

*EL DERECHO AL OLVIDO EN INTERNET
COMO NUEVO DERECHO
FUNDAMENTAL EN LA SOCIEDAD DE LA
INFORMACIÓN. PERSPECTIVA
CONSTITUCIONAL ESPAÑOLA Y
EUROPEA.**

*Mario Hernández Ramos***

SUMARIO:

Planteamiento de la cuestión; 1) El derecho fundamental a la protección de datos de carácter personal: delimitación conceptual; a) Su diferenciación respecto al derecho a la intimidad; b) El contenido esencial del derecho a la protección de datos de carácter personal: contenido, facultades y límites; c) El ejercicio de las facultades derivadas de este contenido esencial: el poder de disposición de datos personales y el origen del derecho al olvido en internet. Los derechos de oposición y cancelación; 2) El derecho al olvido en internet como parte del contenido esencial del derecho a protección de datos personales; a) La cuestión prejudicial sobre Google y el derecho de cancelación y oposición de datos personales; b) El concepto del derecho al olvido en internet y la ponderación de derechos. A modo de conclusión; 3. Fuentes de consulta.

* Este artículo ha sido elaborado en el marco de los proyectos de investigación "Estatuto de los Jueces e Independencia Judicial" DER2011-29207-C02-01 y "La protección de los derechos en Latinoamérica: los casos de Brasil, Bolivia y Chile", DER2009-11776

** Doctor en Derecho por la Universidad de Salamanca. Licenciado en Derecho con Premio Extraordinario por la misma Universidad. Profesor ayudante Facultad de Derecho, Universidad de Salamanca, España.

Recibido: 17 de febrero de 2013

Aceptado: 22 de febrero de 2013

Resumen:

El internet hoy en día se ha convertido en una herramienta indispensable en la sociedad, pues coloca al alcance de las personas información y conocimiento a nivel mundial. Actualmente en esta era digital la información personal se almacena masivamente y es fácil tener acceso a la misma.

Con todos estos avances surgen a la par diversas necesidades y derechos como el de protección de datos y el derecho a la intimidad, refiriéndose el primero a la garantía que tienen los ciudadanos de poder disponer sobre sus datos personales; y el segundo a poder excluir ciertos datos de una persona del conocimiento ajeno.

A raíz de la aparición de ambos derechos el Estado debe de procurar los medios apropiados para el respeto a dichos intereses de respeto, con la prudente determinación de no hacer retroceder este gran avance de la tecnología.

Palabras clave: internet, derecho al olvido, derecho a la intimidad, datos personales, protección de datos.

Abstract:

The Right to Forget in internet as new fundamental right in the information society. Spaniard and European Constitutional Perspective. Nowadays the internet has become a new essential tool for the society, it is so that brings information and knowledge in a global level. Currently in this digital age the personal information is stored massively and easy to access.

Diverse needs and rights parallel emerge as data protection, intimacy rights meaning be able to access to personal data and exclude certain alien data respectively.

In the wake of both rights, the State must seek appropriate means of respect concerning these respect interests, with prudent determination and not back up this great technologic progress.

Key words: internet, Right to forget, Intimacy right, personal data, data protection.

Planteamiento de la cuestión

La transmisión de conocimientos o información tanto de una persona a otra como de una generación a la siguiente, ha sido una de los mayores retos y una las mayores pretensiones perseguidas por el ser humano desde sus orígenes. La tenencia de información y conocimiento siempre ha significado poder y bienestar. La imprenta, la revolución tecnológica del siglo XX con la radio, la televisión y la telefonía, y sobre todo internet en los últimos años, han puesto a disposición de las personas la posibilidad de acceder en tiempo real a información y conocimiento a nivel mundial. Hoy en día es posible obtener información en cualquier momento, con independencia de la fecha en la que se haya generado o publicado el dato y es posible obtenerla desde cualquier lugar, con independencia de la mayor o menor lejanía geográfica. Internet ha supuesto una herramienta esencial para el ciudadano, que ha podido emanciparse de versiones oficiales, capciosas y tendenciosas de interesados medios de comunicación, formar sus propias opiniones y demandas, y poder perseguirlas. Esta información y conocimiento contribuyen de manera esencial a la transparencia en la vida pública, para mejorar la calidad democrática de países con modelos democráticos ya asentados; pero también ha jugado un papel determinante en aquellos movimientos sociales que demandan zafarse de dictaduras y opresiones de muy diverso género en todo el mundo. Un ejemplo paradigmático lo constituyen las revoluciones en países árabes bautizadas como "la primavera árabe", y para cuyo inicio y triunfo fue imprescindible el acceso a la información libre que facilita internet.

A lo largo de la historia de la humanidad guardar la información y transmitirla siempre ha sido caro y, por tanto, algo limitado. Pero en la era digital esa relación se ha invertido: grabar, guardar, almacenar información es muy barato y, por contra, borrar información exige dedicación, tiempo y dinero. Hoy, la información personal se almacena masivamente y es fácilmente accesible para cualquiera con sólo tener una terminal de acceso a internet. Datos o informaciones recientes o lejanas, procedentes de las fuentes más diversas, están al alcance de cualquiera y para cualquier finalidad. Por ello, junto a la muy positiva contribución al

disfrute y efectividad de los derechos fundamentales por parte de la sociedad que ha supuesto internet, ha de tenerse en cuenta que también supone una herramienta muy potente para la vulneración de otros derechos fundamentales. El acto de presencia de internet en las sociedades actuales supone abrir las puertas, sin barreras ni temporales ni geográficas a una cantidad de información, conocimientos y opiniones inabarcable. En esta avalancha diaria de información los buscadores, una herramienta que nos facilita la localización de aquellos contenidos o información en la que estemos interesados, han cobrado un protagonismo indiscutible. Sin embargo, al mismo tiempo, su potencial resulta cada vez más problemático, ya que permiten localizar instantáneamente, salvando cualquier barrera de tiempo y espacio, información de todo tipo relativa a una persona. Las capacidades de recuperación y agregación de estos motores de búsqueda pueden ocasionar, y lo están haciendo de hecho a nivel mundial, considerables perjuicios a los individuos, tanto en su vida personal como en sus relaciones sociales.¹

Este es el escenario en el que se van a desarrollar las siguientes páginas, centrándonos principalmente en la posición de fragilidad en la que los individuos se encuentran frente a internet y estos buscadores. En este sentido empieza a cobrar cada vez más importancia el derecho fundamental a la protección de datos.²

