteca digital pueda obtenerse una información vinculada a los afectados. Lo que permite este derecho es la "oscuridad práctica", en palabras del Tribunal Supremo de los Estados Unidos[510], lo que, según explica nuestro Tribunal Supremo,

[510] Tribunal Supremo de los Estados Unidos (caso *U.S. Department of Justice v. Reporters Committee*, 109 S.Ct. 1468 (1989).

consiste en evitar que con una simple búsqueda en Internet pueda accederse al perfil completo de la persona, incluyendo informaciones obsoletas y gravemente perjudiciales para su reputación y su vida privada. Lógicamente, este derecho solo se da cuando el afectado no sea personaje público, no exista un interés histórico en la noticia y estén afectados los derechos de la personalidad.

A la vista de este pronunciamiento podemos extraer algunos principios sobre el conflicto entre el derecho al olvido digital y la libertad de información. El tratamiento de datos que se lleva a cabo en las hemerotecas digitales está amparado por la libertad de información. A tales efectos, el medio de comunicación, en los términos del artículo 20 CE, está legitimado para mantener la información inalterada, sin borrarla ni anonimizarla, ni en la página web ni en su hemeroteca. No obstante, hay que tener en cuenta que el factor tiempo y la divulgación de las informaciones periodísticas del pasado a través de los motores de búsqueda de Internet pueden ser lesivos para la intimidad y reputación del afectado, por lo que se impone la ponderación de la libertad de información y el derecho fundamental a la protección de datos.

Por lo tanto, independientemente de la posibilidad del ejercicio del derecho de oposición frente al tratamiento de datos que llevan a cabo los buscadores generalistas, que no son medios de comunicación y cuya actividad no se apoya en la libertad de información sino en la libertad de empresa, como ya quedó resuelto por la sentencia Google, el problema que plantea la sentencia del Tribunal Supremo examinada es si el derecho al olvido digital ampara el ejercicio por el afectado de un derecho de oposición contra el editor

de la página web sustentado en razones legítimas vinculadas a su situación personal.

Como señala Brotons Molina, quien edita una página web no solo debe ser responsable por el contenido de la misma sino también por las consecuencias y alcance de facilitar su difusión en Internet. Cualquier empresa con presencia en la red, incluidos los medios de comunicación, desea fomentar el tráfico que la actividad de los buscadores genera para sus páginas web; este tráfico supone un beneficio empresarial, tanto directo como indirecto (ingresos por publicidad). No parece descabellado concluir, por tanto, que si estas empresas atraen y reclaman tales ingresos, también se les debe reclamar una cuota de responsabilidad por la difusión exponencial de datos personales que se produce, efectivamente, cuando permiten la indexación de sus páginas web en los resultados de uno o varios motores de búsqueda. Suponer lo contrario, cuando la propia tecnología permite a estas empresas graduar el alcance de la permanencia y exposición de los datos en la red, nos conduciría a una tierra de nadie jurídica en la que los datos personales flotan y se difunden por Internet, lastrando nuestra vida personal y familiar y coartando nuestro derecho a una identidad en constante evolución, en consonancia con nuestra existencia *off-line*[511].

Para el Tribunal Supremo, cabría el derecho de oposición contra el editor de la página web, cuyos efectos, dada la excepción periodística, se limitarían a introducir “protocolos de exclusión”, es decir, el cese en la divulgación, para

[511] BROTONS MOLINA, O.: "Caso Google: tratamiento de datos y derecho al olvido. Análisis de las Conclusiones del Abogado General, asunto C-131/12", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 33, 2013.

evitar que las noticias sobre el pasado penal puedan ser indexadas por los motores de búsqueda, pues este último tratamiento de datos, debido al tiempo transcurrido sería inadecuado, no pertinente y excesivo, es decir, desproporcionado para los derechos de la personalidad del afectado.

El Tribunal Supremo, siguiendo la doctrina del Tribunal Europeo de Derechos Humanos, ha distinguido la función que cumplen las hemerotecas digitales de la que llevan a cabo los medios de comunicación. La función primaria de garantizar la existencia de una opinión publica libre en un Estado democrático es propia de los medios de comunicación, mientras que la que persiguen las hemerotecas digitales es secundaria y consiste en mantener y hacer accesibles al público los archivos de noticias previamente publicadas, teniendo, en ocasiones, un interés histórico. En caso de colisión con otros bienes o derechos constitucionales, no cabe duda de que el nivel de protección es inferior que si se tratara de un medio de comunicación.

Lo cierto es que, como venimos afirmando a lo largo del presente trabajo, el tratamiento de los datos personales debe cumplir con el principio de calidad de los datos no solo en el momento inicial, sino durante todo el tiempo que se produce ese tratamiento. Sobre estas premisas, los datos tratados deben ser los estrictamente necesarios para alcanzar la finalidad a la que sirve el tratamiento y este solo puede prolongarse durante el tiempo estrictamente indispensable para la satisfacción de dicha finalidad. Por tanto, a la luz del derecho fundamental a la protección de datos, y más concretamente del principio de calidad, habría que analizar hasta qué punto el tratamiento de datos que llevan a cabo las hemerotecas digitales es adecuado, necesario y proporcionado. En el asunto *Google* hay autores que sostienen que no debió

haber existido impedimento legal alguno ni para la cancelación de la publicación del anuncio de la subasta en la versión digitalizada del medio de comunicación, ni para la obstaculización de su indexación por los motores de búsqueda, ya que el argumento de que la publicación del anuncio de la subasta en La Vanguardia estaba amparado en la obligación legal de garantizar la máxima difusión posible de la misma había dejado de ser válido a partir del momento de su celebración, y el mantenimiento del anuncio no respondía a finalidad alguna[512].

En el asunto objeto de la sentencia del Tribunal Supremo que estamos comentando, la respuesta no es tan clara. La finalidad del tratamiento de los datos personales en los años ochenta estaba avalada por la libertad de información, pues tenía por objeto la transmisión de hechos que gozaban de trascendencia pública, esto es eran noticiables. El Tribunal Constitucional ha afirmado que los sucesos delictivos son noticiables por su propia naturaleza, con independencia de la condición de sujeto privado de la persona o personas afectadas por la noticia[513]. Y no cabe duda de que las hemerotecas digitales gozan de la protección de la libertad de información, al satisfacer un interés público en el acceso a la información. En cambio, es discutible si el tratamiento de datos consistente en la digitalización de una información previamente publicada que afecta a hechos que en su día fueron ciertos, relevantes y noticiables -la condena penal- debe prevalecer sobre el derecho al olvido del condenado. El carácter indeleble de Internet lo hace difícilmente compatible con la reinserción social y el libre desarrollo de la personalidad del delincuente.

[512] En este sentido se pronuncian Rallo Lombarte y Brotons Molina. RALLO LOMBARTE, A.: *op. cit.*, pág. 242 y BROTONS MOLINA, O.: art. cit.
[513] SSTC 178/1993, FJ 4; 320/1994, FJ 5; 154/1999, FJ 4.

En este supuesto, los demandantes no eran personajes públicos. Asimismo, los hechos objeto de la información carecían de interés histórico y, aunque habían tenido lugar hacía más de veinte años y ciertamente eran veraces, la licitud del tratamiento no exige solamente su veracidad, sino también su adecuación, pertinencia y carácter no excesivo en relación con el ámbito y finalidad para la que se haya realizado el tratamiento.

Cotino Hueso entiende que las hemerotecas digitales no son un medio de comunicación en sentido estricto, esto es, no deberían tener la consideración de fuentes de acceso público de acuerdo con el artículo 3.j) LOPD, sino que son ficheros que dan un tratamiento a fuentes accesibles al público que proceden de los medios de comunicación. De esta manera, los afectados tendrían derecho a cancelar también los datos personales que se incluyen en los servicios de búsqueda de las hemerotecas digitales[514]. Por el contrario, Marc Carrillo cree que sería paradójico que "una información de interés público y obtenida con escrupuloso respeto al canon de la diligencia profesional se pueda consultar en la hemeroteca de la edición escrita de un diario y, por el contrario, haya de desaparecer de la edición digital"[515].

Para Berrocal Lanzarot, en la línea de las sentencias del Juzgado de Primera Instancia y de la Audiencia Provincial dictadas en el asunto que

---

[514] COTINO HUESO, L.: "Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público (Art. 3 de la LOPD)", en TRONCOSO REIGADA, A. (dir.): *Comentario a la Ley Orgánica de Protección de Datos Personales*, Civitas, Cizur Menor, 2010, págs. 298 y 299. También vid, COTINO HUESO, L.: "La colisión del derecho a la protección de datos personales y las libertades informativas en la red: pautas generales y particulares de solución", en COTINO HUESO, L (editor).: *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*, Publicaciones de la Universidad de Valencia, Valencia, 2011, pág. 399. Disponible en Internet: http://www. derec hotics.com/congresos/2010-libertades-y-20/e-libro-elibertades-2010.

[515] CARRILLO, M.: "El derecho al olvido en Internet", *El País*, 23 de octubre de 2009, disponible en Internet: http://bit.ly/2srRjO

venimos comentando, podría obligarse a Ediciones el País a cesar en el uso de los datos personales en el código fuente de la página web que contenía la noticia relativa a la persona afectada "sin que pueda constar ni sus nombres ni apellidos ni sus iniciales", y a no mencionar los datos identificativos de las personas demandantes, ni sus nombres, apellidos o sus iniciales, en la noticia que pudiera publicarse sobre el proceso. La finalidad de la información cuando se publicó la noticia en los años ochenta en la edición en papel del diario se justificaba por la libertad de información; ahora, para esta autora, la falta de interés público de la noticia y la falta de relevancia pública de las personas demandantes y, por ende, la falta de finalidad periodística de la inclusión de la noticia en la hemeroteca digital de El País, justificaría el borrado o hacer anónimos los datos personales conforme a lo establecido en el artículo 17 del RGPD, o, en todo caso, la adopción de medidas de no indexación[516].

Para Di Pizzo Chiacchio[517], el fallo del Tribunal Supremo merece varios reproches. En primer lugar, el Pleno asume que existe una diferencia entre los motores de búsqueda de Internet externos e internos y equipara la consulta efectuada en estos últimos a la que podía realizarse en una hemeroteca en papel. Sin embargo, en las hemerotecas tradicionales no es posible efectuar una búsqueda a partir de los datos personales.

En segundo lugar, el Tribunal Supremo estima que el riesgo para los derechos de la personalidad proviene, sobre todo, de la consulta en los motores de búsqueda externos, por lo que considera legítimo imponer al

[516] BERROCAL LANZAROT, A.I.: *Derecho de supresión de datos o derecho al olvido*, Reus, Madrid, 2017, págs. 192-193.
[517] DI PIZZO CHIACCHIO, A.: art. cit., págs. 951-952.

afectado la tolerancia del daño "minoritario" que pueda provocarle la búsqueda de información en un motor de búsqueda interno.

Por tanto, considera este autor que, si se implementase la desindexación en el motor de búsqueda en Internet interno, la información en la hemeroteca digital continuaría siendo accesible de cualquier modo, pero su localización se restringiría a parámetros de búsqueda ajenos a los datos personales de los interesados. En tal sentido, afirma que la libertad de información del editor no debería amparar la consulta de información de una persona física a partir de sus datos personales si dicha información ya no cumple el principio de calidad de los datos y si los derechos de la personalidad resultasen lesionados, con indiferencia de la tipología del motor de búsqueda de Internet -externo o interno- utilizado en la consulta[518].

Por su parte el Grupo de Trabajo sobre Protección de Datos del artículo 29 expuso que "los motores de búsqueda incluidos en las páginas web no producen los mismos efectos que los motores de búsqueda 'externos'. Por un lado solo recuperan la información contenida en páginas web específicas. Por otro lado, incluso si un usuario busca a la misma persona en varias páginas web, los motores de búsqueda no establecerán un perfil completo del individuo afectado y los resultados no tendrán un impacto serio en él. Por lo tanto, como regla general el derecho de desindexación no debe aplicarse a los motores de

[518] *Ibidem,* pág. 88. En el mismo sentido, Troncoso Reigada, para quien es muy discutible que una persona que no tenga relevancia pública o cuando no exista un claro interés público tenga que asumir la injerencia en la privacidad que representan los motores de búsqueda de la propia hemeroteca digital. Según este autor "no estamos negando la buscabilidad de la información en virtud de materias; únicamente estamos limitando la injerencia en la privacidad que suponen los tratamientos de datos personales que permitan rápidas consultas a través de los motores de búsqueda de la propia web utilizando como palabras clave los datos personales." *Vid.* TRONCOSO REIGADA, A.: "El derecho al olvido digital de los médicos a la luz de la sentencia del Tribunal Supremo de 15 de octubre de 2015", *I+S Informática y salud*, núm. 114, 2015, pág. 68.

búsqueda con un campo de acción restringido particularmente en el caso de las herramientas de búsqueda de las páginas web de los periódicos"[519].

Hechas las consideraciones anteriores, lo cierto es que, partiendo de la doctrina del TEDH, el interés legítimo del público en el acceso a los archivos de las hemerotecas digitales está protegido por el artículo 10 de la CEDH.

La integridad de los archivos digitales es un bien jurídico protegido por la libertad de expresión en sentido amplio y, por ello, no corresponde a las autoridades judiciales reescribir la historia ordenando la eliminación del dominio público de todo rastro de publicaciones que en el pasado se hayan divulgado, aunque supongan ataques injustificados a la reputación de los individuos[520].

El pasado penal no puede ser objeto de cancelación o borrado. No obstante, no cabe duda de que el paso del tiempo puede producir que un tratamiento de datos que era inicialmente lícito en su origen, resulte inadecuado y desproporcionado por su contenido distorsionador de la imagen de la persona que ha visto cancelados sus antecedentes penales y rehecho su vida. El riesgo para el derecho al olvido no es que la información sea accesible a través de la página web del medio de comunicación, a través del buscador interno de la hemeroteca digital. El peligro es el efecto multiplicador de la noticia obsoleta que generan los motores de búsqueda generalista, que puede llevar a la estigmatización social de la persona. Por lo tanto, comparto la posición del Tribunal Supremo de que una justa ponderación entre el derecho de cancelación de datos y la libertad de información debe permitir un ejercicio

[519] Grupo de Trabajo sobre Protección de datos del Artículo 29, *Guidelines on the implementation of the Court of Justice of the European Union judgment on Google Spain and Inc. v. Agencia Española de Protección de Datos an Mario Costeja González*, pág. 8. Disponible en Internet:http://ec.europa.eu/justice/data-protection/article-29/documentation /opinion-recommendation /files/2014/wp225_en.pdf

[520] STEDH 16 de Julio de 2013, caso Wegrzynowski y Smolczewski contra. Polonia, párrafo 65.

del derecho de oposición frente al editor de la página web que lo obligue a instalar códigos que impidan la indexación por los motores de búsqueda generalistas, pues, en definitiva, lo que se pretende es evitar el tratamiento de estos datos personales por cualquier motor de búsqueda generalista, es decir, prevenir que en el futuro no se pueda volver a acceder a la página web fuente desde cualquier buscador generalista introduciendo el nombre y apellidos de la persona. Todo lo dicho, sin perjuicio de que también hay que reconocer que en este supuesto el tratamiento de datos personales que lleva a cabo la hemeroteca digital, aunque lícito, es inexacto y obsoleto. Por tanto, en este caso, lo que habría procedido es que las demandantes hubieran ejercitado el derecho rectificación de los datos personales ante la inexactitud sobrevenida de la información, que podría consistir, como señala el artículo 16 RGPD, en una declaración adicional que aludiera a la cancelación de sus antecedentes penales[521].