En España este aumento se evidencia en el número creciente de demandas de protección de datos personales solicitadas a la Agencia Española de

¹ A nivel europeo se ha constatado con diversos estudios una percepción generalizada de la opinión pública de que existen riesgos significativos, especialmente por lo que se refiere a la actividad en línea. Véase el interesante Eurobarómetro especial (EB) 359, *Data Protection and Electronic Identity in the EU* (Protección de datos e identidad electrónica en la UE, 2011). Disponible en: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf; así como el *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, enero de 2010*. http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

² Art. 18.4 Constitución Española (CE), art. 8 Convenio Europeo de Derechos Humanos (CEDH) y art. 10 Carta de Derechos Fundamentales de la Unión Europea. También está regulado por los arts. 5, 6, 8 y 9 del Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo el 28 de enero de 1981 y, por último, 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, y muy en especial su art. 13.

Protección de Datos (en adelante AEPD).³ Como consecuencia de esta concienciación por parte de la sociedad de la protección de sus derechos fundamentales en la red, se empieza a demandar ampliar el contenido de ese derecho fundamental de la protección de datos con el llamado "derecho al olvido".

Este derecho al olvido se demanda frente a páginas web concretas e identificadas, pero también frente a buscadores. La reacción de páginas web y buscadores no ha sido la misma, y mientras las primeras suelen acatar las decisiones de la AEPD a raíz de demandas de cancelación y oposición al tratamiento de los datos, en virtud de lo establecido en Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (en adelante LOPD) y su Reglamento de Desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre (en adelante RLOPD), los buscadores, concretamente Google, se ha opuesto a acatar estas decisiones y ha acudido a la jurisdicción contencioso-administrativa, alegando que deben ser las páginas que incluyeron la información las que deberían satisfacer las demandas de cancelación y oposición de los titulares, además de proteger derechos fundamentales como la libertad de expresión e información. Es tal el punto de indeterminación en este tema debido a la

³ Según datos de la memoria del 2011 de la Agencia Española de Protección de Datos, las consultas al servicio de atención al ciudadano no sólo consolidan la tendencia de crecimiento de años anteriores, sino que se han ampliado en un porcentaje significativo que se aproxima al 30% (28,4%), alcanzando la cifra de 134.635. Asimismo, se han incrementado los accesos a la página web de la Agencia que se aproximan a los 3 millones (2.892.516), con un promedio diario cercano a los 8.000 accesos (7.923). La forma de consulta sobre la normativa de la protección de datos a la Agencia más utilizada ha sido el canal telefónico, con 113.579 consultas. También se realizan consultas por escrito (17.715) y de manera presencial, aunque disminuye respecto al año anterior (3.341 consultas frente a 4.093). El ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO) se mantiene como principal objeto de consulta por los ciudadanos en un porcentaje próximo al 30% (28,81%). Más de la mitad de estas cuestiones (50,35%) están relacionadas con el ejercicio del derecho de cancelación, lo que resulta indicativo del rechazo que a los ciudadanos les suscita que se utilice indebidamente su información personal. Este indicador se ve reforzado con el amplio porcentaje de quienes consultan acerca del modo de ejercer el derecho de oposición al tratamiento de sus datos personales, que asciende al 27,85% de las que versan sobre el ejercicio de derechos. Estas últimas consultas adquieren especial relevancia si se tiene en cuenta que el ejercicio del derecho de oposición constituye una de las principales vías para hacer frente al fenómeno de la indexación de datos publicados en medios de comunicación y en diarios y boletines oficiales por parte de los buscadores en internet, posibilitando el acceso universal y permanente a la información disponible en internet. En definitiva, algo más del 80% de las consultas sobre el ejercicio de derechos están relacionadas con la decisión de los ciudadanos de evitar el tratamiento de sus datos personales. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2011/common/Memoria_2011.pdf

antigüedad de la Directiva que la Sala de lo Contencioso-Administrativo de la Audiencia Nacional ha planteado una cuestión prejudicial al Tribunal de Justicia de la Unión Europea para que resuelva estas cuestiones.

Las siguientes páginas tratan de ilustrar un poco mejor esta discusión, adoptando un enfoque constitucional. Por ello, se estudiará en primer lugar el contenido esencial del derecho a la protección de datos personales con el objetivo de determinar si el pretendido derecho al olvido en internet forma parte de este contenido esencial, con las consecuencias que ello conllevaría. En segundo lugar, se abordará un estudio introductorio del significado del derecho al olvido y la problemática suscitada entre Google y la AEPD.

1) El derecho fundamental a la protección de datos de carácter personal: delimitación conceptual

Como ha señalado de manera constante el Tribunal Constitucional (en adelante TC) el precepto del art. 18.4 CE "contiene un instituto de garantía de los derechos a la intimidad y al honor del pleno disfrute de los restantes de los ciudadanos". Al mismo tiempo, este precepto es "además, en sí mismo, un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona proveniente de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama "la informática".⁴

Por tanto, el art. 18.4 CE consagra, por un lado, un derecho fundamental al ciudadano y por otro un mandato al legislador.

a) Su diferenciación respecto al derecho a la intimidad

Hoy en día la informática e internet están presentes en todos los ámbitos de las relaciones sociales. En especial, es de destacar la proliferación de

⁴ Afirmación realizada por primera vez en la STC 254/1994, de 9 de mayo, FJ 6, y reiterada en las SSTC 292/2000, de 30 de noviembre FJ 5; 290/2000, de 30 de noviembre, FJ 7; 202/1999, de 8 de noviembre; FJ 2; 94/1998, de 4 de mayo, FJ 6; 11/1998, FJ 4; 143/1994, FJ 7.)

instrumentos de recopilación de información hasta el punto de que una persona pueda ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero de entidades públicas o privadas sino también si han sido trasladados a otro y con qué finalidad. Es necesario, por tanto, estar atentos al uso desviado que se puede efectuar de esta información y a la eventual invasión de la esfera privada de los ciudadanos afectados. En palabras del Tribunal Constitucional, "es un hecho también admitido en la jurisprudencia de este Tribunal que el incremento de medios técnicos de tratamiento de la información hace precisa la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento, aun indirecto" (...) "y a incrementar las facultades de conocimiento y control que se otorgue al ciudadano, para salvaguardar el núcleo esencial de su derecho".⁵ En este sentido, el Tribunal Constitucional es consciente de que tanto la Administración Pública como agentes privados almacenan y utilizan cotidianamente datos personales, por ello "no es posible aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión".⁶ Es imprescindible establecer las garantías adecuadas frente a un uso potencialmente invasor de la vida privada del ciudadano, para que un sistema normativo autorizado para la recogida de datos, incluso con fines legítimos y de contenido aparentemente neutro, no vulnere el derecho a la intimidad.⁷

En consecuencia, el Tribunal Constitucional ha sentenciado que el derecho fundamental a la intimidad (art. 18.1 CE) concebido únicamente como facultad negativa, no constituye por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico. En este sentido, "la garantía de la intimidad, *latu sensu*, adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos

⁵ STC 254/1993, de 9 de mayo, FJ 7.

⁶ STC 254/1993, de 9 de mayo, FJ 7.

⁷ STC 143/1994, de 9 de mayo, FJ 7.

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".⁸

Con la inclusión del vigente art. 18.4 CE, el Constituyente puso de relieve que era consciente de los riesgos que podría entrañar el uso de la informática y encomendó al legislador la garantía tanto de ciertos derechos fundamentales como del pleno ejercicio de los derechos de la persona.⁹

El art. 18.4 CE establece que "La ley limitará el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno uso de sus derechos". Como afirma DIEZ PICAZO, "la redacción de este precepto no es afortunada, ya que limitar el uso de la informática es, además de poco factible, escasamente deseable. No tiene sentido oponerse al progreso tecnológico. Cosa distinta, que es lo que sin duda el Constituyente quiso decir, es poner coto a los eventuales abusos en el empleo de nuevas tecnologías".¹⁰ Este derecho fundamental a la protección de datos comparte con el derecho a la intimidad el objetivo de proteger la vida privada personal y familiar. Sin embargo, la principal diferencia entre ambos derechos es la atribución al titular del derecho del art. 18.4 CE un "haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos". Ambos derechos fundamentales, por tanto, tienen una función, un objeto y un contenido diferente.¹¹

La *función* del derecho fundamental a la intimidad del art. 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

⁸ STC 11/1998, de 13 de enero, FJ 4.

⁹ STC 292/2000, de 30 de noviembre, FJ 4.

¹⁰ DÍEZ PICAZO, L.M. "Sistema de derechos fundamentales". Thomson Civitas, 3ª ed., Navarra, 2008, p. 325.

¹¹ STC 292/2000, de 30 de noviembre, FJ 5.

voluntad,¹² "necesario - según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana".¹³ 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 derecho del afectado. El derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno,¹⁴ es decir, "el poder de resguardar su vida privada de una publicidad no querida. Por el contrario, el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebida de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin."¹⁵

De esta diferente función y finalidad se deriva por tanto que el *objeto de protección* de ambos derechos fundamentales no son coincidentes, sino que es más amplio en el caso del derecho a la protección de datos, pues extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a "la esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal", como el derecho al honor, y al pleno ejercicio de los derechos de la persona (art. 18.4 CE). Por tanto, el derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos datos "que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado. De este modo, el objeto de protección del

¹² STC 144/1999, de 22 de julio, FJ 8.

¹³ STC 231/1988, de 2 de diciembre, FJ 3.

¹⁴ SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4.

¹⁵ STC 292/2000, de 30 de noviembre, FJ 6.

derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. De todo esto se deriva que la calificación de "carácter personal" a los datos no quiere decir que sólo queden amparados de protección los relativos a la vida privada o íntima de la persona, sino que se protegen todos aquellos que contribuyan a 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."¹⁶

Por último, el *contenido* del derecho a la protección de datos difiere del derecho a la intimidad en que este último confiere a su titular el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido,¹⁷ mientras que 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 que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los ya mencionados deberes de hacer. Ésto implica el derecho a que se requiera "el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y

¹⁶ STC 292/2000, de 30 de noviembre, FJ 6.

¹⁷ SSTC 73/1982, de 2 de diciembre, FJ 5; 110/1984, de 26 de noviembre, FJ 3; 89/1987, de 3 de junio, FJ 3; 231/1988, de 2 de diciembre, FJ 3; 197/1991, de 17 de octubre, FJ 3, y en general las SSTC 134/1999, de 15 de julio, 144/1999, de 22 de julio, y 115/2000, de 10 de mayo.

uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales".¹⁸ Con estas notas de diferenciación respecto del derecho a la intimidad se ha trazado ya un claro contorno conceptual de lo que debería entenderse por derecho a la protección de datos. Nos interesa ahora ahondar en el contenido esencial de este derecho, como medida de protección y garantía (art. 53.1 CE), para lo cual acudiremos también a la clara y concisa jurisprudencia constitucional sobre la materia.

b) El contenido esencial del derecho a la protección de datos de carácter personal: contenido, facultades y límites

Debido a la constante evolución y desarrollo de la tecnología, el objeto de regulación y protección del art. 18.4 CE ha sufrido un imparable crecimiento, que aumenta día a día. Es por ello que la legislación que intenta embridar jurídicamente este campo se queda anticuada con rapidez. No obstante, en las numerosas sentencias que el Tribunal Constitucional ha dictado sobre este derecho, puede identificarse claramente su contenido esencial,¹⁹ tanto por su naturaleza jurídica o "el modo de concebir o de configurar cada derecho",²⁰ como por sus bienes o intereses jurídicamente protegidos.²¹

El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona. Esta potestad incluye poder decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, así como permitir al individuo saber quién

¹⁸ STC 292/2000, de 30 de noviembre, FJ 6; véase también la STC 254/1993, de 20 de julio, FJ 7.

¹⁹ STC 11/1981, de 8 de abril, FJ 8.

²⁰ "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", STC 11/1981, de 8 de abril, FJ 8.