Más recientemente el problema que plantean las hemerotecas digitales ha tenido su reflejo en la sentencia del Tribunal Supremo de 6 de julio de

[521] Según doctrina jurisprudencial italiana, concretamente la sentencia de la Corte de Casación de 5 de abril, el volcado de la noticia en Internet constituye un tratamiento de datos y debe preservarse la exactitud de estos, esto es, debe garantizarse que "han sido debidamente actualizados a la luz de la evolución posterior de los hechos en la noticia original". Garantizar la exactitud de los datos no solo garantiza el derecho del afectado por la noticia, sino también el derecho de los ciudadanos a recibir una completa y correcta información. Frente a esta tesis, el Tribunal Supremo alemán, para el que la publicidad de una hemeroteca es puramente pasiva, la libertad de expresión garantiza el mantenimiento de este tipo de archivos. Rechaza este Tribunal que pueda imponerse un deber de controlar la corrección actual de las noticias pasadas, porque constituiría una limitación inadmisible de la libertad de expresión (BGH, sentencia de 15 de diciembre de 1999, VI ZR 227/08, par. 21). El alcance del deber de diligencia de los medios de comunicación de acuerdo con la jurisprudencia del TEDH, se ha afirmado en relación con informaciones que habían dado lugar a procedimientos judiciales, exigiendo que en la noticia accesible en la hemeroteca se advirtiera de la existencia del carácter litigioso de la información. *Vid.* MIERES MIERES, L. J.: *op. cit*., págs. 34-36. Disponible en. Internet.: http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo =attach&db=snciv&id=./20120410/snciv@s30@a2012@n05525@tS.clean.pdf

2017[522]. La pretensión de ejercicio del derecho al olvido, en este caso, se basaba en que, al teclear en los buscadores generalistas un crimen ocurrido en una determinada población, la lista de resultados traía a colación la página web del periódico que ilustraba la información escrita con la fotografía del recurrente tomada lícitamente en la Sala donde se celebraba el juicio en el que fue absuelto de la acusación de doble asesinato. El recurrente solicitaba que se retirara la información litigiosa, incluyendo su imagen, de todos los archivos informáticos que la pudieran alojar, también en buscadores y redes sociales. En el recurso de casación, expresamente, se pedía que se prohibiera la indexación de la noticia por los motores de búsqueda.

La sentencias dictadas en primera instancia y en apelación desestimaron la demanda para la tutela civil de los derechos fundamentales al honor y a la propia imagen frente al periódico Levante-EMV (Levante-EMV.com) y contra los periodistas por la publicación del artículo en el que se recogía la información de la absolución del acusado, sin mencionar su nombre y apellidos, acompañada de una fotografía. La noticia era veraz, al limitarse a describir los acontecimientos sin incluir juicios de valor, y la imagen también, al haber sido captada con autorización del Tribunal en la sala de vistas. Además, aquella ilustraba una información de innegable interés general, como era la celebración de un juicio oral ante un jurado popular en el que el demandante intervenía como acusado por graves delitos.

La Sala Primera del Tribunal Supremo considera que la actuación de los demandados estuvo amparada en la libertad de información. Para el Tribunal

[522] Sentencia del Tribunal Supremo (Sala de lo Civil, Sección 1ª), de 6 de julio de 2017. Y, en el mismo sentido, la sentencia de la Sala de lo Civil del Tribunal Supremo de 13 de julio de 2017, en este caso contra el diario 20 minutos.

Supremo, en el caso objeto del recurso, la información escrita y gráfica publicada tenía indudable interés general, no tanto por la persona concernida, sino por razón de la materia, dado que venía referida al enjuiciamiento por el tribunal del jurado de unos hechos de extraordinaria gravedad e impacto social, que constituían un doble asesinato. Se trataba de una información que seguía siendo de actualidad en aquel momento, aunque el crimen se hubiera cometido quince años antes, porque el objeto de la noticia era el acto del juicio oral celebrado contra el segundo de los acusados una vez localizado, extraditado y puesto a disposición de los tribunales españoles[523]. Fue el interés informativo del juicio lo que motivó que el gabinete de prensa del Tribunal Superior de Justicia de la Comunidad Valenciana avisara a los medios de comunicación del señalamiento del juicio oral y se permitiera hacer fotos en el interior de la sala de vistas al comienzo del juicio.

El Tribunal Supremo tiene en cuenta que la regla constitucional de la veracidad ampara las informaciones sobre imputaciones de hechos delictivos que finalmente no queden probados[524]. En este caso el periódico había ofrecido, pues, una información veraz, basada en fuentes objetivas y fiables y en los datos que las mismas proporcionaban en el momento en que la noticia se produjo[525]. El Tribunal Supremo apreció que todas las referencias al caso estaban justificadas en la intención de ofrecer una información completa y

[523] El primero de los dos acusados, que no huyó, ya había sido juzgado por estos mismos hechos y absuelto en el año 1999.

[524]Sentencia del Tribunal Supremo (Sala de lo Civil) de 8 de mayo de 2015, sentencia del Tribunal Supremo (Sala de lo Civil) de 20 de mayo de 2016 y SSTC 258/2015 y 337/2016.

[525] La información se publicó precedida del titular "absuelto un acusado de un doble crimen tras destruir la Audiencia las pruebas" y del subtítulo "la fiscalía muestra su convicción en la culpabilidad del acusado, para el que pedía 50 años de cárcel y lamenta la carencia de evidencias al no aparecer tampoco un testigo de cargo. El TSJ resta importancia a la destrucción de las piezas de convicción".

adecuada sobre los hechos y debían considerarse razonables. En conclusión, no hubo intromisión ilegítima en el derecho al honor del demandante, puesto que la información fue veraz, versó sobre una cuestión de interés público y no se emplearon expresiones innecesariamente ofensivas para el demandante[526]. Y lo mismo podía concluirse respecto a la información gráfica, por lo que no se apreció vulneración del derecho a la propia imagen.

En relación con el derecho al olvido digital, el Tribunal Supremo viene a aclarar que la pretensión formulada no tiene encaje en este derecho, tal y como se ha ido construyendo en su reciente jurisprudencia. El principal obstáculo para reconocer en este caso el derecho al olvido digital, como concreción del derecho fundamental a la protección de datos de carácter personal, que protege instrumentalmente los derechos de la personalidad, es que la noticia original omitió el uso del nombre y apellidos para referirse al demandante. Por lo tanto, no cabía alegar que, al teclear en el buscador generalista tales datos personales, los motores de búsqueda pudieran indexar la noticia sobre la acusación de doble crimen del que finalmente el recurrente fue absuelto. No obstante, hay que recordar que el problema era que, al llevar a cabo la búsqueda utilizando como palabras clave los crímenes de aquella localidad, el buscador indexaba la información aludida, en la que aparecía la imagen del recurrente, menoscabando lógicamente la presunción de inocencia del afectado.

Hecha la observación anterior, está fuera de toda duda que el derecho al olvido digital no autoriza para borrar el pasado que no nos complace ni para censurar el ejercicio de la libertad de información. Por tanto, la solicitud de

[526]Sentencia del Tribunal Supremo (Sala de lo Civil, Sección 1ª), de 6 de julio de 2017, FJ 3.

eliminar los archivos informáticos que alojaban dicha información, tanto escrita como gráfica, no solo de la hemeroteca digital del periódico y de su página web, sino también de los buscadores de Internet, estaba, para el Tribunal Supremo, absolutamente fuera de lugar.

El Tribunal Supremo, aplicando la doctrina expuesta en su sentencia de 2015, estudiada anteriormente, determina que el tratamiento de datos personales que puede dar lugar al ejercicio del olvido digital es el que llevan a cabo las hemerotecas digitales de los periódicos. Y, en tal caso, solo procede el derecho de oposición si se demuestra que, tiempo después de que se publicara la información original, el periódico editor de la página web permite que la misma continúe estando accesible indiscriminadamente, mediante su indexado y tratamiento por los motores de búsqueda generalistas, con la utilización en estos, como términos clave, de los datos personales del afectado (como el nombre y los apellidos), al no haber introducido instrucciones en el código fuente de la página web destinadas a impedir la indexación de la información contenida en ella. Sin embargo, al haber omitido la noticia el nombre y apellidos del afectado, en el caso, no era posible acceder a la noticia sobre la acusación de haber cometido un crimen, mediante una búsqueda en la que se utilizaran los datos personales del recurrente.

Ahora bien, como expresamente recuerda la Sala, la imagen de una persona es también un dato de carácter personal, según la normativa de protección de datos. Para el recurrente el tratamiento del dato gráfico era innecesario, y provocaba un daño a su reputación y su intimidad, ya que solo contribuía a incrementar la ofensa a su dignidad, al permitir que cualquier

persona lo pudiera reconocer por su apariencia física, a pesar de haber sido absuelto.

Por tanto, tiene sentido la discusión sobre si el derecho al olvido digital, en este caso, ampararía que el afectado pudiera ejercitar frente al editor de la página web, más que el derecho de cancelación, ya que el tratamiento de sus datos personales por el medio de comunicación es lícito, el derecho de oposición al tratamiento de su imagen, que le impondría al medio la obligación de utilizar los protocolos de exclusión, por resultar el tratamiento del dato gráfico, llevado a cabo por los motores de búsqueda, inadecuado, no pertinente y excesivo con la finalidad con que los datos fueron recogidos, que era la de informar sobre unos hechos de indudable interés público. La vinculación de los crímenes con la imagen del afectado a través de los buscadores podía, sin duda, causar un daño a la reputación y a la vida privada desproporcionado respecto al interés público de los hechos objeto de la noticia, que podían seguir consultándose en la hemeroteca digital de la página web del periódico. La cuestión, por tanto, es si podría reconocerse en este caso al afectado el derecho a la oscuridad digital.

En nuestra opinión, lo que trata de proteger el derecho al olvido digital del pasado penal es la formación por parte de los internautas de un perfil de la persona que pueda perjudicar el libre desarrollo de su personalidad y su reinserción social. Cuando se introduce el nombre y apellidos de una persona en un motor de búsqueda generalista, el internauta quiere conocer qué páginas de Internet se relacionan con ella. Pero cuando se introduce otro criterio de búsqueda, como, en este caso, un suceso de gran repercusión mediática, el internauta puede no ser consciente de que una imagen sin nombre y apellidos

que acompaña a la noticia puede servir para identificar a la persona a la que acompaña la información. Por consiguiente, entendemos que sería desproporcionado el derecho a exigir la desindexación de una página web cuando el criterio de búsqueda no es el nombre y los apellidos porque el interés del público general en conocer esa información debe prevalecer sobre el riesgo que para la persona supone la indexación de la noticia por parte del buscador[527].

En Internet, en definitiva, solo existe el derecho a que la información sea olvidada o, mejor dicho, desindexada cuando la búsqueda se lleve a cabo por el nombre y apellidos. En esta ocasión, como manifiesta el Tribunal Supremo, no se había demostrado que pudiera utilizarse como criterio de búsqueda una imagen, aunque la rapidez de los avances tecnológicos no harían esta posibilidad descartable a corto plazo. El derecho al olvido, como ha dicho el Tribunal Supremo, no implica que cada persona pueda construirse un pasado a su medida, haciendo que desaparezca información negativa sobre sí misma.

Por otra parte, en este caso, la información no había perdido relevancia a pesar de haber transcurrido los hechos quince años antes, porque formaba parte de una noticia actual, como era la celebración de un juicio en el que el acusado había sido absuelto. El transcurso del tiempo no había hecho que un tratamiento de datos inicialmente lícito se hubiera convertido en inadecuado, no pertinente o excesivo. Es el dato de la imagen, captada en la actualidad en el

[527] Según Pazos Castro impidiendo que los motores de búsqueda indexen la información, la clasifiquen y, sobre todo, la muestren, se pone un claro freno a los avances que supone internet y se obstaculiza el ejercicio de las libertades de expresión y de información. *Vid.* PAZOS CASTRO, R.: "El derecho al olvido frente a los editores de las hemerotecas digitales", *Indret,* núm. 4, 2016, pág. 24.

ejercicio de la libertad de información, la que ha resultado desproporcionada a juicio del recurrente.

Desde nuestro punto de vista, en el caso de autos, no resultaba justificado que el interesado buscara oscurecer informaciones actuales, porque la noticia se traía a colación de una realidad del presente, aunque aludiera a sucesos del pasado, y dotada de un interés público, vigente e indiscutible, dado que el recurrente, una vez localizado y extraditado tras su huida, había sido puesto a disposición de los tribunales españoles. Por consiguiente, faltarían los presupuestos del derecho al olvido digital, pues no estaríamos ante informaciones obsoletas y descontextualizadas, carentes de relevancia pública[528].

---

[528] Distinto es el supuesto resuelto por sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1ª) de 13 de julio de 2017. Aquí, el derecho al olvido digital se ejercita contra el motor de búsqueda y la Audiencia Nacional aprecia el dato del tiempo transcurrido y la falta de relevancia pública del sujeto implicado. Así, con fecha 7 de junio de 2014, aquel ejercitó frente a *Google Inc,* el derecho de cancelación/oposición en relación con sus datos que figuraban en dos enlaces a las páginas webs de dos diarios. En el primer enlace aparecían los datos del interesado en una noticia publicada en un diario el 6 de octubre de 1992, en referencia al inicio de un juicio contra el reclamante en su calidad de ginecólogo por haber dejado compresas en una paciente fallecida, tras una cesárea. En el segundo enlace aparecen los datos en una noticia publicada en otro diario el 5 de noviembre de 1992, que versa sobre su absolución del delito de homicidio del que estaba acusado en el denominado "caso de la compresa", condenándolo como autor de una falta de imprudencia con resultado de muerte a una pena de multa y a indemnizar al marido e hija de la fallecida. Google Inc le contestó el 27 de agosto de 2014 denegándole la solicitud, por considerar que las URLs en cuestión estaban relacionadas con asuntos de interés público en relación con su vida profesional. Por ejemplo, estas URLs podrían resultar de interés para sus actuales/potenciales clientes, usuarios o participantes en sus servicios. Interpuesta reclamación ante la AEPD, esta resolvió que, a pesar de que el tratamiento de los datos del interesado en los enlaces reclamados fue inicialmente lícito, procedía la exclusión de los datos personales del reclamante, al tratarse de datos obsoletos, dado que se trataba de un hecho del año 1988 por el que fue juzgado en el año 1992, Y accesibles a través de una búsqueda en Internet a partir del nombre de dicha persona. En el presente caso, la Audiencia Nacional, en aplicación de la doctrina establecida por la STJUE de 13 de mayo de 2014, y siguiendo la citada STS de 5 de abril de 2016, tomó en consideración la antigüedad de la información, publicada más de veinte años atrás, los hechos no revistieron carácter de delito y el carácter sensible de la información, y no apreciándose que el afectado fuera una persona de relevancia pública, la Sala consideró que debía prevalecer el derecho a la protección de datos del afectado. Es decir, a la vista de las concretas circunstancias del caso, el interesado ostenta el derecho a que esa información relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre en el citado buscador

2.2. El derecho al olvido digital y el principio de transparencia de la información pública.

El principio de transparencia de la información pública permite dar a conocer a la generalidad de los ciudadanos asuntos relacionados con la actividad de los poderes públicos, para fomentar el control de la gestión de la vida pública, con anclaje constitucional en el principio democrático. En palabras de Rodríguez Álvarez, este principio demanda una completa rendición de cuentas de los gobernantes ante la ciudadanía en relación con todas sus actuaciones con relevancia pública. A su vez, la información contenida en los documentos administrativos y, en general, toda la información en manos de los organismos públicos constituye una fuente de conocimiento de primera magnitud para la participación eficaz de los ciudadanos en los procesos democráticos[529].

La transparencia es esencial en un Estado de Derecho, para la formación de una opinión pública libre y para facilitar la participación activa de la sociedad en las decisiones políticas. Este principio, sin embargo, puede dar lugar a controversias en los casos en que su ejercicio entra en conflicto con derechos fundamentales.

---

en Internet, o, lo que es igual, a que se eliminen de la citada lista de resultados los vínculos a los citados enlaces objeto de reclamación. Importa destacar que el derecho a la información justifica su permanencia en la fuente, si bien no resulta justificado, dado el tiempo transcurrido, que aparezca en los resultados de un motor de búsqueda. Para Troncoso Reigada es importante que los medios de comunicación sean especialmente prudentes en los procesos judiciales en los que se ven inmersos los médicos, respetando la presunción de inocencia y dando una mayor publicidad a la sentencia que a la fase de instrucción. *Vid*. TRONCOSO REIGADA, A.: " El derecho al olvido digital de los médicos…", pág. 68.

[529] RODRÍGUEZ ÁLVAREZ, J. L.: *op. cit.,* págs. 53-54.

En tal sentido, la divulgación en el mundo digital por los poderes públicos de informaciones relativas a personas identificadas o identificables sin el consentimiento de los interesados, en virtud de la habilitación legal que faculta a las Administraciones Publicas para ello, puede afectar a los derechos fundamentales de los individuos relacionados con la esfera personal y el libre desarrollo de la personalidad, en particular al derecho fundamental a la protección de datos.