²¹ Contenido esencial como "esencialidad del contenido del derecho para hacer referencia a aquella parte del contenido del derecho que es absolutamente necesaria para que los intereses jurídicamente protegibles, que dan vida al derecho, resulten real, concreta y efectivamente protegidos. 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", STC 11/1981, de 8 de abril, FJ 8.

posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

Estos poderes de *disposición* y *control* sobre los datos personales constituyen por tanto el núcleo esencial del contenido del derecho fundamental a la protección de datos, y se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a *consentir* sobre la recogida y uso de sus datos personales, y a *saber* de los mismos. Para hacer efectivo ese contenido resultan indispensables el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin; y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que *ponga fin a la posesión y empleo* de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele.²²

Estas facultades forman parte también del contenido esencial del derecho de protección de datos de carácter personal²³ y deben de integrar la

²² STC 292/2000, de 30 de noviembre, FJ 7. En opinión del defensor del pueblo, "los derechos de los afectados a ser informados y a consentir así como los de acceso, rectificación y cancelación, integran el derecho fundamental de todos a controlar la recogida y el uso de aquellos datos personales que puedan poseer tanto el Estado y otros entes públicos como los particulares, lo que forma parte del contenido esencial (art. 53.1 CE) de los derechos fundamentales a la intimidad personal y familiar (art. 18.1 CE) y a la autodeterminación informativa (art. 18.4 CE)", STC 292/2000, de 30 de noviembre, FJ 2.

²³ STC 292/2000, de 30 de noviembre, FJ 10.

regulación legal que desarrolle y garantice el disfrute de este derecho. Por tanto, las facultades legalmente atribuidas a los sujetos concernidos y las consiguientes posibilidades de actuación de éstos son necesarias para el reconocimiento e identidad constitucionales del derecho fundamental a la protección de datos. Asimismo, esas facultades o posibilidades de actuación son absolutamente necesarias para que los intereses jurídicamente protegibles, que constituyen la razón de ser del aludido derecho fundamental, resulten real, concreta y efectivamente protegidos. De manera que, privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo estará también de su derecho fundamental a la protección de datos, puesto que, como concluyó en este punto la STC 11/1981, de 8 de abril (FJ 8), "se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección".²⁴

Este contenido esencial es el mismo que el establecido por los textos internacionales vinculantes para España en la materia, como por ejemplo la Resolución 45/95 de la Asamblea General de las Naciones Unidas donde se recoge la versión revisada de los Principios Rectores aplicables a los Ficheros Computadorizados de Datos Personales; del Convenio para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal hecho en Estrasburgo el 28 de enero de 1981;²⁵ Directiva 95/46, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos;²⁶ el art. 16 del Tratado de Funcionamiento de la Unión

²⁴ STC 292/2000, de 30 de noviembre, FJ 10.

²⁵ Arts. 5, 6, 7, 8 y 11.

²⁶ La Directiva 95/46/CE es la piedra angular de la legislación vigente de la UE en materia de protección de datos. Fue adoptada en 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos datos entre los estados miembros. Se complementó mediante la Decisión Marco 2008/977/JAI, en su calidad de instrumento general a escala de la Unión para la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, DO L 350 de 30.12.2008, p. 60). Existe una propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes a efectos de la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y a la libre circulación de estos datos, COM (2012) 10 final.

Europea, introducido por el Tratado de Lisboa,²⁷ así como el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea.

Otra cuestión a tener en cuenta en el ejercicio de estas facultades son sus límites. Como subrayó el Tribunal de Justicia de la UE²⁸ (en adelante TJUE), el derecho a la protección de datos de carácter personal no es un derecho absoluto, sino que se ha de considerar en relación con su función en la sociedad.²⁹ En primer lugar, la Constitución establece la posibilidad de acceso a los archivos y registros administrativos "salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas".³⁰ El Tribunal Constitucional ha reconocido también que la distribución equitativa del sostenimiento del gasto público y las actividades de control en materia tributaria (art. 31 CE) son bienes y finalidades constitucionales legítimas capaces de restringir los derechos del art. 18.1 y 4 CE.³¹

El Convenio Europeo de 1981 también ha tenido en cuenta estas exigencias en su art. 9, al igual que el Tribunal Europeo de Derechos Humanos, quien refiriéndose a la garantía de la intimidad individual y familiar del art. 8 CEDH, aplicable también al tráfico de datos de carácter personal, reconociendo que pudiera tener límites como la seguridad del Estado³² o

²⁷ Art. 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".

²⁸ Tribunal de Justicia de la UE, sentencia de 9.11.2010 en los asuntos acumulados C-92/09 y C-93/09, *Volker und Markus Schecke y Eifert*, Rec. 2010, p. I-0000.

²⁹ En consonancia con el artículo 52.1 CDFUE, pueden introducirse limitaciones al ejercicio del derecho a la protección de datos, siempre que tales limitaciones estén establecidas por ley, respeten el contenido esencial de dichos derechos y libertades y, respetando el principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

³⁰ El TC ha afirmado de manera firme y constante que la persecución y castigo del delito constituye un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana, reconocidos en los arts. 10.1 y 104.1 CE. Véanse, por ejemplo, las SSTC 166/1999, de 27 de septiembre, FJ 2, y 127/2000, de 16 de mayo, FJ 3.a; ATC 155/1999, de 14 de junio.

³¹ SSTC 110/1984 y 143/1994.

³² STEDH caso *Leander*, de 26 de marzo de 1987, §§ 47 y ss.

la persecución de infracciones penales³³ ha exigido que tales limitaciones estén previstas legalmente y sean las indispensables en una sociedad democrática, lo que implica que la ley que establezca esos límites sea accesible al individuo concernido por ella, que resulten previsibles las consecuencias que para él pueda tener su aplicación, y que los límites respondan a una necesidad social imperiosa y sean adecuados y proporcionados para el logro de su propósito.³⁴

Como señala DÍEZ PICAZO, "el valor o bien jurídico protegido es, así, la libertad del individuo frente a los abusos y presiones a que puede verse sometido como consecuencia del tratamiento automatizado de datos. Se trata de un derecho de libertad."³⁵ Es importante destacar que los datos protegidos por el art. 18.4 CE no son sólo aquellos que pueden calificarse de íntimos, sino también cualesquiera otros datos relativos a la persona.³⁶ Ello se debe, a juicio de DÍEZ PICAZO a las enormes posibilidades de opresión inherentes al tratamiento automatizado de la información; y ello además es lo que explica que se esté en presencia de un derecho fundamental autónomo, diferenciado del derecho a la intimidad.³⁷

Los titulares de este derecho, dada su obvia conexión con el derecho a la dignidad humana, son todos los individuos tanto españoles como extranjeros. Consecuentemente, es muy dudoso, en cambio, que este derecho corresponda también a las personas jurídicas. El art. 3 LOPD sólo incluye en el ámbito de aplicación de la misma "la información concerniente a personas físicas".³⁸

³³ Mutatis mutandis, SSTEDH, casos Z, de 25 de febrero de 1997, y *Funke*, de 25 de febrero de 1993.