Como afirma Guichot Reina, cada tipo de publicación administrativa telemática entraña una gradación en los riesgos para la privacidad: no es lo mismo un tablón al que solo se tiene acceso mediante clave, que un tablón de acceso libre o un Boletín oficial. Esta última, de hecho, es, en su opinión, la modalidad de publicidad potencialmente más lesiva para el derecho de protección de datos, entre otras razones porque los Boletines se editan en formato electrónico de acceso libre y son susceptibles de indexación sin límite de tiempo, de modo que cualquier persona desde cualquier lugar y en cualquier momento puede acceder a la información personal que contengan con simplemente teclear el nombre de una persona en cualquier buscador[530]. Como es notorio, los datos personales que constan en los Boletines oficiales en su versión digital son fácilmente accesibles en Internet, tanto a través de los buscadores generalistas, como a través del mismo buscador del Boletín. Al ser fuente de acceso público, conforme al artículo 3. j LOPD, pueden ser tratados por terceros sin consentimiento del titular.

[530] GUICHOT REINA, E.: "La publicidad de datos personales en Internet por parte de las Administraciones Públicas…", págs. 142-143.

En el marco de las consideraciones anteriores, es evidente el interés público de la publicación de los indultos como manifestación del principio de transparencia. La publicación en el Boletín oficial del Estado de esta medida de gracia está prevista en una ley de casi ciento cincuenta años de antigüedad.

El problema de la publicidad de este tipo de información en Internet es que permanece ahí de por vida. Como afirma Troncoso, no parece adecuado mantener de manera permanente en Internet los datos de personas indultadas. La publicación en Internet de esta información, que es accesible a través de los distintos buscadores, hace que todo el pasado permanezca siempre como presente y acompañe a la persona el resto de su vida. Puede haber en su momento un interés público en la publicidad de esta información relativa a indultos, pero este interés no es permanente y desaparece con el paso del tiempo, lo que convierte a este tratamiento en excesivo.

No existe ninguna finalidad propia del Boletín oficial –distinta del interés público que exige la publicación y que está prevista en la legislación de cada procedimiento- que obligue a mantener de manera indefinida la publicidad de aquello que una vez ha sido publicado. La publicidad permanente supone una intromisión continuada en el derecho fundamental a la protección de datos personales y es, por tanto, una injerencia en el citado derecho fundamental que no respeta el principio de proporcionalidad[531]. Por consiguiente, el saber que una persona fue indultada y, por ende, cometió un delito, con simplemente teclear su nombre tiene, como señala Guichot Reina, un potencial tremendo de lesividad para el libre desarrollo de la personalidad y las posibilidades efectivas

[531] TRONCOSO REIGADA, A.: *La protección de datos personales. En busca*…, págs. 772 y 773.

de participación en la vida social, hasta el punto de que podría cuestionarse si en algunos casos puede ser preferible no ser indultado a serlo con conocimiento público, en la medida en que impide *de facto* la reinserción social[532].

Precisamente, el derecho al olvido digital en el supuesto de la concesión de un indulto fue tratado por la sentencia del Tribunal Supremo de 5 de abril de 2016[533]. El demandante había sido indultado por Real Decreto de 27 de agosto de 1999 de la pena privativa de libertad pendiente de cumplimiento a la que había sido condenado como autor de un delito contra la salud pública, por hechos cometidos en el año 1981. El citado Real Decreto se publicó en el BOE de 18 de septiembre de 1999, de conformidad con el artículo 30 de la Ley del Indulto de 1870, que impone la obligatoriedad de la publicación oficial de los indultos.

En el año 2009, el afectado afirmaba que, al realizar una consulta en Google a partir de su nombre y apellidos, el buscador le remitía en primer lugar a la página del BOE que informaba sobre su indulto. Por consiguiente, solicitó al BOE y a Google Spain la retirada de dicha página del buscador en cumplimiento de la LOPD[534.] Mientras que la segunda respondió con un mensaje estándar automatizado pidiéndole que se redirigiera a una web que ofrecía respuestas a preguntas frecuentes, el BOE le respondió afirmando

---

[532] GUICHOT REINA, E.: *op. cit.,* pág. 165.
[533] Sentencia del Tribunal Supremo (Sala de lo Civil, Sección Pleno) de 5 abril de 2016.
[534] También se dirigió a *Yahoo* por correo electrónico. Según su declaración, desde hacía años, cuando se insertaba su nombre en este buscador, aparecían varias páginas ilegales (no hacía referencia alguna a la página del BOE) en las cuales se informaba de su vida pasada, años 1981 y 1999, incumpliendo muchos artículos de la LOPD, lo que le perjudicaba en lo personal, familiar, laboral, económico y social, de manera desmesurada y en prácticamente todos los países del mundo, saliendo siempre en la primera página del buscador. Solicitaba que retiraran las páginas citadas del buscador y reclamaba una compensación.

haber adoptado las medidas a su alcance para evitar la automatización de sus datos personales, esto es, que eliminó su nombre y apellidos del buscador interno, de modo que no era posible ya acceder mediante su nombre al Real Decreto por el que se le indultó, a través de ninguno de los buscadores de la web del BOE[535]. Se añadía que, siguiendo indicaciones de la Agencia Española de Protección de Datos, los documentos en que aparecía el nombre del demandante habían sido incluidos en una lista de exclusión (robots.txt), para notificar a las empresas con buscadores en Internet que no debían utilizar esos datos, los cuales, en unos días, debían desaparecer de tales buscadores.

En el procedimiento ante la AEPD[536] sobre la reclamación del demandante contra BOE, *Google Spain* y *Yahoo Iberia*, la Agencia estimó el derecho de oposición ejercido contra *Google Spain* e instó a dicha entidad que adoptara las medidas necesarias para retirar los datos de su índice e imposibilitara el acceso futuro a los mismos. Al mismo tiempo, desestimó la reclamación formulada contra el BOE y estimó en parte la reclamación contra *Yahoo* Iberia, pues apreció como procedente la exclusión de los datos personales del reclamante de los índices elaborados por *Yahoo,* pero tuvo en cuenta que, durante la tramitación del procedimiento, ese buscador había arbitrado las medidas necesarias para evitar la indexación de los datos[537].

---

[535] Exponía que la página electrónica del BOE reproduce fielmente la edición en papel, por lo que cualquier modificación sobre la página significaría una manipulación sustancial del contenido que alteraría de forma grave una "fuente de acceso público" (cualidad que tiene el BOE conforme al art. 3.j de la LOPD), y debido a ello no procedía la modificación de datos del propio Boletín.

[536] TD/00921/2009 Resolución R/02694/2009.

[537] El demandante reclamó también ante la AEPD contra *Lycos España Internet Services*, SL y contra Telefónica de España, S.A.U. (Terra), por no haber sido debidamente atendido su derecho de cancelación. En el procedimiento TD/00326/2010, se dictó la resolución R/01553/2010, en la cual la Agencia estimó por motivos formales la reclamación contra Telefónica, aunque decidió que no procedía que dicha entidad emitiera una nueva certificación,

El afectado presentó posteriormente una demanda civil por vulneración de los derechos a la intimidad, al honor y a la propia imagen, contra el responsable del motor de búsqueda en Internet, aunque no contra el editor de la página web en la que se contenían los datos.

Por lo que afecta al derecho fundamental a la protección de datos, el Juzgado de Primera Instancia estimó que los buscadores demandados no eran responsables de los daños y perjuicios derivados del acceso al contenido del BOE hasta la notificación y firmeza de las resoluciones de la AEPD.

En la sentencia dictada en apelación[538], la Audiencia Provincial estima que el núcleo de la controversia lo constituye la responsabilidad de los buscadores por el daño causado mediante la vulneración del derecho a la protección de datos. Recogiendo la doctrina emanada de la STJUE de 13 de mayo de 2014, caso *Google*, consideró que el enlace al BOE que publicaba el indulto no se ajustaba a los principios que rigen el tratamiento de los datos personales. Contra dicha resolución de la Audiencia Provincial recurrieron en casación tanto el demandante como *Google Spain*.

En el recurso[539], *Google Spain* defendió sus posiciones sobre la base de la necesaria ponderación entre el derecho a la protección de datos y el derecho a la información derivado del artículo 20.1 CE.

---

al haber quedado acreditado que había cancelado los datos del reclamante fuera del plazo establecido legalmente, y desestimó la reclamación contra *Lycos*, porque no constaba la recepción por esta empresa de la solicitud del demandante y porque no existía información acerca del administrador de la empresa en España.

[538] Sentencia de la Audiencia Provincial de Barcelona (sección 16ª), de 17 de julio de 2014.

[539] En relación con los motivos formales del recurso, el Tribunal Supremo (Sala de lo Civil) entiende que *Google Spain* es responsable del tratamiento de los datos que realiza el buscador *Google Search* en su versión española, conjuntamente con su matriz *Google Inc,* y ,en consecuencia, está legitimada pasivamente como demandada en los litigios promovidos en España por afectados que ejerciten en un proceso civil sus derechos de acceso, rectificación, cancelación y oposición. Según el fundamento jurídico 3º, 2: “una solución en sentido contrario

De acuerdo con su argumentación, la publicación del indulto en el BOE viene impuesta por la ley. Al tratarse de una fuente de acceso público, la indexación de los datos personales del demandante por parte de *Google* no necesitaría su consentimiento, sería lícita y, por tanto, el afectado no podría oponerse al tratamiento automatizado que supone la indexación de sus datos personales asociados a la concesión del indulto y su comunicación a los internautas que realicen búsquedas utilizando su nombre y sus apellidos.

Para *Google* el derecho al olvido no es un derecho ilimitado, sino que debería ceder ante el interés preponderante del público de tener acceso a la información que se pretende borrar. En este caso, subraya que los indultos concedidos por el gobierno gozan de un interés general y los ciudadanos tienen derecho a conocerlos como elemento imprescindible de la democracia. La publicación en el BOE de un indulto, por la comisión de un delito relacionado con el tráfico de drogas, tiene, destaca *Google,* relevancia pública. Ante la falta

---

supondría debilitar la protección de los derechos de las personas físicas, en particular, del derecho a la intimidad en lo que respecta al tratamiento de los datos personales". Esta sentencia vino precedida días antes por la sentencia del Tribunal Supremo (Sala de lo contencioso-Administrativo) de 14 de marzo de 2016, que interpretó de manera expresamente contradictoria el concepto de tratamiento de datos personales sin plantear una cuestión prejudicial al Tribunal de Justicia de la Unión Europea, sino basándose en la sentencia del caso *Google*. Esta cuestión ha quedado definitivamente zanjada por el artículo 3 del RGPD, que trata de superar los problemas de aplicación territorial del Derecho de la Unión Europea, y el artículo 79 RGPD sobre jurisdicción aplicable. *Vid.* DE MIGUEL ASENSIO, P. A.: "La contradictoria doctrina del Tribunal Supremo acerca del responsable del tratamiento de datos por el buscador Google", *La Ley unión Europea*, núm. 37, 2016. Por su parte, Di Pizzo hace referencia a un conjunto de sentencias del Tribunal Supremo (Sala de lo Contencioso-Administrativo) de junio y julio de 2016 que fallan a favor de *Google Spain,* afirmando que no existe corresponsabilidad en el tratamiento de datos entre *Google Spain* y *Google Inc,* que la inexistencia de la condición de responsable determina la falta de legitimación pasiva de *Google* y que la legitimación pasiva de *Google Inc* no comporta una carga procesal desmedida para el afectado. Esto, como afirma el autor fomentará una falta de seguridad jurídica en la tutela del derecho al olvido digital. DI PIZZO CHIACCHIO, A.: art. cit., págs. 964-970. En este sentido, Murga Fernández para quien sería deseable que esta disparidad de criterios que puede constatarse en las Salas Primera y Tercera del Tribunal Supremo se superara, pues así lo exige la seguridad jurídica, cual principio rector del ordenamiento jurídico ex artículo 9.3 CE, para el que resulta más convincente y coherente con los planteamientos del Tribunal de Justicia de la Unión Europea la doctrina sentada por la Sala Primera. *Vid.* MURGA FERNÁNDEZ, J. P.: *op. cit.*, pág. 198.

de motivación de esta medida de gracia, los ciudadanos tienen derecho a indagar cuáles son los motivos que pueden haber influido en la condonación por el Gobierno de una pena impuesta por el poder judicial. En este caso, el reconocimiento del derecho al olvido conllevaría un riesgo claro de censura y una vulneración del principio de transparencia de los poderes públicos que debe regir en todo Estado democrático de Derecho. El hecho de que en ocasiones esa publicidad pueda trascender al conocimiento público, porque aparezca en buscadores de Internet, como es el caso, constituye un daño que el perjudicado por ese hecho estaría, en opinión de la entidad recurrente, obligado a soportar en todo caso.

El Tribunal Supremo, sobre base de la doctrina sentada por la sentencia del Tribunal de Justicia de la Unión Europea del caso *Google*, considera en su sentencia que la actuación del motor de búsqueda *Google* debe calificarse de tratamiento de datos personales, pues “recoge” datos que “extrae”, “registra” y “organiza” posteriormente en el marco de sus programas de indexación, los “conserva” en sus servidores y “comunica” y "facilita el acceso" a sus usuarios en forma de listas de resultados de sus búsquedas[540].

Afrima el Tribunal Supremo que, como regla general, la mención a los datos personales del demandante y al delito que había cometido, en la publicación en el BOE del Real Decreto de indulto, y la posibilidad de que esta información pudiera ser indexada por los buscadores no pueden considerarse contrarias a la normativa de protección de datos, ya que la afectación al honor y a la intimidad del indultado debe ser soportada en aras al derecho a la información en una sociedad democrática. No obstante, el Tribunal Supremo

[540] Sentencia del Tribunal Supremo (Sala de lo Civil, Sección Pleno) de 5 abril de 2016, FJ 5.2.

entiende también que un tratamiento de datos inicialmente lícito, por respetar el principio de calidad de los datos, puede dejar de serlo *a posteriori*, pues el transcurso del tiempo puede convertirlo en inadecuado para la finalidad con que los datos personales fueron recogidos y tratados. El Tribunal Supremo destaca la fundamental importancia del factor tiempo en esta cuestión, puesto que el tratamiento de los datos personales debe cumplir con los requisitos de adecuación, pertinencia, proporcionalidad y exactitud, no solo en el momento en que los datos son recogidos e inicialmente tratados, sino durante todo el tiempo que se produce ese tratamiento.

En el caso, el Tribunal Supremo, teniendo en cuenta el tiempo transcurrido desde que sucedieron los hechos a los que se refiere el tratamiento de datos y, además, que el demandante no era una persona de relevancia pública, ni el asunto presentaba un interés histórico, consideró el tratamiento ilícito por inadecuado y desproporcionado para la finalidad que inicialmente lo justificaba.

El Tribunal Supremo distingue, a estos efectos, por una parte, el derecho a la información y el control de la actividad gubernamental, que justifican que esos datos puedan ser accesibles en el BOE para una búsqueda específica, pues revisten interés general, y frente a los que no puede alegarse la afectación de los derechos de la persona indultada, y, por otra, el tratamiento de datos que realiza *Google,* que supone que cada vez que alguien realiza una búsqueda del nombre y los apellidos del demandado aparezca, entre los primeros enlaces, el que informa de los hechos delictivos que aquel cometió en

el pasado aunque sea indirectamente[541]. La gravedad del daño que, en estas circunstancias, se le causa al afectado, que muchos años después debe sufrir el estigma social de haber sido condenado por un delito, no puede justificarse en el derecho a acceder a la información, cuyo interés público se ha visto mermado por el transcurso de un largo período de tiempo.

Internet es una herramienta de comunicación con enorme capacidad para almacenar y difundir información. Esta red de redes, que enlaza a millones de usuarios por todo el mundo, hace posible que la información sea accesible durante un tiempo indefinido. El riesgo de provocar daños en el ejercicio y goce de los derechos fundamentales y las libertades públicas, particularmente el derecho al respeto de la vida privada, que representan el contenido y las comunicaciones en Internet es enorme, y se ve potenciado por la actuación de los motores de búsqueda.

El Tribunal Supremo considera que, en estos supuestos, aunque no puede exigírsele al gestor de un motor de búsqueda que por su propia iniciativa depure estos datos, porque ello supondría un sacrificio desproporcionado para la libertad de información, sí se le puede requerir que dé una respuesta adecuada a los afectados que ejerciten sus derechos de cancelación y

---

[541] Sentencia del Tribunal Supremo (Sala de lo Civil, Sección Pleno) de 5 abril de 2016, FJ 6.12: "Transcurrido ese tiempo, el derecho a la información y el control de la actividad gubernamental justifica que esos datos puedan ser accesibles para una búsqueda específica, en la página web en la que se publican oficialmente los indultos, la del BOE, porque la posibilidad de investigar sobre la política de indultos llevada a cabo por el Gobierno, incluso en tiempos pasados, o comprobar si una persona que se presenta a un cargo público ha sido indultada en el pasado, reviste interés general y justifica la afectación de derechos de la persona indultada que supone tal posibilidad de búsqueda. Pero no está justificado un tratamiento como el que realiza *Google*, que supone que cada vez que alguien realiza una búsqueda con cualquier finalidad (elaboración de informes comerciales, selección para un puesto de trabajo, búsqueda por clientes, conocidos o familiares del teléfono o la dirección de una persona, simple cotilleo, etc.) aparezca entre los primeros enlaces el que informa sobre los hechos delictivos que cometió una persona en un pasado lejano, aunque sea indirectamente, a través de la información sobre el indulto que le fue concedido".

oposición al tratamiento de datos. De esta manera, deberá cancelar el tratamiento de sus datos personales cuando haya transcurrido un período de tiempo que lo haga inadecuado, por carecer las personas afectadas de relevancia pública, y no tener interés histórico la vinculación de la información con sus datos personales. La conjunción del transcurso de un período de tiempo considerable y la falta de atención al requerimiento formulado por el afectado y por la AEPD llevaron al Tribunal Supremo a apreciar la ilicitud del tratamiento de tales datos efectuado por *Google Search*.

Por otra parte, tratándose de este tipo de informaciones, el Tribunal Supremo deja claro que no basta que el interesado desee que la información sea olvidada, sino que, para que la controversia tenga sustancia jurídica, es necesario que la información perjudique su reputación o su intimidad y afecte a su reinserción social. En este sentido afirma: "El llamado 'derecho al olvido digital', que es una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento de datos personales, no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos. Tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículo a su gusto, controlando el discurso sobre sí mismos, eliminando de Internet las informaciones negativas, 'posicionando' a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones. De admitirse esta tesis, se perturbarían gravemente los mecanismos de información

necesarios para que los ciudadanos adopten sus decisiones en la vida democrática de un país.

Pero dicho derecho sí ampara que el afectado, cuando no tenga la consideración de personaje público, pueda oponerse a un tratamiento de sus datos personales que permita que una simple consulta en un buscador generalista de Internet, utilizando como palabras clave sus datos personales tales como su nombre y apellidos, haga permanentemente presentes y de conocimiento general informaciones gravemente dañosas para su honor o su intimidad sobre hechos ocurridos mucho tiempo atrás, de modo que se distorsione gravemente la percepción que los demás ciudadanos tengan de su persona, provocando un efecto estigmatizador e impidiendo su plena inserción en la sociedad, inserción que se vería obstaculizada por el rechazo que determinadas informaciones pueden causar en sus conciudadanos".

En conclusión, en estos casos, el tratamiento de datos referentes al indulto que lleva a cabo el BOE es lícito y no procedería el ejercicio del derecho de cancelación, puesto que el borrado de los datos no resulta posible por la obligación de publicidad derivada de la normativa vigente[542].

No obstante, el análisis de la legitimidad del tratamiento examinado desde el principio de calidad de los datos, obliga a aplicar en cada caso el principio de proporcionalidad y, en tal sentido, los ciudadanos afectados podrían reaccionar mediante el ejercicio del derecho de oposición a un tratamiento de datos personales que, en principio, fue adecuado y necesario

[542] La integridad e inalterabilidad del Boletín Oficial afecta a la cancelación. El artículo 11.2 de la Ley 11/2007 de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos dispone: "2. La publicación del «Boletín Oficial del Estado» en la sede electrónica del organismo competente tendrá carácter oficial y auténtico en las condiciones y con las garantías que se determinen reglamentariamente, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables".

para satisfacer la finalidad de transparencia, pero que el transcurso del tiempo y la permanencia inalterable de la información *sine die* ha transformado en desproporcionado, pues impide el libre desarrollo de la personalidad del indultado y la posibilidad de su reinserción social. De ahí que el ejercicio de este derecho imponga a los responsables de ambos tratamientos, tanto los del BOE como los buscadores, la supresión de las posibilidades de búsqueda por el nombre y apellidos del indultado, articulando en el primer caso medios para impedir su indexación por los motores de búsqueda con el objeto de que en el futuro los buscadores no puedan asociarlos al reclamante, al tiempo que obligaría a los segundos a suprimir de sus índices los enlaces a la página web del BOE. Todo ello, sin perjuicio de que desde el punto de vista legislativo sea necesario repensar las previsiones de publicación de los indultos[543], de modo que se permita armonizar el control de esta medida de gracia, como manifestación del principio de transparencia, con el derecho fundamental a la protección de datos mediante, por ejemplo, el uso de la página web del Ministerio de Justicia, autoridad responsable de la publicación de este tipo de decisiones, que podría permitir la búsqueda de esta información a través de otros criterios diferentes a los datos personales.

En términos más comprometidos con el derecho fundamental a la protección de datos se pronuncia Troncoso[544], para quien sería razonable exigir al responsable del fichero, que es la Administración Pública que ordenó al boletín la publicación de una resolución, que ordene también el bloqueo de la

---

[543] *Vid*. en este sentido GUICHOT REINA, E.: art. cit., pág. 167.
[544] *Vid.* TRONCOSO REIGADA, A.: *La protección de datos de carácter personal. En busca*…, págs. 775 y 780.

publicación de la información en la edición electrónica del boletín oficial, cuando ha dejado de ser necesaria. El responsable está obligado a respetar el principio de calidad y la prohibición de tratamiento excesivos y, en opinión de este autor, dicha obligación debe cumplirse de oficio y no debe depender del ejercicio del derecho de rectificación, cancelación y oposición del interesado. A su juicio, también es responsabilidad de las Administraciones Públicas limitar las herramientas de búsqueda de los propios diarios oficiales y sitios webs que facilitan la localización masiva de información personal, los cuales deben someterse al derecho fundamental a la protección de datos personales.

CONCLUSIONES

1.- El reconocimiento del derecho fundamental a la protección de datos personales como categoría autónoma está ligado a las nuevas amenazas a la dignidad humana derivadas del vertiginoso avance tecnológico. La relevancia de los bienes que ampara, la vida privada, la identidad digital, la protección de la libertad y la autorrealización del individuo, justificaron su consagración legislativa y jurisprudencial.

2.- En el ordenamiento jurídico español, la ambigua redacción del artículo 18.4 de la Constitución reveló, al menos, la conciencia del constituyente del 1978 acerca de los peligros del incipiente desarrollo del tratamiento de datos personales.

3.- El Tribunal Constitucional ha delimitado el derecho a la protección de datos personales como un derecho fundamental autónomo y distinto del derecho a la intimidad, cuya finalidad es garantizar a las personas un poder de disposición y control sobre sus datos personales, sobre su uso y destino (SSTC 290/2000 y 292/2000). Su reconocimiento jurisprudencial es reflejo de la apertura en la interpretación de los derechos fundamentales -artículo 10.2 CE- al contenido de los Tratados y Convenios internacionales sobre la materia, de modo que, en la práctica, estos instrumentos se han convertido en fuente del contenido esencial del derecho fundamental a la protección de datos.

4.- El derecho fundamental a la protección de datos, concebido como el control sobre el tratamiento de la información personal, tiene en el espacio digital un alcance mucho más extenso que el derecho a la intimidad en sentido estricto, no solamente porque su objeto no se reduce a los datos íntimos sino, que se extiende a cualquier dato personal que identique o permita la identificación de la persona. Además, este derecho garantiza al individuo un poder de control sobre sus datos frente a la facultad de exclusión del conocimiento ajeno del ámbito propio y reservado que implica el derecho a la intimidad. Por consiguiente, si bien en ocasiones se confunde con el derecho a la intimidad por los bienes jurídicos que protege, el derecho fundamental a la protección de datos salvaguarda también otros bienes jurídicos y libertades fundamentales, como el honor, la propia imagen, la no discriminación y el libre desarrollo de la personalidad. En este contexto, aspira a proteger la vida privada frente a los moldes tradicionales derivados del derecho a la intimidad.

5.- Nos encontramos ante un derecho fundamental atípico en cuanto a su configuración legal. La asunción de la competencia sobre protección de datos personales por la Unión Europea puso de manifiesto las diferencias en los niveles de tutela de los derechos y libertades de las personas en el tratamiento de datos personales, debido a la disparidad legislativa, que obstaculizaba el ejercicio de actividades económicas a escala de la Unión, al propio tiempo que existía en las instituciones europeas la inquietud de que se garantizase la protección de datos entre los derechos fundamentales de las personas, de la que es fiel reflejo el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. El particular régimen jurídico derivado de la trascendencia

europea de este derecho está representado hoy por el Reglamento General de Protección de Datos que entrará en vigor el próximo 25 de mayo, y la Ley Orgánica de Protección de Datos, que se aplicarán cuando el tratamiento de datos se realice en el marco del derecho de la Unión Europea, mientras que para aquellos tratamientos de datos excluidos de su ámbito de aplicación operará únicamente la segunda.

6.- La delimitación del contenido esencial del derecho a la protección de datos personales comprende, en nuestra opinión, los principios que inspiran toda la actividad del tratamiento de datos personales y aquellas facultades indispensables para hacer efectiva la decisión de la persona de preservar su identidad, es decir la privacidad en sentido amplio, a través del control de sus datos de carácter personal en las diferentes fases del tratamiento de la información.

Aquellos principios representan la cara interna del contenido esencial del derecho fundamental a la protección de datos. Así pues, el poder de disposición que un individuo tiene sobre sus datos personales se manifiesta en la capacidad para consentir o rechazar un tratamiento de los mismos, decisión que solo podrá tomar si ha sido informado previamente. La transparencia forma parte de la esencia del poder de control de la persona sobre sus datos, incluso cuando el tratamiento no esté basado en el consentimiento, sino que tenga un fundamento legal. De la misma manera, el principio de calidad de los datos afecta a todo el proceso, pues la determinación de la finalidad del tratamiento condiciona la recogida, el uso, la conservación y la supresión de la información. Con frecuencia, el principio de calidad será contemplado como principio de

proporcionalidad en el sentido de que los datos deberán ser adecuados, necesarios y proporcionales a la finalidad para la que se destinan. Este principio exige conservar la información, respetando la exactitud, autenticidad e integridad de la misma durante todo el tiempo que dure el tratamiento. A tales efectos, el principio de seguridad de los datos es una garantía de la integridad, de la disponibilidad y de la confidencialidad de la información.

La cara externa del contenido esencial del derecho fundamental a la protección de datos lo constituyen los derechos ARSLPO. Solo accediendo a sus datos personales, el afectado puede comprobar la licitud del tratamiento y ejercitar el haz de facultades que conforma el derecho fundamental a la protección de datos, entre las que se encuentran la rectificación, supresión, limitación, portabilidad y oposición.

7.- A diferencia de los restantes derechos de la personalidad, la tutela eficaz del derecho fundamental a la protección de datos exige la creación de una autoridad de control independiente.

8.- Como todos los derechos fundamentales, el derecho fundamental a la protección de datos no tiene carácter absoluto. Los límites deben venir concretados en una ley, tienen que respetar el contenido esencial del derecho, límite infranqueable para el legislador, y han de encontrar su fundamento en un interés constitucionalmente necesitado de protección. Son, en este sentido, aptos para limitar el ejercicio del derecho, entre otros, la seguridad del Estado o la persecución de las infracciones penales porque son instrumentos para asegurar la paz social y la seguridad ciudadana. En todo caso, la resolución de

los conflictos con otros derechos fundamentales o bienes constitucionalmente garantizados como las libertades de expresión e información o el principio de transparencia exige el respeto al principio de proporcionalidad.

9.- Un tratamiento de datos personales, para ser legítimo, debe apoyarse en el consentimiento del afectado o en otro fundamento legal, pero, además, debe respetar el principio de calidad, lo que implica que los datos que se procesan deben ser fieles a la finalidad concreta para la que se obtienen. Desde esta perspectiva, los datos personales registrados deben ser adecuados, pertinentes y no excesivos para el fin para el que han sido recabados, al propio tiempo que la finalidad del tratamiento debe ser igualmente legítima, determinada y explícita con respeto a la Constitución y a la Ley.

10.-Con fundamento en el principio de calidad de los datos, la Ley Orgánica de Protección de Datos contempla el derecho a la rectificación de los datos inexactos así como su cancelación, cuando han dejado de ser necesarios o pertinentes para la finalidad para la que hubieran sido recabados. Asimismo cuando para el tratamiento de los datos no se precisa el consentimiento del afectado, este puede oponerse al mismo. El Reglamento General de Protección de Datos ha regulado en su artículo 17 el derecho de supresión ("el derecho al olvido") de manera más amplia que la del tradicional derecho de cancelación. El citado derecho se traduce en una obligación de cese en el tratamiento y borrado de los datos para todo responsable del mismo en determinados supuestos, entre los que se incluye el derecho al olvido digital, entendiendo por

tal la supresión en el contexto de los motores de búsqueda u otros responsables del tratamiento en Internet.

11.-La expresión derecho al olvido, en general, evoca la facultad de controlar y limitar la difusión actual, sin consentimiento del afectado, de hechos verídicos que lo identifican, que tuvieron relevancia pública en el pasado, pero que no tienen interés público vigente, y que el interesado preferiría que no salieran de su esfera privada. Este derecho al olvido presenta alcance diferente según el país y la tradición jurídica del common law y del civil law. En el ámbito europeo y desde la perspectiva de los derechos fundamentales, es patente el conflicto entre las libertades informativas y los derechos que protegen la vida privada. La doctrina ha optado por configurar el derecho al olvido, en ocasiones, como un derecho autónomo vinculado al libre desarrollo de la personalidad. Asimismo, hay quienes prefieren considerarlo como un instrumento para la garantía de los derechos al honor y a la intimidad personal o simplemente como una manifestación del derecho fundamental a la protección de datos.

12.-Hasta mediados del siglo XX, el factor tiempo podía crear una cierta expectativa de privacidad. Resultaría razonable no someter a las personas a la divulgación permanente de sus datos publicados en el pasado. El auge de las nuevas tecnologías, y en especial de Internet, ha planteado cuestiones tales como si el interés público puede, por el transcurso del tiempo, desaparecer ante informaciones del pasado que son susceptibles de recuperarse al instante. La obsolescencia del interés informativo será determinante para apreciar el derecho al olvido digital.

13.-El derecho al olvido digital tiene que ver con los riesgos que el uso de Internet produce sobre la reputación, la libertad o la vida privada, en definitiva, la dignidad humana. No se puede comprender este derecho sin tomar conciencia de la complejidad del mundo virtual. Una de las características de Internet es la presencia de nuevos prestadores de servicios en el intercambio de datos en la red, los buscadores. Sobre la base de estas consideraciones, los nuevos hábitos sociales nos obligan sistemáticamente a revelar datos personales, de manera consentida o no. Generamos gran cantidad de información digital que queda almacenada en la red y puede ser rastreada y recuperada al instante a través de los motores de búsqueda, facilitando retratos de nuestra personalidad que eventualmente no se corresponden con la realidad y que en ocasiones nos afectan negativamente. Partiendo de la premisa de que cualquier publicación de datos en línea es un tratamiento de datos personales y de que el factor tiempo puede hacer que el tratamiento de datos en Internet resulte inadecuado, no pertinente o excesivo para la finalidad para la que los datos fueron recabados, el derecho al olvido digital encuentra, en este sentido, su fundamento en el derecho a la protección de datos personales como poder de control sobre la información personal y en el principio de calidad de los datos.

14.-La sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, el conocido como caso Google, vino a aclarar la normativa europea en relación con la actividad de los motores de búsqueda en Internet y la

aplicación territorial de la misma, así como el alcance del derecho de cancelación y oposición en este contexto.