³⁴ STEDH, caso *X e Y*, de 26 de marzo de 1985; caso *Leander*, de 26 de marzo de 1987; caso *Gaskin*, de 7 de julio de 1989; mutatis mutandis, caso *Funke*, de 25 de febrero de 1993; caso Z, de 25 de febrero de 1997.

³⁵ DÍEZ PICAZO, L.M., *Sistema de derechos...*, Op.Cit. p. 326.

³⁶ STC 292/2000, de 30 de noviembre.

³⁷ DÍEZ PICAZO, L.M., *Sistema de derechos...*, Op.Cit. p. 326.

³⁸ Art. 3 LOPD: "A los efectos de la presente Ley Orgánica se entenderá por: a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables".

c) El ejercicio de las facultades derivadas de este contenido esencial: el poder de disposición de datos personales y el origen del derecho al olvido en internet. Los derechos de oposición y cancelación

Ya señalamos que el art. 18.4 CE contiene tanto un derecho fundamental de los ciudadanos como un mandato al legislador para que el disfrute de ese y otros derechos fundamentales sea eficaz.

En primer lugar, el Tribunal Constitucional reconoce en el art. 18.4 CE un derecho fundamental que "garantiza a la persona un poder de control y disposición sobre sus datos personales".³⁹ Como ya se ha estudiado, este poder de control y disposición, concretado en una serie de facultades de su titular como consentir la recogida y el uso de sus datos personales, conocer los mismos, ser informado de quién los posee y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo que ponga fin a la posesión y empleo de tales datos constituyen el contenido esencial del mismo.

Este conjunto de derechos, que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales⁴⁰ sólo puede realizarse a partir del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. Es por ello consustancial a este derecho que los afectados hayan sido informados y hayan emitido su preceptivo consentimiento para el acceso, rectificación y cancelación de esos datos personales. Es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la

³⁹ La LOPD define "datos de carácter personal" como "cualquier información concerniente a personas físicas identificadas o identificables" (art. 3.a) LOPD. El Reglamento (CE) No. 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000, en su art. 2. a) ahonda en el concepto de persona física identificada o identificable: "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

⁴⁰ La LOPD define "fichero" como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso" (art. 3.b) LOPD). Por su parte, la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, define "fichero de datos personales" en su artículo 2.c) como "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

salvaguardia del derecho fundamental⁴¹ que ha de regular la legislación pertinente a raíz del mandato al Legislador que el art. 18.4 CE contiene, garantizando en primera instancia el contenido esencial del derecho a la protección de datos.

En segundo lugar, sobre el legislador pesa "un deber de regular el tratamiento de datos de manera tal que dicha actividad se realice de forma respetuosa para con los derechos fundamentales". La respuesta actual a este mandato, para regular los derechos de la personalidad y controlar los riesgos que puedan derivarse del acopio y tratamientos de datos personales, la constituye la LOPD y su Reglamento de desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD). A raíz de esta Ley Orgánica se ha creado la Agencia Española de Protección de Datos (AEDP),⁴² con la finalidad de controlar la creación y utilización de ficheros de datos.⁴³ Este mandato, y la creación de esta AEPD, supone "una garantía para la plena efectividad de otros derechos como son destacadamente el honor y la intimidad que el art. 18.4 CE menciona de manera expresa",⁴⁴ debiendo añadir el derecho fundamental a la propia imagen por el aumento de la utilización de redes sociales como Facebook, Tuenti, Twitter o You tube.

El Título III de la LOPD y del RLOPD se ocupan de los derechos de los ciudadanos en el tratamiento de sus datos personales, concretamente los derechos de acceso, rectificación, cancelación y oposición que, recordemos, constituyen el contenido esencial del derecho reconocido en

⁴¹ STC 290/2000, de 30 de noviembre, FJ 7.

⁴² Prevista y regulada en el Título VI de la L.O. 15/1999, de 13 de diciembre, así como Real Decreto 1720/2007, de 21 de diciembre, de desarrollo. Disponible en: <http://www.agpd.es>. A juicio del Tribunal Constitucional, la competencia de ámbito nacional atribuida a la Agencia de Protección de Datos está justificada como condición básica para la igualdad en el ejercicio de derechos fundamentales, con base en el art. 149.1.1ª, STC 290/2000. Ésto no es óbice para que existan organismos análogos de ámbito autonómico. De hecho, el Consejo Consultivo que regula su funcionamiento está constituido en parte "un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial" (art. 38 LOPD). Véase, por ejemplo, la Agencia de Protección de Datos de la Comunidad autónoma de Madrid. Disponible en: http://www.madrid.org/cs/Satellite?language=es&pagename=PortalAPDCM%2FPAGE%2FPAPD_home

⁴³ A nivel europeo, el encargado de velar por la protección de datos de carácter personal manejados por las instituciones europeas es el Supervisor Europeo de Protección de Datos (SEPD), <http://www.edps.europa.eu/EDPSWEB/edps/EDPS>

⁴⁴ Díez PICAZO, L.M., *Sistema de derechos...*, *Op. Cit.*, pág. 325.

el art. 18.4 CE, pues a través de ellos, por un lado, se garantiza que cualquier persona pueda tener control sobre sus datos personales y por otro, impone a terceros, ya sean públicos o privados, los ya estudiados deberes de hacer.⁴⁵

El paso previo e imprescindible para ejercitar las facultades conferidas por el derecho recogido en el art. 18.4 CE es tener conocimiento de todos los datos que se encuentran recogidos en internet sobre uno mismo y su tratamiento.⁴⁶ Esta facultad ha sido cristalizada en los derechos de consulta al Registro General de Protección de Datos (art. 14 LOPD)⁴⁷ y de acceso a los datos personales utilizados.⁴⁸ De esta forma, el titular de los datos personales podrá en cualquier momento estar informado de qué datos están siendo sometidos a tratamiento en internet, su origen, qué uso se les está dando, con qué finalidad, por quién y las comunicaciones realizadas o que se prevén hacer de los mismos.