Respecto a la primera cuestión, para el Tribunal de Justicia de la Unión Europea hay que diferenciar el tratamiento de datos personales llevado a cabo por los editores de páginas web del efectuado por los gestores de motores de búsqueda. El primero divulga los datos personales en una página de Internet; el segundo desempeña un papel decisivo en la difusión global de dichos datos, cuyos efectos se multiplican y permiten la construcción de perfiles de la personalidad. Por consiguiente, un tratamiento de datos personales efectuado por un motor de búsqueda afecta significativamente a los derechos fundamentales de respeto a la vida privada y de protección de datos personales, de modo adicional al que se desprende de la actividad de los editores. El mero interés económico en este tratamiento no justifica tal afección, al propio tiempo que el interés legítimo de los internautas en tener acceso a la información en cuestión habrá de ser objeto de ponderación, atendiendo, de un lado, a la naturaleza de la información y su carácter sensible para la vida privada de la persona afectada, y, de otro, al interés de la colectividad en disponer de esta información, que puede variar en función del papel que esta persona desempeñe en la vida pública.

Para el Tribunal de Justicia de la Unión Europea, el gestor del motor de búsqueda debe considerarse responsable del tratamiento de datos personales. Por lo tanto, puede estar obligado a eliminar de la lista de resultados obtenida, tras una búsqueda efectuada a partir del nombre de una persona, los vínculos a páginas web publicadas por terceros que contienen información relativa a dicha persona, incluso si esta información no se borra previa o

simultáneamente de las páginas webs en que han sido publicadas y aunque la publicación en dichas páginas sea lícita.

15.-En lo relativo a la aplicación territorial de la normativa europea, objeto de la segunda cuestión prejudicial resuelta por la STJUE del caso Google, el Tribunal de Justicia de la Unión Europea determinó que si bien Google Search es un buscador a nivel mundial gestionado por Google Inc, domiciliada en Estados Unidos, presta sus servicios en España a través de Google Spain. Por lo tanto, el tratamiento de datos personales llevado a cabo para el funcionamiento del mencionado motor de búsqueda estaba sujeto a las obligaciones y garantías previstas por la normativa europea.

16.-En lo que respecta al derecho al olvido, el Tribunal de Justicia de la Unión Europea concluyó que un tratamiento de datos inicialmente lícito puede resultar, con el tiempo, incompatible con la Directiva 95/46/CE, cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron. El derecho del afectado a que la información personal no esté, en la actualidad, vinculada a su nombre por una lista de resultados obtenida a través de un buscador no presupone que exista un perjuicio para el interesado. No obstante, aquel puede solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados cuando lesione sus derechos al respeto a la vida privada y a la protección de datos. En tales casos, estos derechos prevalecen, en principio, no solo sobre el interés económico del gestor del motor de búsqueda, sino también, sobre el interés del público en acceder a la

mencionada información en una búsqueda que verse sobre el nombre de esa persona. Se exceptúa el caso de que, por el papel desempeñado por el interesado en la vida pública, la injerencia en sus derechos fundamentales esté justificada por el interés preponderante del público en tener acceso a la información de que se trate.

17.-Las principales críticas a la sentencia Google se centran en que el interés de los usuarios de Internet en disponer de información no es considerado por aquella como un contenido de la libertad de información, de manera que el acceso a la información queda desvalorizado en la ponderación con los derechos a la vida privada y a la protección de datos. Sin embargo, a mi juicio, esta resolución no afecta al derecho a ser informados de los internautas porque la información no desaparece de donde está, sino que solamente se desindexa de las búsquedas que, a través del motor, se hagan por el nombre y apellidos del afectado. Por lo tanto, rastreándola de otro modo se seguirá encontrando. En definitiva, solo afecta a la forma de búsqueda. La sentencia no está reconociendo un derecho al olvido en Internet, sino que da respuesta a unas preguntas en torno a un litigio concreto, lo que explica que en ella se demande borrar los enlaces, pero no la información.

18.-Lo decisivo de la sentencia Google es que toca cuestiones concluyentes para la efectividad del derecho fundamental a la protección de datos personales en Internet. Por una parte, viene a interpretar los derechos de cancelación y oposición de manera lógica en el conflicto entre libertad de empresa y derecho fundamental a la protección de datos, conforme al sentido

que se deriva de uno de los principios que informan este derecho, el de calidad de los datos. Y, por otro lado, son dos las pautas que marca la sentencia ante futuros conflictos entre el derecho fundamental a la protección de datos y las libertades informativas: el interés público actual y el paso del tiempo. Pone, pues, término a la situación de desprotección generada por la negativa de la empresa Google a someterse a la normativa europea y española sobre la materia, estableciendo que el derecho fundamental a la protección de datos prevalece sobre la libertad de empresa, esto es, el mero interés económico del gestor del motor de búsqueda. Se diferencia así, dicha actividad del ejercicio de las libertades informativas, que prevalecerá sobre el derecho fundamental a la protección de datos salvo que el interesado no tenga relevancia pública y el acceso a la información no esté justificado por el interés público actual.

19.-El tratamiento de datos personales relativos al pasado penal en Internet debe justificarse en la tutela de otros bienes o derechos constitucionales. El control sobre la difusión de las condenas penales encuentra en el derecho fundamental a la protección de datos un encaje más idóneo que el que representan los tradicionales derechos al honor y a la intimidad. No obstante, las dificultades de aquellos que quieren poner en marcha el derecho al olvido digital son mayores cuando los datos están contenidos en fuentes accesibles al público porque han sido publicados por terceros sin su consentimiento, amparados en la libertad de información, o cuando su consentimiento es irrelevante, por tratarse de datos que resultan de Diarios y Boletines Oficiales publicados en aras al principio de transparencia de la información pública.

20.- El derecho al olvido digital es un derecho en construcción a través de la jurisprudencia, a día de hoy, fundamentalmente, de los órganos judiciales y del Tribunal Supremo, a falta de un pronunciamiento en esta materia por parte de nuestro Tribunal Constitucional. En cualquier caso, no cabe duda de que una hipotética sentencia sobre esta materia por parte de este último estaría condicionada por la protección dispensada por el Tribunal de Justicia de la Unión Europea al derecho a la protección de datos personales sobre la base del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y, por lo tanto, no podría alterar este estándar de protección.

21.- No existe un derecho al olvido del pasado penal, sino concretas situaciones en las que el transcurso del tiempo produce la caducidad de sus efectos jurídicos. Entre ellas está la prescripción de la responsabilidad penal, que responde a la necesidad de garantizar la libertad y la reinserción social del individuo.

Los antecedentes penales son datos personales de los sujetos condenados por sentencia penal firme recogidos en el Registro Central de Penados y Rebeldes. Son datos especialmente sensibles y reservados. De ahí su conexión con los derechos fundamentales al honor, a la intimidad y a la protección de datos de carácter personal, pues estamos ante un tratamiento de una categoría especial de datos sometido a fuertes limitaciones, que obligan a una interpretación restrictiva y rigurosa de los términos en los que esa información puede divulgarse o transmitirse.

22.- El Tribunal Constitucional tuvo ocasión de analizar el conflicto entre los derechos de la personalidad y las libertades informativas al hilo de la divulgación de los antecedentes penales. La doctrina de la confidencialidad de los antecedentes penales parte de la base de que su difusión puede dañar la reputación de la persona, en cuanto conlleva un desmerecimiento en la consideración ajena, quedando menoscabado su honor y, paralelamente, su intimidad, al convertirse en una fuente de información sobre su vida privada y su familia. No obstante, estos derechos pueden verse limitados por la relevancia pública de la información.

23.-En este último sentido, el tema del impacto que sobre los derechos fundamentales puede tener la publicidad de los antecedentes penales surgió a propósito de la necesidad potenciar ante la opinión pública el rechazo a la violencia doméstica y otros casos de maltrato, tortura y vejaciones. En el primer caso, la limitación del principio de confidencialidad de los antecedentes penales encontró su fundamento en la ley y en el afán de las Administraciones Publicas en hacer frente a esta lacra social. En los restantes casos, y de acuerdo con la LOPD, partiendo de que el derecho fundamental a la protección de datos personales no se refiere solo a los datos íntimos de la persona, sino también a los datos públicos, solo las Administraciones Públicas competentes pueden realizar un tratamiento de datos relativos a la comisión de infracciones penales. Por lo tanto, al amparo de la libertad de información no puede llevarse a cabo un tratamiento de datos personales de estas características, confeccionando un fichero para dar publicidad en Internet a tales datos sensibles de las personas, lo cual está reservado a las Administraciones Públicas.

24.-La jurisprudencia del Tribunal Europeo de Derechos Humanos también ha tenido ocasión de pronunciarse sobre la conservación de datos relativos a los antecedentes penales y su almacenamiento sistemático por el riesgo de estigmatización de la persona. En este sentido, llamó la atención sobre la circunstancia de que esta clase de información se pudiera revelar mucho tiempo después de producirse los hechos, cuando todos, salvo la persona afectada, posiblemente la hubieran olvidado. Así pues, el Tribunal Europeo de Derechos Humanos vino a precisar que cuando la condena o la medida penal fuera remota en el tiempo, estos datos vienen a formar parte de la vida privada de la persona, la cual debe ser respetada.

25.-Otra de las manifestaciones del derecho al olvido del pasado penal es la situación de los indultados a los que el Estado exime de cumplir la pena, pero cuyos datos personales nunca se borran del diario oficial en el que, con motivo de la concesión de un indulto, se insertaron. En principio, en aras al principio de transparencia, y por imperativo legal, procede la publicación de este tipo de datos. Sin embargo, el derecho al olvido tropieza con esta necesidad de transparencia, pues la divulgación de tal información en la edición digital de los diarios oficiales supone una injerencia en el derecho fundamental a la protección de datos personal, dada su fácil localización y el carácter de fuente de acceso público de los diarios oficiales.

Como regla general, el Tribunal Supremo ha afirmado que la mención a los datos personales del indultado y al delito que ha cometido, en la publicación en el BOE del Real Decreto de indulto, y la posibilidad de que esta información

pudiera ser indexada por los buscadores no pueden considerarse contrarias a la normativa de protección de datos, ya que la afectación al honor y a la intimidad del indultado debe ser soportada en aras al derecho a la información en una sociedad democrática. No obstante, el Tribunal Supremo entiende también que un tratamiento de datos inicialmente lícito, por respetar el principio de calidad de los datos, puede dejar de serlo a posteriori, pues el transcurso del tiempo puede convertirlo en inadecuado para la finalidad con que los datos personales fueron recogidos y tratados. El Tribunal Supremo destaca la fundamental importancia del factor tiempo en esta cuestión, puesto que el tratamiento de los datos personales debe cumplir con los requisitos de adecuación, pertinencia, proporcionalidad y exactitud, no solo en el momento en que los datos son recogidos e inicialmente tratados, sino durante todo el tiempo que se produce ese tratamiento.

Como resultado, el ejercicio de este derecho impone a los responsables de ambos tratamientos, tanto los del BOE como los buscadores, la supresión de las posibilidades de búsqueda por el nombre y apellidos del indultado, articulando en el primer caso medios para impedir su indexación por los motores de búsqueda con el objeto de que en el futuro los buscadores no puedan asociarlos al reclamante, al tiempo que obligaría a los segundos a suprimir de sus índices los enlaces a la página web del BOE. Todo ello, sin perjuicio de que desde el punto de vista legislativo sea necesario repensar las previsiones de publicación de los indultos.

26.-Como complemento a lo ya expuesto, sin perjuicio del principio de publicidad de las sentencias (art. 120 CE), las resoluciones judiciales no

pueden ser consideradas como fuentes accesibles al público. En tal sentido se intenta compaginar el libre acceso de los ciudadanos a los fallos judiciales, con el derecho a la protección de los datos de carácter personal. Así, la jurisprudencia publicada Internet, de modo libre y gratuito, aparece vaciada de datos personales con algunas excepciones, como los contenidos en los fallos de las sentencias firmes condenatorias por delito de defraudación tributaria.

27.- El alcance de la publicidad de las sentencias del Tribunal Constitucional vino a poner de manifiesto la absoluta independencia de este respecto a los demás órganos constitucionales del Estado, siendo su papel de máximo intérprete de nuestra Carta Magna el fundamento de la máxima divulgación de la doctrina constitucional que proviene de sus resoluciones. No obstante, tal principio no es tan absoluto. A partir de la entrada en vigor del Acuerdo del Pleno del Tribunal Constitucional de 23 de julio de 2015, que regula la exclusión de los datos de identidad personal en la publicación de sus resoluciones, este es el criterio general cuando se trate de menores y personas que requieran un especial deber de tutela, de las víctimas de delitos de cuya difusión se deriven especiales perjuicios y de las personas que no estén constituidas en parte en el proceso constitucional. En los demás casos, la exigencia constitucional de publicidad de sus resoluciones (artículo 164 CE), en lo relativo a los datos de identidad y situación personal de las partes intervinientes en el proceso, podrá ser excepcionada por el Alto Tribunal de oficio o a instancia de parte, a partir de la ponderación de circunstancias debidamente acreditadas concurrentes en el caso.

28.-En términos generales, un tratamiento de datos personales no precisa el consentimiento del interesado cuando sea consecuencia del ejercicio de las libertades de expresión e información. Sin embargo, esta actividad ha de respetar en todo caso el principio de calidad de los datos. La digitalización de la prensa escrita, en particular, en su sección de hemeroteca, ha provocado su indexación por los motores de búsqueda de Internet, lo que ha facilitado el acceso a informaciones del pasado que, en ocasiones, lesionan los derechos de la personalidad de las personas afectadas.

29.-El tema de la divulgación indiscriminada del pasado penal por los buscadores de internet a propósito de las hemerotecas digitales fue abordado por la Sentencia de la Sala de lo Civil del Tribunal Supremo de 15 octubre de 2015. El tratamiento de datos personales que llevó a cabo el editor de la página web como consecuencia de la digitalización de una noticia, con determinadas características técnicas, permitía su indexación y aparición en los resultados de los buscadores de Internet, de modo que perjudicaban el honor y la intimidad de las personas afectadas. El tratamiento que inicialmente respondía a la finalidad periodística que lo justificaba, con el transcurso del tiempo, se transformó en inadecuado para esa finalidad, y el daño a los derechos de la personalidad resultó desproporcionado en relación con el derecho que originalmente amparaba el tratamiento de datos.

A tal efecto, el Tribunal Supremo distingue la función principal que cumplen los medios de comunicación cuando difunden noticias de actualidad de la función secundaria de las hemerotecas digitales, para concluir definiendo el derecho al olvido digital como una concreción en este campo de los derechos

derivados de los requisitos de calidad del tratamiento, que garantiza que, cuando el afectado no tenga la consideración de personaje público, pueda oponerse al tratamiento de sus datos personales, dirigiéndose, como en este caso, contra el editor de la página web que gestione la hemeroteca digital. Como consecuencia del ejercicio del derecho al olvido digital, este último estará obligado a utilizar “protocolos de exclusión” para evitar que las noticias antiguas pueden ser indexadas por buscadores generalistas cuando la información carezca de interés público. Tal medida es el resultado de ponderar el derecho de cancelación que la normativa de protección de datos atribuye a los afectados por un tratamiento de datos personales que no reúna los requisitos de calidad con la libertad de información que ampara a las hemerotecas digitales en Internet. Sin bien los editores de la página web no están obligados a modificar la noticia de la hemeroteca ni adoptar medidas tendentes a desindexar los datos de carácter personal de sus buscadores internos, ya que las hemerotecas digitales gozan de la protección de la libertad de información, al satisfacer un interés público en el acceso a la noticia y estar protegidas por el artículo 20 de la Constitución.

30.- A la luz del derecho fundamental a la protección de datos, y más concretamente del principio de calidad de los datos, habría que analizar hasta qué punto el tratamiento de datos que llevan a cabo las hemerotecas digitales es adecuado, necesario y proporcionado. Es discutible si el tratamiento de datos consistente en la digitalización de una información previamente publicada que afecta a hechos que en su día fueron ciertos, relevantes y noticiables -la condena penal- debe prevalecer sobre el derecho al olvido del condenado. El

carácter indeleble de Internet lo hace difícilmente compatible con la reinserción social y el libre desarrollo de la personalidad del que ha cumplido ya su pena. Por consiguiente, hay voces que abogan por el cese del uso de los datos también por los servicios de búsqueda internos de las hemerotecas digitales. Sin embargo, a nuestro parecer, el riesgo para el derecho al olvido digital no es que la información sea accesible a través de la página web del medio de comunicación, por medio del buscador interno de la hemeroteca digital. El peligro es el efecto multiplicador de la noticia obsoleta que generan los motores de búsqueda generalistas, que puede llevar a la estigmatización social de la persona.

31.-Por último, conviene precisar que el derecho al olvido digital no puede amparar pretensiones dirigidas a borrar el pasado que no nos complace ni a censurar el ejercicio de la libertad de información. El tratamiento de datos personales que puede dar lugar al derecho al olvido digital es el que llevan a cabo las hemerotecas digitales de los periódicos. Y, en tal caso, solo procede el derecho de oposición si se demuestra que, tiempo después de que se publicara la información original, el periódico editor de la página web permite que la misma continúe estando accesible indiscriminadamente, mediante su indexado y tratamiento por los motores de búsqueda generalistas, con la utilización en estos, como términos clave, de los datos personales del afectado (como el nombre y los apellidos). En Internet, en definitiva, solo existe el derecho a que la información sea olvidada o, mejor dicho, desindexada cuando la búsqueda se lleve a cabo por el nombre y apellidos.

En definitiva, el derecho de oposición solo actúa a instancia de parte, no es un derecho absoluto y puede ejercitarse contra la webmaster que edita originalmente la información o contra el motor de búsqueda generalista que con su indexación favorece su difusión. En el primer caso, el medio de comunicación, en el ejercicio de la libertad de información, podrá mantener la información inalterada siempre y cuando tenga relevancia actual y afecte a un personaje público. En el segundo caso, la libertad de empresa ejercida por el buscador generalista decae frente al derecho fundamental a la protección de datos para evitar su divulgación permanente y lesiva en internet.

No es la presencia en Internet de una determinada información la que expone la privacidad del individuo sino que es su fácil localización y amplia difusión, en uno o varios motores de búsqueda generalistas, lo que posibilita que el pasado de un individuo permanezca inalterable ante la sociedad. Por lo tanto, hay que diferenciar entre la obtención de información específica acudiendo al buscador de una hemeroteca digital y la averiguación de un perfil completo que cualquiera pueda obtener en un buscador de Internet con tan solo introducir el nombre de una persona. Esto es la base de lo que se ha denominado como el derecho a la "oscuridad práctica", que solo se da cuando el afectado no sea personaje público, no exista un interés histórico en la noticia y estén afectados los derechos de la personalidad.

BIBLIOGRAFíA

AA.VV.: *Derecho de la comunicación,* Iustel, Madrid, 2016.

ABERASTURI GORRIÑO**,** U.: " Derecho a ser olvidado en Internet y medios de comunicación digitales. A propósito de la Sentencia del Tribunal Supremo de 15 de octubre de 2015", *Revista Española de Derecho Administrativo*, núm. 175, 2016.

AGUADO RENEDO, C.: "Análisis (estrictamente jurídico) de un indulto conflictivo: el caso Gómez de Liaño", *Revista Española de Derecho Constitucional,* núm. 63, 2001.

- "La clemencia vinculada por el derecho", *Revista de Derecho Político*, núm. 74, 2009.

- "El derecho de gracia. El indulto", disponible en Internet: http://0-.iustel.com.fama.us.es/v2/c.asp.

ALGUACIL GONZÁLEZ-AURIOLES, J.: "La libertad informática: aspectos sustantivos y competenciales (SSTC 290 y 292/2000)", *Teoría y Realidad Constitucional*, núm. 7, 2001.

ALONSO MARTÍNEZ, C. y CERQUEIRA SÁNCHEZ, M.: "Ficheros sobre solvencia patrimonial y crédito", en AA.VV.: *El Reglamento general de protección de datos hacia un nuevo modelo europeo de privacidad,* Reus, Madrid*,* 2017.

ÁLVAREZ CARO, M.: *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*, Reus, Madrid, 2015.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M.: “El derecho a la intimidad personal, la libre difusión de información y el control del Estado sobre los bancos de datos”, *Actualidad Administrativa,* núm. 37, 1999.

- "El registro de penados y rebeldes y la intimidad de los ciudadanos (Comentario a la Sentencia 144/1999, de 22 de julio", *Actualidad Jurídica Aranzadi*, núm. 409, 1999.

APARICIO SALOM, J.: "La calidad de los datos", en AA.VV.: *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi, Cizur Menor (Navarra), 2010.

ARENAS RAMIRO, M.: "El derecho a la protección de datos personales como garantía de las libertades de expresión e información", en COTINO HUESO, L (coord.): *Libertad en Internet: la red y las libertades de expresión e información*, Tirant lo Blanch, Valencia, 2007.

- El *derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, 2006.

- “UNFORGETTABLE: a propósito de la STJUE de 13 de mayo de 2014. caso C*osteja (Google vs AEPD*)", *Teoría y Realidad Constitucional*, núm. 34, 2014.

- "Protección de datos personales y sentencias del Tribunal Constitucional

a propósito de la sentencia del Tribunal Constitucional 114/2006", *Revista Española de Protección de datos*, núm. 1, 2006.

- "Reforzando el ejercicio de la Protección de Datos: viejas y nuevas facultades", en RALLO LOMBARTE, A y GARCIA MAHAMUT, R. (eds.): *Hacia un nuevo Derecho Europeo de Protección de Datos*, Tirant lo Blanch, Valencia, 2015.

AZURMENDI, A.: "Por un 'derecho al olvido' para los europeos: aportaciones jurisprudenciales de la Sentencia del Tribunal de Justicia Europeo del caso Google Spain y su recepción por la Sentencia de la Audiencia Nacional Española de 29 de diciembre de 2014", *Revista de Derecho Político*, *UNED,* núm. 92, 2015.

BARRERO ORTEGA, A.: *Juicios por la prensa y ordenamiento constitucional*, Tirant lo Blanch, Valencia, 2010.

BENGHOZI, P, J.: “Les moteurs de recherche: trou noir de la regulation?” en STROWEL, A. y TRIAILLE, J. P. (dirs.): *Google et les nouveaux services en ligne. Impact sur l’économie du contenu et questions de propiéte intellectuelle*, Larcier, Bruselas, 2008.

BERROCAL LANZAROT, A. I.: "El derecho de supresión de datos o derecho al olvido en el Reglamento General de Protección de Datos", *Revista General de Legislación y Jurisprudencia,* núm. 1, 2017.

- *Derecho de supresión de datos o derecho al olvido*, Reus, Madrid, 2017.

BIGLINO CAMPOS, M. P.: "Derechos fundamentales en la Unión y en los Estados miembros: algunos problemas de conexión", *Revista Española de Derecho Constitucional*, núm. 69, 2003

BOIX PALOP, A.: “El equilibrio entre los derechos del art.18 de la Constitución, el derecho al olvido y las libertades informativas tras la Sentencia Google”, *Revista General de Derecho Administrativo*, núm. 38, 2015.

BROTONS MOLINA, O.: "Caso Google: tratamiento de datos y derecho al olvido. Análisis de las Conclusiones del Abogado General, asunto C-131/12", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 33, 2013.

BRU CUADRADA, E.: “La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad”, *IDP*: *revista de Internet, derecho y política,* núm. 5, 2007.

BUISÁN GARCÍA, N.: “El derecho al olvido: el nuevo contenido de un derecho antiguo”, *El Cronista del Estado Social y Democrático de Derecho*, núm. 46, 2014.

BUSTOS GISBERT, R.: "Vida privada y derecho a la información. Desarrollos jurisprudenciales en 2013-2014: la extraña y tardía recepción de Carolina en España", *Revista Española de Derecho Constitucional*, núm. 107, 2016.

CANALS AMETLLER, D.: "El acceso público a datos en un contexto de transparencia y de buena regulación" en CANALS AMETLLER, D. (ed.): *Datos.*

Protección, Transparencia y Buena Regulación, Documenta Universitaria, Girona, 2016.

CARMONA CONTRERAS, A.: "El espacio europeo de los derechos fundamentales: de la Carta a las Constituciones nacionales", *Revista Española de Derecho Constitucional*, núm. 107, 2016.

CARMONA RUANO, M.: ”Aplicación de la Carta de Derechos Fundamentales en la Unión Europea por la jurisprudencia española”, Seminario sobre la aplicación jurisprudencial de la Carta de Derechos Fundamentales en la Unión Europea, Sevilla, 3 de noviembre de 2006, disponible en Internet: http://www.juecesdemocracia.es/fundacion/ponenciassevilla/Aplicaci%F3ndela CartaMiguelCarmona.pdf

CARRASCO DURÁN, M.: *Los procesos para la tutela judicial de los derechos fundamentales*, Centro de Estudios Políticos y Constitucionales, Madrid, 2002.

-"Relaciones entre la Carta de derechos fundamentales de la Unión Europea y la declaración de derechos contenida en la Constitución" en GORDILLO PÉREZ, L. I. (coord.): *Constitución Española e integración europea: treinta años de Derecho constitucional de la integración*, Tirant lo Blanch, Valencia, 2017.

CARRERAS SERRA, F.: "El derecho fundamental a la protección de datos personales", en AA.VV.: *Los nuevos derechos fundamentales, seminario: Baeza, 13 y 14 de octubre de 2005: XXV aniversario Tribunal Constitucional,* Academia de Ciencias Sociales y del Medio Ambiente de Andalucía, 2007.

CARRILLO, M.: “Derecho a la información y veracidad informativa (Comentario a las SSTC 168/86 y 6/88)”, *Revista Española de Derecho Constitucional*, núm. 23, 1988.

- “El derecho al olvido en Internet”, *El País*, 23 de octubre de 2009, disponible en Internet: http://bit.ly/2srRjO.

- *El derecho a no ser molestado. Información y vida privada*. Aranzadi, Cizur Menor (Navarra), 2003.

- “Los derechos fundamentales en la Constitución europea”, en VIDAL-BENEYTO, J. (coord.): *El reto constitucional de Europa,* Madrid, Dykinson, 2005.

- "Protección de datos en Internet", *El País,* 17 de abril de 2008, disponible en Internet: https://elpais.com/diario/2008/04/17/opinion/1208383205_850215html

CERNADA BADÍA, R.: "El derecho al olvido judicial en la red", en CORREDOIRA, L. y COTINO HUESO, L. (dirs.): *Libertad de expresión e información en la Red. Amenazas y protección de los derechos personales*, Centro de Estudios Políticos y Constitucionales, Madrid, 2013.

CHÉLIZ INGLÉS, M. C.: "El 'derecho al olvido digital'. Una exigencia de las nuevas tecnologías, recogida en el futuro reglamento general de protección de datos', *Actualidad Jurídica Iberoamericana*, núm. 5, 2016.

CIAVATTONE, C.: "I diritti della personalità e le nuove tecnologie: il diritto all’oblio e strumenti di tutela" en Jornadas sobre Documento informatico e la

prova nel proceso civile: un codice al passo con i tempi?, Roma, 2016. Disponible en Internet: http://www.giustizia.lazio.it/apello.it/form_conv-didattico/Relazione_diritto_all_oblio_dott.ssa_Ciavattone.pdf

CIDONCHA MARTÍN, A.: “Garantía institucional, dimensión institucional y derecho fundamental: balance jurisprudencial”, *Teoría y Realidad Constitucional*, núm. 23, 2009.

CONDE ORTIZ, C.: *El derecho a la protección de datos personales: un derecho autónomo sobre la base de los conceptos de intimidad y privacidad*, Dykinson, Madrid, 2005.

CONTRERAS NAVIDAD, S.: La *protección del honor, la intimidad y la propia imagen en Internet,* Aranzadi, Cizur Menor (Navarra), 2012.

COTINO HUESO, L.: "Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público (Art. 3 de la LOPD)", en TRONCOSO REIGADA, A. (dir.): *Comentario a la Ley Orgánica de Protección de Datos Personales*, Civitas, Cizur Menor, 2010.

- “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”, en BEL, I. y CORREDOIRA, L.: *Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia*, Centro de Estudios Políticos y Constitucionales, Madrid, 2015.

- “La colisión del derecho a la protección de datos personales y las libertades informativas en la red: pautas generales y particulares de solución", en COTINO HUESO, L (ed.): *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*, Publicaciones de la Universidad de Valencia, Valencia, 2011. Disponible en Internet: http://www.derechotics.com/congresos/2010-libertades-y-20/e-libro-elibertades-2010.

- "La selección y personalización de las noticias por el usuario de las nuevas tecnologías", en CORREDOIRA, L. y COTINO HUESO, L. (dirs.): *Libertad de expresión e información en la Red. Amenazas y protección de los derechos personales*, Centro de Estudios Políticos y Constitucionales, Madrid, 2013.

- "Nuestros jueces y tribunales ante Internet y la libertad de expresión: el estado de la cuestión", en COTINO HUESO, L (coord.): *Libertad en Internet: la red y las libertades de expresión e información*, Tirant lo Blanch, Valencia, 2007.

DAVARA RODRÍGUEZ, M. A.: L*a protección de datos en Europa: principios, derechos y procedimiento*, Universidad Pontificia de Comillas, Madrid, 1998.

- *Manual de Derecho Informático*, Aranzadi, Cizur Menor (Navarra), 2015.

DE MIGUEL ASENSIO, P. A.: "La contradictoria doctrina del Tribunal Supremo acerca del responsable del tratamiento de datos por el buscador Google", *La Ley Unión Europea*, núm. 37, 2016.

DE TERWANGNE, C.: “Privacidad en Internet y derecho a ser olvidado/derecho al olvido”, *IDP: revista de Internet, Derecho y Política*, núm. 13, 2012.

DEL CASTILLO VÁZQUEZ, I. C.: *La protección de datos cuestiones constitucionales y administrativas,* Aranzadi, Cizur Menor (Navarra), 2007.

DENNINGER, E, "El derecho a la autodeterminación informativa" en PÉREZ LUÑO, A. E.: *Problemas actuales de la documentación y la informática jurídica*, Tecnos, Madrid, 1987.

DI PIZZO CHIACCHIO, A.: “Efectos en la jurisprudencia del Tribunal Supremo de la doctrina sentada en el caso «Google Spain»: la interpretación de la responsabilidad de los gestores de motores de búsqueda en la implementación del derecho al olvido digital", *Revista Jurídica de Catalunya,* núm. 4, 2016.

DÍEZ-PICAZO, L. M.: *Sistema de derechos fundamentales*, Aranzadi, Cizur Menor (Navarra), 2013.

ESPÍN TEMPLADO, E.: “Fundamento y alcance del derecho fundamental a la inviolabilidad del domicilio*”, Revista del Centro de Estudios Constitucionales,* núm. 8, 1991.

FERNÁNDEZ ESTEBAN, M. L.: "El impacto de las nuevas tecnologías e Internet en los derechos del artículo 18 de la Constitución", *Anuario de la Facultad de Derecho , Universidad de Extremadura*, núm. 17, 1999.

FERNÁNDEZ TOMÁS, A. F.: "La Carta de Derechos Fundamentales de la Unión Europea tras el Tratado de Lisboa. Limitaciones a su eficacia y alcance generadas por el Protocolo para la aplicación de la Carta al Reino Unido y

Polonia", en MARTÍN Y PÉREZ DE NANCLARES, J. (coord.): *El Tratado de Lisboa. La salida de la crisis constitucional.* Madrid, Iustel, 2008.

FLIQUETE LLISO, E. F: "El indulto un enfoque jurídico constitucional", Universidad Miguel Hernández, Elche, 2015, disponible en Internet: http://dspace.umh.es/bitstream/11000/1953/1/TD%20Fliquete%20Lliso%2C%20Enrique%20Fco.pdf.

FREIXAS GUTIÉRREZ, G.: *La protección de datos de carácter personal en el Derecho Español,* Bosch, Barcelona, 2001.

FROSINI, T. E.: "Nuevas tecnologías y constitucionalismo", *Revista de Estudios Políticos*, núm. 124, 2004.

FROSINI, V.: “Bancos de datos tutela de la persona”, *Revista de Estudios Políticos*, núm. 30, 1982.