Las facultades más trascendentales atribuidas al titular de los datos, pues suponen la eventual imposición de "obligaciones de hacer" para terceros

⁴⁵ STC 292/2000, de 30 de noviembre.

⁴⁶ Art. 3.c) LOPD: "A los efectos de la presente Ley Orgánica se entenderá por tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias". Una definición semejante establece el art. 2.b) del Reglamento (CE) No. 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos "tratamiento de datos personales": "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, aplicadas a datos personales, como la recogida, registro, organización, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que permita el acceso a los mismos, así como la alineación o interconexión, y el bloqueo, supresión o destrucción."

⁴⁷ Art. 14 LOPD: "Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita."

⁴⁸ Art. 15 LOPD: "1) El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. 2) La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible o inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. 3) El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes."

con la posible incidencia en otros derechos fundamentales como se estudiará más adelante, son los derechos de rectificación y cancelación, que podrán ser demandados cuando el tratamiento de sus datos no se ajuste a lo dispuesto en la LOPD y, en particular, cuando tales datos resulten inexactos o incompletos (art. 16 LOPD).⁴⁹ El supuesto más común dentro del tratamiento de datos no ajustado a lo establecido en la LOPD es el relacionado con el consentimiento informado, regulado en el art. 6 LOPD.⁵⁰

El procedimiento para instar por el titular la oposición, rectificación o cancelación de sus datos personales se regula en el art. 17 LOPD⁵¹ que remite al Reglamento de Desarrollo de la LOPD.⁵² En caso de que la página web deniegue al afectado el ejercicio de su derecho de cancelación

⁴⁹ Art. 16 LOPD: "*Derecho de rectificación y cancelación. 1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. 2. Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos. 3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. 4. Si los datos rectificadas o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación. 5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado*".

⁵⁰ Art. 6 LOPD: "*Consentimiento del afectado. 1) El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal 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 de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o 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, siempre que no se vulneren los derechos y libertades fundamentales del interesado. 3) El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. 4) En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado*".

⁵¹ Art. 17 LOPD: "*Procedimiento de oposición, acceso, rectificación o cancelación. 1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente. 2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación*".

⁵² Art. 25 RLOPD.

podrá denunciarlo ante la AEPD y enfrentarse a una elevada multa pecuniaria pues constituye una infracción grave prevista por la LOPD.⁵³ El tratamiento de datos en internet puede ser llevado a cabo por páginas web⁵⁴ o por buscadores, conforme a la definición de "responsable de fichero o tratamiento de datos".⁵⁵

Los buscadores de internet son servicios de la sociedad de la información sujetos a las garantías de la LOPD, además de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI). Estos tratan y retienen grandes volúmenes de datos de los usuarios a los que ofrecen sus servicios, teniendo la capacidad de crear con ellos perfiles que pueden ser utilizados por el buscador sin que el propio afectado sea consciente de lo que ello supone. Muchas veces, la retención de esos datos deja de tener justificación con el paso del tiempo, ya que aunque en un principio su recogida estaba legitimada, su conservación indefinida y sin motivo que la sustente deja de tener sentido. Por este motivo, las demandas en ejercicio de los derechos para lograr la cancelación de datos en internet, y/o para evitar que los datos personales figuren en los resultados de los buscadores se consolida y amplía año a año. En este sentido de las tres solicitudes iniciales recibidas en la AEPD en 2007 se ha pasado a las 160 reclamaciones de 2011.⁵⁶

Ante la creciente demanda de este derecho la AEPD llama de manera muy acertada a la reflexión sobre si la configuración de las hemerotecas digitales y su contenido ha de ser sólo accesible desde la propia página

⁵³ Art. 18 LOPD: "*Tutela de derechos: en el caso de que la página web deniegue al afectado el ejercicio de su derecho de cancelación, podrá denunciarlo ante la Agencia de Protección de Datos, al constituir una infracción grave del artículo 44.3.e de la LOPD, sancionado con multa de 40.001 a 300.000 euros (Art. 45.2 LOPD). Será necesario concretar exactamente los datos que se desea sean eliminados así como acreditar que el destinatario de la comunicación la ha recibido correctamente*".

⁵⁴ Véase la importante sentencia del TJUE de 6 de noviembre de 2003, (caso *Lindqvist*) en el que determinó que "la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un tratamiento total o parcialmente de datos personales".

⁵⁵ Art. 3.d) LOPD: "*Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*".

⁵⁶ Memoria de 2011 de la Agencia Española de Protección de Datos. Disponible en: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/septiembre/120924_NP_memoria_2011.pdf

web o si, como ahora sucede en muchos casos, su contenido puede ser íntegramente indexable por los buscadores y, como consecuencia de ello, al introducir el nombre y los apellidos de una persona, traer al presente cualquier noticia publicada hace varios años. También se exige a los responsables de las páginas web y de los motores de búsqueda que atiendan las demandas de los ciudadanos cuando ejerzan los derechos que les reconoce la LOPD, ya sea el derecho a cancelar sus datos personales cuando han sido publicados sin su consentimiento y sin cobertura legal, ya sea el derecho de oponerse a que, aún cuando su publicación originaria fuese legal, sean objeto de tratamientos posteriores que compartan una multiplicación de esa publicidad, como sucede con los buscadores. La AEPD da respuesta a esta demanda ciudadana a través de los derechos de cancelación y oposición que regula la LOPD y su Reglamento de Desarrollo. El *derecho de oposición*⁵⁷ se aplica para evitar la indexación de datos personales por los motores de búsqueda valorando siempre, en cada caso concreto, la incidencia que pueda tener en los derechos del ciudadano, atendiendo a sus circunstancias específicas. Las resoluciones de la Agencia tutelando estos derechos son en general atendidas por los responsables de las páginas web, pero no por el prestador del servicio de búsqueda mayoritario, Google. Es más, este buscador ha impugnado sistemáticamente ante la jurisdicción contencioso-administrativa estas resoluciones, lo que ha llevado a la Audiencia Nacional a plantear una interesantísima cuestión prejudicial al Tribunal de Justicia de la Unión Europea por Auto de 27 de febrero de 2012. En ella se suscitan las cuestiones esenciales sobre la garantía de estos derechos en cuanto a la ley aplicable, la responsabilidad de los buscadores y titulares

⁵⁷ El derecho de oposición consiste en el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en una serie de supuestos (art. 35 RLOPD). Artículo 34 RLOPD. "*Derecho de oposición. El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos: a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una ley no disponga lo contrario. b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación. c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento*".

de sitios web, las competencias de las autoridades de protección de datos y la posibilidad de evitar la indexación de la información personal.