- *Cibernética diritto e societá*, Edizioni di Comunita, Milano, 1968.

- "El horizonte jurídico de Internet", *Revista de Derecho Constitucional Europeo*, núm. 28, 2017. Disponible en Internet: https://dialnet.unirioja.es/servlet/libro?codigo=706704.

- “La tutela de la privacidad: de la libertad informática al bien jurídico informático”, *Revista del Colegio de Abogados de Buenos Aires*, núm. 2, 1989.

GALÁN MUÑOZ, A.: “La protección de datos de carácter personal en los tratamientos destinados a la prevención, investigación y represión de delitos:

hacia una nueva orientación de la política criminal en la Unión Europea", en COLOMER HERNÁNDEZ, I (dir.) y OUBIÑA BARBOLLA, S. (dir.): *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Cizur Menor (Navarra), Aranzadi, 2015.

GARCÍA MAHAMUT, R.: *El indulto un análisis jurídico-constitucional*, Marcial Pons, Barcelona, 2004.

GARCÍA MEXIA, P.: "Olvido en Internet: mejor una mentira en el aire que una verdad en el cajón" en el blog *la Ley en la red,* 2014, Disponible en Internet: http://abcblogs.abc.es/ley-red/public/post/olvido-en-internet-mejor-una-mentira-al-aire-que-una-verdad-en-el-cajon-15898.asp/

GASCÓN MARCÉN, A.: " El derecho a la protección de datos personales en Europa: actualidad y retos", en GALINDO AYUDA, F (coord.): *Ciencia del Derecho y tecnologías: aproximaciones de presente y fu*turo, Prensas Universitarias de Zaragoza, Zaragoza, 2014.

GÓMEZ ABEJA, L.: "Registro obligatorio para objetores de conciencia a la interrupción voluntaria del embarazo. Reflexiones constitucionales", *Revista Aranzadi doctrinal,* núm. 4, 2016.

GÓMEZ CORONA, E.: "Derecho a la propia imagen nuevas tecnologías e Internet" en COTINO HUESO, L (ed.): *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*, Publicaciones de la Universidad de Valencia, Valencia, 2011. Disponible en Internet: http://www.derechotics.com/congresos/2010-libertades-y-20/e-libro-elibertades-2010.

GROSSO GALVÁN, M.: *Los antecedentes penales: rehabilitación y control social*, Bosch, Barcelona, 1983.

GUASCH PORTAS, V y SOLER FUENSANTA, J. R.: "El derecho al olvido en Internet", *Revista de Derecho UNED*, núm. 16, 2015.

GUERRERO PICÓ, M. C.: "El derecho fundamental a la protección de los datos de carácter personal en la constitución europea", *Revista de Derecho Constitucional Europeo*, núm. 4, 2005.

- *El impacto de Internet en el Derecho Fundamental a la protección de datos de carácter personal*, Aranzadi, Cizur Menor (Navarra), 2006.

GUICHOT REINA, E.: *Derecho de la Comunicación*, Iustel, Madrid, 2013.

- "El derecho al olvido digital", en BOIX PALOP, A. (coord.), MARTÍNEZ OTERO, J. M. (coord.), MONTIEL ROIG, G (coord.): *Regulación y control sobre contenidos audiovisuales en España,* Aranzadi, Cizur Menor (Navarra), 2017.

- "La publicidad de los datos personales en Internet por parte de las Administraciones Publicas y el derecho al olvido", *Revista Española de Derecho Administrativo*, núm. 154, 2012.

- *Publicidad y privacidad de la información administrativa*, Aranzadi, Cizur Menor (Navarra), 2009.

GUILLÉN LÓPEZ, E.: "Sentencia del Tribunal Supremo de los Estados Unidos *Whalen v. Roe* (1977) 429 U.S. 589, sobre protección de datos personales",

Revista de Derecho Constitucional Europeo, núm. 7, 2007. Disponible en Internet: http://www.ugr.es/~redce/REDCE7/articulos/16sentenciasupremoamericano.htm

HEREDERO CAMPOS, M. T.: "Derecho al olvido", en BUENO DE MATA, F. (coord.): *FODERTICS: Estudios sobre derecho y nuevas tecnologías*, Andavita, Santiago de Compostela, 2012.

- "El nuevo reglamento general de protección de datos y el reconocimiento del derecho de supresión", en AA.VV.: *Hacia una Justicia 2.0: actas del XX Congreso Iberoamericano de Derecho e Informática,* Ratio Legis, Salamanca, 2016.

HEREDERO HIGUERAS, M.: *La Directiva Comunitaria de Protección de Datos de Carácter Personal,* Aranzadi, Pamplona, 1997.

- "La protección de datos de interés policial y judicial en la Unión Europea de Shengen a Prüm", *Revista jurídica de Navarra,* núrm. 42, 2006.

- “La sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de Población de 1983”, *Revista de Documentación Administrativa,* núm. 198, 1983. Disponible en Internet: https://revistasonline.inap.es/index.php?journal=DA&page=article&op=view&path%5B%5D=4687

HERNÁNDEZ CORCHETE, J. A.: “Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus

derechos", en AA. VV.: *El Reglamento general de protección de datos hacia un nuevo modelo europeo de privacidad,* Reus, Madrid*,* 2017.

HERNÁNDEZ LÓPEZ, J. M.: *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*, Aranzadi, Cizur Menor (Navarra), 2013

HERRANZ ORTIZ, A. I.: *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales,* Dykinson, Madrid, 2002.

- *El derecho a la protección de datos personales en la sociedad de la información*, Universidad de Deusto, Bilbao, 2003.

- *La violación de la intimidad en la protección de datos personales*, Dyckison, Madrid, 1998.

JACOBS, J. B. y LARRAURI, E.: "¿Son las sentencias públicas? ¿Son los antecedentes penales privados? Una comparación de la cultura jurídica de Estados Unidos y España", *Indret: revista de análisis del derecho,* 2010.

JIMÉNEZ CAMPO, J.: *Derechos fundamentales; concepto y garantías,* Trotta, Madrid, 1999.

JIMÉNEZ-CASTELLANOS BALLESTEROS, I.: "A vueltas con la contaminación acústica: comentario a la STC 150/2011 de 29 de septiembre", *Revista Europea de Derechos Fundamentales,* núm. 18, 2011.

- "Videovigilancia laboral y derecho fundamental a la protección de datos", *Temas Laborales*, núm. 136, 2017.

LETTERON, R.: "Le droit à l'oublie", *Revue du Droit Public et de la Science Politique en France et à L'étranger,* núm. 2, 1996.

LETURIA INFANTE, F. J.: "Fundamentos jurídicos del derecho al olvido, ¿un nuevo derecho de origen europeo o una respuesta típica ante colisiones entre ciertos derechos fundamentales?", *Revista Chilena de Derecho*, núm. 1, 2016.

LÓPEZ AGUILAR, J. F.: "Data protection package y Parlamento Europeo", en RALLO LOMBARTE, A y GARCÍA MAHAMUT, R. (eds.): *Hacia un nuevo Derecho Europeo de Protección de Datos*, Tirant lo Blanch, Valencia, 2015.

- "La protección de datos personales en la más reciente jurisprudencia del TJUE: los derechos de la CDFUE como parámetro de validez del derecho europeo, y su impacto en la relación transatlántica UE-EEUU", *Teoría y Realidad Constitucional*, núm. 39, 2017.

LÓPEZ PORTAS, M. B.: "La configuración jurídica del Derecho al olvido en el Derecho Español a tenor de la doctrina del TJUE", *Revista de Derecho Político*, núm. 93, 2015.

LUCAS MURILLO DE LA CUEVA, P.: "Derechos fundamentales e Internet. Consideraciones introductorias", en AA.VV.: *Desafíos para los derechos de la persona ante el siglo XXI: Internet y nuevas tecnologías*, Thomson Reuters-Aranzadi, Cizur Menor (Navarra), 2013.

- *El derecho a la intimidad*, Tecnos, Madrid, 1997.

- *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009.

- *El derecho a la autodeterminación informativa. La protección de los datos personales frente al uso de la informática*, Tecnos, Madrid, 1990.

- ”El derecho a la autodeterminación informativa y la protección de datos personales”, *Cuadernos de Derecho*, núm. 20, 2008.

- "El derecho al olvido y la sujeción de Google al derecho europeo según el abogado general del Estado", *Revista de Jurisprudencia*, núm. 1, 2014.

- *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992 de regulación del Tratamiento automatizado de datos de carácter personal),* Colección Cuadernos y Debates, núm. 43, Centro de Estudios Constitucionales, Madrid, 1993.

- “La Constitución y el derecho a la autodeterminación informativa”, *Cuadernos de Derecho Público*, núm. 19-20, 2003.

- “La construcción del derecho a la autodeterminación informativa”, *Revista de Estudios Políticos,* núm. 104, 1999.

- "La distancia y el olvido. A propósito del derecho a la autodeterminación informativa (Comentario al Auto de la Sección Primera de la Audiencia Nacional de 27 de febrero 2012 en el recurso 725/2012)", *Revista de Jurisprudencia*, núm. 1, 2012.

- “La distancia y el olvido en la Red. Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 en el asunto C-131-12” en AA.VV.: *El juez del derecho Administrativo. Libro homenaje a Javier Delgado Barrio.* Marcial Pons*,* Madrid, 2015.

- "La primera jurisprudencia sobre el derecho a la autodeterminación informativa", *Datos personales.org*, núm. 1,2003

- "La protección de datos en la administración de justicia", en AA. VV.: *Derecho a la intimidad y nuevas tecnologías,* Cuadernos de Derecho Judicial, CGPJ, Madrid, 2004.

- "La protección de los datos de carácter personal en el horizonte de 2010", *Anuario de la Facultad de Derecho (Universidad de Alcalá),* núm. 2, 2009.

- "Las vicisitudes del derecho a la protección de datos personales", *Revista Vasca de Administración Pública*, núm. 58, 2000.

- "Perspectivas del derecho a la autodeterminación informativa", *IDP, Revista de Internet, Derecho y Política,* núm. 5, 2007

LUZÓN CANOVAS, M.: "Antecedentes Penales", disponible en Internet: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Luz%C3%B3n%20C%C3%A1novas,%20Mar%C3%ADa.pdf?idFile=2ab36b02-6023-49a0-bd19-8fb338837685.

MADRID CONESA, F.: *Derecho a la intimidad, informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984.

MANGAS MARTÍN, A.: "Comentario al artículo 51", en MANGAS MARTÍN, A (dir.) *Carta de los Derechos fundamentales de la Unión Europea, comentario artículo por artículo*, Fundación Banco Bilbao Vizcaya, Bilbao, 2008.

MARTÍNEZ CABALLERO, J.: "Cómo conjugar el derecho al olvido", *Revista jurídica de Castilla la Mancha*, núm. 57, 2015.

MARTÍNEZ MARTÍNEZ, R.: "Aplicar el derecho al olvido", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 36, 2014.

- "El derecho fundamental a la protección de datos: perspectivas", *IDP, Revista de Internet, Derecho y Política*, núm. 5, 2007.

- "La anonimización de las sentencias del tribunal constitucional", *Unir Revista*, 2015, disponible en Internet: http://www.unir.net/derecho/revista /noticias/la-anonimizacion-de-las-sentencias-del-tribunal-constitucional/549201456751/.

-"La protección de datos: Principios básicos", en BEL, I. y CORREDOIRA, L.: *Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia*, Centro de Estudios Políticos y Constitucionales, Madrid, 2015.

- “Las costuras de la privacidad”, *El País*, 25 de junio de 2013.

- *Una aproximación crítica a la autodeterminación informativa,* Civitas, Madrid, 2004.

MARTÍNEZ OTERO, J, M.: “El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja”, *Revista de Derecho Político,* núm. 93, 2015.

- "Derechos fundamentales y publicación de imágenes ajenas en las redes sociales sin consentimiento", *Revista Española de Derecho Constitucional*, núm. 106, 2016.

MARTÍNEZ SOSPEDRA, M: *Libertades públicas,* vol. I, Fundación Universitaria San Pablo CEU, Valencia, 1993.

MAYER-SCHÖNBERGER, V.: *Delete: the virtue of forgetting in the digital age*, Princenton University Press, 2009.

MEDINA GUERRERO, M.: *La protección constitucional de la intimidad frente a los medios de comunicación*, Tirant lo Blanch, Valencia, 2005.

MEZZANOTTE, M.: *Il diritto all'oblio. Contributo allo studio della privacy storica,* Edizioni Scientifique Italiane, Nápoles, 2009.

MIERES MIERES, L. J.: "El Derecho al olvido digital", *Laboratorio de Alternativas*, 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,* núm. 30, 2014.

- "Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea", *Anuario Jurídico y Económico Escurialense*, 2017.

MORENO MARÍN, M. D.: "El derecho al olvido en el marco del nuevo Reglamento General de Protección de Datos", en BUENO DE MATA, F. (dir/coord.): *Fodertics 6.0 Los nuevos retos del derecho ante la era digital*, Comares, Granada, 2017.

MOYA IZQUIERDO, S. y CRESPO VITORIQUE, I.: "Los motores de búsqueda y el derecho al olvido: cuando la tecnología avanza más rápido que el Derecho", *Revista Aranzadi Unión Europea*, núm. 10, 2014.

MUÑOZ RODRÍGUEZ, J.:" La incidencia de la sentencia del Tribunal Supremo (STS núm. 574/2016) para los usuarios que ejercitan el derecho al olvido", Diario la Ley, núm. 8733, 2016.

MURGA FERNÁNDEZ, J. P.: "El derecho al olvido digital en un supuesto de concesión de indulto versus la libertad de información. A propósito de la STS del Pleno de la Sala Primera de 5 de abril de 2016 y la reciente jurisprudencia dictada en la materia", *Boletín del Colegio de Registradores de España*, núm. 34, 2016.

- "La protección de datos y los motores de búsqueda en Internet: cuestiones actuales y perspectivas de futuro acerca del derecho al olvido", *Revista de Derecho Civil*, núm. 4, 2017.

NOVAL LAMAS, J. J.: "Algunas consideraciones sobre la futura regulación del derecho al olvido", *Revista de contratación electrónica*, núm. 120, 2012.

ORDOÑEZ SOLÍS, D.: "El derecho al olvido en Internet y la Sentencia Google Spain", *Revista Aranzadi Unión Europea*, núm. 6, 2014.

- "La reformulación de los derechos fundamentales en la era digital: privacidad, libertad de expresión y propiedad intelectual", *Revista Europea de Derechos Fundamentales*, núm. 25, 2015.

ORENES RUIZ, J. C.: "Publicidad de sentencias, Internet y protección de datos de carácter persona", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 30, 2012.

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*, núm. 2, 1994.

ORZA LINARES, R. M.: "Derechos Fundamentales e Internet: nuevos problemas, nuevos retos", *Revista de Derecho Constitucional Europeo*, núm. 18, 2012.

- "El derecho al olvido en Internet: algunos intentos para su regulación legal", en CORREDOIRA, L. y COTINO HUESO, L. (dirs.): *Libertad de expresión e información en la Red. Amenazas y protección de los derechos personales*, Centro de Estudios Políticos y Constitucionales, Madrid, 2013.

OUBIÑA BARBOLLA, S.: "Cambio de enfoque en la cooperación judicial penal y policial en la UE en relación con la transmisión de datos personales: las nuevas propuestas normativas y la STJUE de 8 de abril de 2014", en COLOMER HERNÁNDEZ, I. (dir.), OUBIÑA BARBOLLA, S. (dir.): *La transmisión de datos personales en el seno de la cooperación judicial penal y policial en la Unión Europea*, Cizur Menor (Navarra), Aranzadi, 2015.

PARDO FALCÓN, J.: “Los derechos del artículo 18 de la Constitución en la Jurisprudencia del Tribunal Constitucional”, *Revista Española de Derecho Constitucional*, núm. 34, 1992.

PAUNER CHULVI, C.: "Implicaciones del futuro reglamento europeo sobre protección de datos en la libertad de información", en FAYOS GARDÓ, A (coord.): *Los derechos a la intimidad y a la privacidad en el siglo XXI,* Dykinson, Madrid, 2014.

- "La actividad periodística en los ordenamientos nacionales y europeos de protección de datos" en RALLO LOMBARTE, A y GARCÍA MAHAMUT, R. (eds.): *Hacia un nuevo Derecho Europeo de Protección de Datos*, Tirant lo Blanch, Valencia, 2015.

- "La libertad de información como límite al derechos a la protección de datos personales: la excepción periodística", *Teoría y realidad constitucional,* núm. 36, 2015.

PAZOS CASTRO, R.: "El derecho al olvido frente a los editores de las hemerotecas digitales", *Indret*: *revista de análisis del derecho*, núm. 4, 2016.

- “El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales ¿una relación imposible?”, *Indret*: *revista de análisis del derecho*, núm. 1, 2015.

- "El mal llamado 'derecho al olvido' en la era de Internet", *Boletín del Ministerio de Justicia*, núm. 2183, 2015.

PERALES ALBERT, A.: "Entre el derecho al olvido y el derecho a conocer: consecuencias derivadas de la doctrina del Tribunal de Justicia de la Unión Europea", *Revista Europea de Derechos Fundamentales*, núm. 25, 2015.

PÉREZ CAMBERO, R.: “Análisis de las últimas e importantes novedades en protección de datos: Reglamento Europeo de Protección de Datos y Escudo de Privacidad UE- EE.UU”, *Actualidad Administrativa,* núm. 11, 2016.

PÉREZ FRANCESCH, J. L. y DOMÍNGUEZ GARCÍA, F.: " El indulto como acto del gobierno: una perspectiva constitucional (Especial análisis del 'caso Liaño')", *Revista de Derecho Político*, núm. 53, 2002.

PÉREZ LUÑO, A. E.: *Cibernética, Informática y Derecho. Un análisis metodológico*, Publicaciones del Real Colegio de España, Bolonia, 1976.

- “Informática y Libertad. Comentario al artículo 18.4 de la Constitución Española”, *Revista de Estudios Políticos,* núm. 24,1981.

- “Intimidad y protección de datos personales: del Habeas Corpus al Habeas Data” en GARCÍA SAN MIGUEL, L. (editor), *Estudios sobre el Derecho a la intimidad*, Tecnos, Madrid, 1992.

- “La protección de datos personales del menor en Internet”, *Revista Española de Protección de Datos*, núm. 5, 2008.

- "Los derechos humanos en la sociedad tecnológica", en AA.VV.: *Libertad informática y leyes de protección de datos personales*, Cuadernos y Debates, núm. 21, Centro de Estudios Constitucionales, Madrid, 1989.

- *Nuevas tecnologías, sociedad y derecho: el impacto de socio-jurídico de las nuevas tecnologías de la información*, Fundesco, Madrid, 1987.

- “Nuevos derechos fundamentales de la era tecnológica: la libertad informática” *Anuario de Derecho Público. Estudios Políticos*, núm. 2, 1989/90.

PIÑAR MAÑAS, J. L.: "Defiendo la privacidad. No me he pasado al enemigo”, *El País*, 8 de junio de 2014.

- *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009.

- “Introducción: hacia un nuevo modelo europeo de protección de datos” en AA.VV.: *Reglamento general de protección de datos hacia un nuevo modelo europeo de privacidad,* Reus, Madrid*,* 2017.

PIZARRO MORENO, E.: "Celada al Derecho al olvido", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 41, 2016.

PLATERO ALCÓN, A.: " El derecho al olvido en Internet. El fenómeno de los motores de búsqueda", *Revista Opinión Jurídica*, vol. 15, núm. 29, 2016.

- "El derecho a ser olvidado en España: estado de la cuestión más de dos años después de la STJUE de 13 de mayo de 2014", *Anuario de la Facultad de Derecho Universidad de Extremadura*, núm. 32, 2017.

- "El derecho a ser olvidado en Europa", *Diálogos de Saberes*, núm. 42, 2015.

-"La aplicación e interpretación del Derecho al olvido en la Jurisprudencia española", en BUENO DE MATA, F (coord.): *FODERTICS 6.0: Los nuevos restos del derecho ante la era digital,* Comares, Granada, 2017.

PUENTE ESCOBAR, A.: “Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal”, en PIÑAR MAÑAS, J. L.: *Protección de datos de carácter personal en Iberoamérica*, Tirant lo Blanch, Valencia, 2005.

- "El derecho al olvido", en PÉREZ BES, F (coord.): *El derecho de Internet*, Atelier, Barcelona, 2016.

PUYOL MONTERO, J.: "Los principios del derecho a la protección de datos" en AA. VV.: *El Reglamento general de protección de datos hacia un nuevo modelo europeo de privacidad,* Reus, Madrid*,* 2017.

RALLO LOMBARTE, A.: "A partir de la protección de datos: el derecho al olvido y su protección”, *Revista TELOS*, 2010.

- "El derecho al olvido en el tiempo de Internet. La experiencia española". Disponible en Internet: http://repositori.uji.es/xmlui/bitstream./ handle /10234/122643/ID66654.pdf?sequence%20=1.

- *El derecho al olvido en Internet, Google versus España*, Centro de Estudios Politicos y Constitucionales, Madrid, 2014.

- "El Tribunal de Justicia de la Unión Europea como Juez garante de la privacidad en Internet", *Teoría y Realidad Constitucional*, núm. 39, 2017.

- "El debate europeo sobre el derecho al olvido en Internet" en RALLO LOMBARTE, A y GARCÍA MAHAMUT, R. (eds.): *Hacia un nuevo Derecho Europeo de Protección de Datos,* Tirant lo Blanch, Valencia, 2015.

- "La garantía del derecho constitucional a la protección de datos personales en los órganos judiciales", *Justicia y Ciudadanía, Instituto Andaluz de Administración Pública,* núm. 5 2009.

RAMOS GONZALEZ, S. MILÁ RAFAEL, R. GILI SALDAÑA, M. A. y SALVADOR CORDECH, P.: "Las Sentencias del Tribunal Constitucional deben publicarse íntegras: Comentario a la Sentencia del Tribunal Constitucional, Sala Primera, 114/2006, de 5 de abril de 2006 (MP: Pablo Pérez Tremps). Recurso de amparo 24-2002 (BOE núm. 110, de 9 de mayo de 2006)", *Indret: revista para el análisis del derecho*, núm. 3, 2006.

RAMOS PRIETO, J: "El nuevo instrumento en la lucha contra el fraude fiscal: la publicación de los datos personales de las sentencias condenatorias por determinados delitos contra la Hacienda Pública", en COLOMER HERNANDEZ, I (dir.): *Cesión de datos* personales *y evidencias entre procesos penales y procedimientos administrativos sancionadores y tributarios,* Aranzadi, Cizur Menor (Navarra), 2017.

REBOLLO DELGADO, L.: "El derecho a la propia imagen y la imagen como dato", *Revista Española de protección de datos*, núm. 5, 2008.

- *Manual de Protección de Datos,* Dykinson, Madrid, 2014.

- *Vida privada y protección de datos en la Unión Europea*, Dykinson, Madrid, 2008.

REUSSER MONSÁLVEZ, C.: "Periodismo digital versus Derecho al olvido. Sobre porqué los medios de prensa deberían eliminar sus contenidos en Internet", en BUENO DE MATA, F (coord.): *FODERTICS 6.0: Los nuevos restos del derecho ante la era digital*, Comares, Granada, 2017.

REY MARTÍNEZ, F.: *Eutanasia y derechos fundamentales*, Centro de Estudios Políticos y Constitucionales, Madrid, 2008.

RODRÍGUEZ ÁLVAREZ, J. L.: "Transparencia y protección de datos personales: criterio legales de conciliación", en CANALS AMETLLER, D (ed.): *Datos. Protección, Transparencia y Buena Regulación,* Documenta Universitaria, Girona, 2016.

RODRÍGUEZ-IZQUIERDO SERRANO, M.: "El tribunal de justicia y los derechos en la sociedad de la información: privacidad y protección de datos frente a libertades informativas", *Revista de Derecho Constitucional Europeo,* núm. 24, 2015. Disponible en Internet: http://www.ugr.es /~redce /REDCE24/ReDCEsumario24.htm

- "Pluralidad de jurisdicciones y tutela de derechos: los efectos de la integración europea sobre la relación entre el juez ordinario y el Tribunal Constitucional", *Revista Española de Derecho Constitucional*, núm. 107, 2016.

- "Protección de datos personales y libertades de comunicación pública en ponderación: líneas y límites de la jurisprudencia constitucional", en MORALES ARROYO, J. M (dir.): *Recurso de Amparo, Derechos fundamentales y trascendencia constitucional,* Aranzadi, Cizur Menor (Navarra), 2014.

RODRÍGUEZ RUIZ, B.: "*El secreto de las comunicaciones: tecnología e intimidad,* McGraw-Hill-Interamericana de España, Madrid, 1998.

- La Carta de Derechos Fundamentales de la Unión Europea: acuerdos y desacuerdos" en LEÑERO BOHÓRQUEZ, R (coord.): *Una Constitución para la ciudadanía de Europa,* Aranzadi, Cizur Menor (Navarra), 2004.

ROIG BATALLA, A.: "Derecho Público y Tecnologías de la información y la comunicación", *Revista catalana de dret public*, núm. 35, 2007.

- "El anonimato y los límites a la libertad en internet" en COTINO HUESO, L. (coord.): *Libertad en Internet: la red y las libertades de expresión e información*, Tirant lo Blanch, Valencia, 2007.

ROLLA, G.: "El difícil equilibrio entre el Derecho a la información y la tutela de la dignidad y la vida privada: breves consideraciones a la luz de la experiencia italiana", *Cuestiones constitucionales*, *Revista Mexicana de Derecho Constitucional*, núm. 7, 2002.

RUBIO LLORENTE, F.: "Mostrar los derechos sin destruir la Unión (Consideraciones sobre la Carta de Derechos Fundamentales de la Unión Europea)", *Revista Española de Derecho Constitucional*, núm. 22, 2002.

RUIZ MIGUEL, C.: “El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: Análisis crítico”, *Revista de Derecho Comunitario Europeo*, núm. 14, 2003.

- *La configuración constitucional del derecho a la intimidad,* Tecnos, Madrid 1995.

SÁNCHEZ SAUS, R.: "El derecho al olvido", *Diario de Sevilla*, 15 de mayo de 2014. Disponible en Internet: http://www.diariodesevilla.es/opinion/articulos/de recho- olvido_0_807219443.html

SANCHO LÓPEZ, M.: “Consideraciones procesales del ejercicio del derecho al olvido: examen de jurisprudencia reciente y del nuevo marco legal", *Revista Aranzadi de Derecho y nuevas tecnologías*, núm. 41, 2016.

SARTOR, G. y VIOLA DE AZEVEDO CUNHA, M.: “The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents”, *International Journal of Law and Information Technology*, vol. 18, núm. 4, 2010.

SCHMIDT, W.: "Die bedrohte Entscheidungsfreiheit", *JZ,* 1974.

SCHWABE, J.: *Jurisprudencia del Tribunal Constitucional Federal Alemán Extractos de las sentencias más relevantes*, KONRAD-ADENAUER-STIFTUNG e. V, México, 2009.

SEMPERE RODRÍGUEZ, C.: "El artículo 18 derecho al honor, a la intimidad y a la propia imagen”, en ALZAGA VILLAAMIL, O.: *Comentarios a la Constitución Española de 1978,* tomo II, Edersa, Madrid, 2006.

SERRANO PÉREZ, M. M.: *El derecho fundamental a la protección de datos. Derecho Español y Comparado,* Thomson-Civitas, Madrid, 2003.

- *Manual de Protección de datos,* Dykinson, Madrid, 2014.

SILVA DE LAPUERTA, M.: "El 'derecho al olvido' como aportación española y el papel de la abogacía del Estado*", Actualidad Jurídica Uría Menéndez*, núm. 38, 2014.

SIMÓN CASTELLANO, P.: "El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos", en CORREDOIRA, L. y COTINO HUESO, L. (dirs.): *Libertad de expresión e información en la Red. Amenazas y protección de los derechos personales*, Centro de Estudios Políticos y Constitucionales, Madrid, 2013.

- "El encaje constitucional del derecho al olvido digital en perspectiva comparada", *Datos personales.org*, núm. 54, 2012.

- *El reconocimiento del derecho al olvido digital en España y en la Unión Europea*, Bosch, Hospitalet de Llobregat, 2015.

- *El régimen constitucional del derecho al olvido*, Tirant lo Blanch, Valencia, 2012.

- "La UE obliga a Google a retirar enlaces con información lesiva", *El País,* 13 de mayo de 2014.

SOLOVE, D. J.: “I´ve got nothing to hide and other misunderstandings of privacy”, *San Diego Law Review*, 2007.

TÉLLEZ AGUILERA, A.: *La protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores,* Edisofer, Madrid, 2002.

TENE, O.: “What Google Knows: Privacy and Internet Search Engines”, *Utah Law Review,* núm.4, 2008.

TOMÁS MALLÉN, B. S.: "Privacidad versus seguridad en el ámbito europeo" en FAYOS GARDÓ, A y CONDE COLMENERO, P (coord.): *Los derechos a la intimidad y a la privacidad en el siglo XXI,* Dykinson, Madrid, 2014.

- "Transparencia y protección de datos: nuevos desafíos para la garantía europea de los derechos fundamentales", en RALLO LOMBARTE, A y GARCÍA MAHAMUT, R. (eds.): *Hacia un nuevo Derecho Europeo de Protección de Datos*, Tirant lo Blanch, Valencia, 2015.

TOURIÑO PENA, A.: *El derecho al olvido y a la intimidad en Internet*, Catarata, Madrid, 2014.

TRONCOSO REIGADA, A.: *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal,* Thomson Reuters-Civitas, Madrid, 2010.

- "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, núm. 43, 2012.

- *La protección de datos personales en busca del equilibrio*, Tirant lo Blanch, Valencia, 2010.

- "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", *Cuadernos de Derecho Público,* núm. 19-20, 2003.

- "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*, núm.15, 2012.

- "Las redes sociales a la luz de la Propuesta de Reglamento general de Protección de Datos Personales: parte dos ", *IDP: revista de Internet, Derecho y Política*, núm. 16, 2013.

- "El derecho al olvido digital de los médicos a la luz de la Sentencia del Tribunal Supremo de 15 de octubre de 2015", *I+S Informática y salud*, núm. 114, 2015.

- "El derecho al olvido en Internet a la luz de la propuesta de Reglamento General de Protección de Datos Personales", *Datos Personales. org.* núm. 59, 2012.

- "Transparencia administrativa y protección de datos personales", en TRONCOSO REIGADA, A. (dir.): *Transparencia administrativa y protección de datos personales, V Encuentro entre Agencias Autonómicas de Protección de datos*, Agencia de Protección de Datos de la Comunidad de Madrid, 2008.

- "Reutilización de información pública y protección de datos personales", *Revista General de información y documentación*, vol.19, núm. 1, 2009.

URIARTE LANDA, I.: “Ámbito de aplicación material”, en AA.VV.: *El Reglamento general de protección de datos hacia un nuevo modelo europeo de privacidad,* Reus, Madrid*,* 2017.

VAN ALSENOY, B, KUCZERAWY, A y AUSLOOS, J.: “Search engines after Google Spain: internet@liberty or privacy@peril?”, *ICRI Research Paper*, núm. 15, 2013.

VILASAU SOLANA, M.: "El caso *Google Spain*: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido (análisis de la STJUE de 13 de mayo de 2014)”, *IDP: revista de Internet, Derecho y Política,* núm. 18, 2014.

VILLAVERDE MENÉNDEZ, I.: "Ciberconstitucionalismo. Las TIC y los espacios virtuales de los derechos fundamentales", *Revista catalana de dret públic*, núm. 35, 2007.

- "La intimidad, ese 'terrible derecho' en la era de la confusa publicidad virtual", *Espaço Jurídico*, vol. 14, núm. 3, 2013.

- "La protección de los datos personales en los estatutos de autonomía. El papel de las agencias autonómicas de protección de datos", *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 20, 2006.

- “Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993”, *Revista Española de Derecho Constitucional*, núm. 41, 1994.

WARREN, S. y BRANDEIS, L.: *El derecho a la intimidad*, Civitas, Madrid, 1996.

WESTIN, A.: *Privacy and Freedom*, Atheneum, New York, 1967.

ZÁRATE ROJAS, S.: "La problemática entre el derecho al olvido y la libertad de prensa", *Derecom*, núm. 13, 2013.