La AEDP defiende que los buscadores han de dar respuesta a la solicitud de cancelación y de oposición de los datos personales demandada por los usuarios, tal y como establece la LOPD. La cada vez mayor demanda de satisfacción de estos derechos de cancelación y oposición al tratamiento de datos configuran lo que empieza a denominarse como derecho al olvido en internet. Sin embargo, el buscador Google se opone a hacer desaparecer de sus resultados de búsqueda ciertos datos alegando, por un lado, que los que deben recibir las demandas de oposición y cancelación son los responsables del sitio web donde se incluyeron los datos, no el buscador;⁵⁸ y, en segundo lugar, la protección de otros derechos fundamentales e intereses jurídicamente protegidos, además de alertar sobre el riesgo que este tipo de prácticas supondría para la aparición de la "censura" en internet.

2) El derecho al olvido en internet como parte del contenido esencial del derecho a protección de datos personales

a) La cuestión prejudicial sobre Google y el derecho de cancelación y oposición de datos personales

La desaparición de los datos personales por parte de sus titulares, ya no sólo de la página web que los introdujo, sino de los resultados de los buscadores persiguen instaurar lo que ya se está denominando como el "derecho al olvido en internet". Son varias las decisiones de la AEPD que compelen a Google a dejar de indexar datos de carácter personal que aparecieran en páginas web, tanto oficiales, por ejemplo la Agencia Estatal del Boletín Oficial del Estado (BOE)⁵⁹ o Administraciones

⁵⁸ Recurso de Reposición Nº RR/00188/2012 ante el Director de la Agencia de Protección de Datos.

⁵⁹ Agencia Española de Protección de Datos, Procedimiento nº. TD/01364/2011, ASUNTO: Recurso de Reposición Nº RR/00188/2012. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/recursos_reposicion/rr_sobre_tutela_de_derechos/common/pdfs/REPOSICION-TD-01364-2011_Resolucion-de-fecha-25-06-2012_Art-ii-culo-16-LOPD-34-RD-1720-b-2007.pdf. Agencia Española de Protección de Datos, Expediente Nº: TD/01118/2012, RESOLUCIÓN Nº.: R/02557/2012. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-01118-2012_Resolucion-de-fecha-02-11-2012_Art-ii-culo-16-LOPD.pdf

Públicas⁶⁰ como particulares, por ejemplo como www.elpais.com,⁶¹ si sus titulares lo solicitasen.⁶²

Las páginas web han solicitado hasta el momento acogerse a la legislación europea y española aplicable. Sin embargo, Google España y la AEPD mantienen un largo contencioso sobre quién debe retirar de internet un enlace a una información o dato sobre una persona cuando ésta lo reclama. La AEPD ha venido manteniendo en sus resoluciones dictadas en los procedimientos de tutela de los derechos de los ciudadanos, que los buscadores de internet están sometidos a la legislación europea y española de protección de datos, y que los ciudadanos pueden invocar y hacer valer sus derechos en España frente a los proveedores de servicios de búsqueda de internet.

Google sostiene que su tarea es rastrear lo que ofrece la red y su papel es el de registrar lo que existe, no de censurarlo. En su defensa, el buscador alega que las filiales de cada país son solamente representantes de Google Inc, y en cuanto a las eventuales reclamaciones realizadas frente a Google Spain S.L. ésta alega que la única responsable sería, en todo caso, Google Inc. y dado que los servicios de buscador los presta Google Inc. desde los Estados Unidos, no resulta de aplicación ni la directiva europea de protección de datos ni la Ley Española que la aplica.

Por esta problemática, antes de resolver los recursos planteados por Google, la Sección Primera de la Sala de lo Contencioso Administrativo de la Audiencia Nacional (AN) acordó mediante Auto de 27 de febrero de 2012 y al amparo del art. 267 del Tratado de Funcionamiento de la Unión Europea (TFUE), plantear al Tribunal de Justicia de la Unión

⁶⁰ Agencia Española de Protección de Datos, Procedimiento N°: TD/00396/2012

RESOLUCIÓN N°.: R/01609/2012. Disponible en:

http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-00396-2012_Resolucion-de-fecha-19-06-2012_Art-ii-culo-16-LOPD-34-RD-1720-b-2007.pdf

⁶¹ Agencia Española de Protección de Datos, Procedimiento N°: TD/00796/2012, RESOLUCIÓN N°.: R/02010/2012. Disponible en:

http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-00796-2012_Resolucion-de-fecha-18-09-2012_Art-ii-culo-34-RD-1720-b-2007.pdf

⁶² Pueden consultarse más resoluciones en la sección pertinente página web de la AEDP. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/index-ides-idphp.php

Europea diversas cuestiones prejudiciales en relación con los recursos interpuestos por Google contra las resoluciones en las que la AEPD ha amparado los derechos de oposición y de cancelación de datos personales de ciudadanos frente a buscadores en internet, y en concreto Google.

La Sala entiende que el recurso plantea "el problema referido a las obligaciones que tienen los buscadores de internet en la protección de datos personales de aquellos afectados que no desean que determinadas informaciones, publicadas en páginas web de terceros y que contienen sus datos personales y permiten relacionarles con la misma, sean localizadas, indexadas y sean puestas a disposición de los internautas de forma indefinida".⁶³ En definitiva, en este auto se plantea de fondo si un particular tiene derecho a reclamar la supresión y bloqueo de informaciones en los buscadores de internet relativas a su persona y que, con las nuevas tecnologías, podrán ser localizadas "a lo largo de toda su vida y la de sus descendientes".

El caso de fondo en el que se plantea la cuestión prejudicial trata de un particular que, al teclear su nombre en Google encontraba el enlace con un anuncio en un periódico de tirada nacional, de la subasta de un inmueble por un impago a la Seguridad Social. El afectado afirmaba que el embargo ya se había solucionado y resuelto desde hace años y, pese a ello, esa referencia seguía apareciendo en el buscador. La AEDP acogió la petición de tutela del afectado y requirió a Google Spain SL y Google Inc. que retiraran los datos del denunciante de su índice. Sin embargo, consideró que la información de la subasta aparecida en el periódico debía mantenerse por tener una justificación legal.⁶⁴

Los magistrados resumen en nueve preguntas que pueden agruparse en tres áreas temáticas todas las dudas jurídicas que pueden plantearse en esta problemática entre los buscadores y los titulares de datos personales contenidos en internet.

⁶³ Auto de la Audiencia Nacional de 27 de febrero de 2012, Fundamento 1.

⁶⁴ Resolución de la AEDP de 30 de julio de 2010.

1) La primera duda que se plantean los jueces es si la normativa europea y nacional en materia de protección de datos se puede aplicar en este caso o, si como sostiene la empresa Google Inc., los afectados deberían acudir a los tribunales de California (EEUU) donde está domiciliada la empresa matriz del grupo.⁶⁵

2) Se pregunta también la Sala si los buscadores, cuando indexan la información, están realizando un tratamiento de datos personales, si son responsables de ese tratamiento y deben atender por tanto a los derechos de cancelación y/o oposición del afectado de forma directa, aunque la información se mantenga en la fuente originaria por considerarse lícita.⁶⁶

⁶⁵ Las cuatro preguntas planteadas sobre este tema son las siguientes:

1.1) ¿Debe interpretarse que existe un "establecimiento", en los términos descritos en el art. 4.1.a) de la Directiva 95/46/CE, cuando concurra alguno o algunos de los siguientes supuestos: -cuando la empresa proveedora del motor de búsqueda crea en un estado miembro una oficina o filial destinada a la promoción y venta de los espacios publicitarios del buscador, que dirige su actividad a los habitantes de ese estado, o -cuando la empresa matriz designa a una filial ubicada en ese estado miembro como su representante y responsable del tratamiento de dos ficheros concretos que guardan relación con los datos de los clientes que contrataron publicidad con dicha empresa o -cuando la oficina o filial establecida en un estado miembro traslada a la empresa matriz, radicada fuera de la Unión Europea, las solicitudes y requerimientos que le dirigen tanto los afectados como las autoridades competentes en relación con el respeto al derecho de protección de datos, aun cuando dicha colaboración se realice de forma voluntaria?.

1.2) ¿Debe interpretarse el art. 4.1.c de la Directiva 95/46/CE en el sentido de que existe un "recurso a medios situados en el territorio de dicho estado miembro" cuando un buscador utilice arañas o robots para localizar e indexar la información contenida en páginas web ubicadas en servidores de ese estado miembro o cuando utilice un nombre de dominio propio de un estado miembro y dirija las búsquedas y los resultados en función del idioma de ese estado miembro?.

1.3) ¿Puede considerarse como un recurso a medios, en los términos del art. 4.1.c de la Directiva 95/46/CE, el almacenamiento temporal de la información indexada por los buscadores en internet? Si la respuesta a esta última cuestión fuera afirmativa, ¿puede entenderse que este criterio de conexión concurre cuando la empresa se niega a revelar el lugar donde almacena estos índices alegando razones competitivas?.

1.4) Con independencia de la respuesta a las preguntas anteriores y especialmente en el caso en que se considere por el Tribunal de Justicia de la Unión que no concurren los criterios de conexión previstos en el art. 4 de la Directiva, ¿Debe aplicarse la Directiva 95/46/CE en materia de protección de datos, a la luz del art. 8 de la Carta Europea de Derechos Fundamentales, en el país miembro donde se localice el centro de gravedad del conflicto y sea posible una tutela más eficaz de los derechos de los ciudadanos de la Unión Europea?.

⁶⁶ Las cuatro preguntas planteadas sobre este tema son las siguientes:

2.1) En relación con la actividad del buscador de la empresa "Google" en internet, como proveedor de contenidos, consistente en localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas, ¿Debe interpretarse una actividad como la descrita comprendida en el concepto de "tratamiento de datos" contenido en el art. 2.b de la Directiva 95/46/CE?.

2.2) En caso de que la respuesta anterior fuera afirmativa y siempre en relación con una actividad como la ya descrita: ¿Debe interpretarse el artículo 2.d) de la Directiva 95/46/CE, en el sentido de considerar que la

3) Por último, los magistrados de la Sala de lo Contencioso preguntan al Tribunal de Luxemburgo si la protección de datos incluye que el afectado pueda negarse a que una información referida a su persona se indexe y difunda, aun siendo lícita y exacta en su origen, pero que la considere negativa o perjudicial para su persona. Concretamente, la Sala se expresa en las siguientes palabras: "¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulado en el art. 14.a) de la Directiva 95/46/CE comprenden que el interesado pueda dirigirse frente 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 perjudicarlo o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?"

Obviamente, para nuestro estudio, la pregunta más interesante es la tercera, aunque para darle respuesta es imprescindible que con carácter previo se conteste a los dos primeros bloques de preguntas. Esa pregunta hace referencia directa a la posibilidad de un derecho al silencio en internet de los titulares de los datos personales. Hasta que el Tribunal de Justicia de la Unión Europea se pronuncie, en nuestra opinión, la jurisprudencia del Tribunal Constitucional en materia de derechos fundamentales debería ser plenamente aplicable para resolver las controversias que los titulares de datos personales plantean, como ya ha utilizado para fundamentar algunas de sus resoluciones la AEPD.

b) El concepto del derecho al olvido en internet y la ponderación de derechos

empresa que gestiona el buscador "Google" es "responsable del tratamiento" de los datos personales contenidos en las páginas web que indexa?.

2.3) En el caso de que la respuesta anterior fuera afirmativa: ¿Puede la autoridad nacional de control de datos (en este caso la Agencia Española de Protección de Datos), tutelando los derechos contenidos en el art. 12.b) y 14.a) de la Directiva 95/46/CE, requerir directamente al buscador de la empresa "Google" para exigirle la retirada de sus índices de una información publicada por terceros, sin dirigirse previa o simultáneamente al titular de la página web en la que se ubica dicha información?.

2.4) En el caso de que la respuesta a esta última pregunta fuera afirmativa, ¿se excluiría la obligación de los buscadores de tutelar estos derechos cuando la información que contiene los datos personales se haya publicado lícitamente por terceros y se mantenga en la página web de origen?.

Tomando en cuenta lo que el Tribunal Constitucional entiende como contenido esencial, es decir, "aquella parte del contenido del Derecho que es absolutamente necesaria para que los intereses jurídicamente protegibles, que dan vida al Derecho, resulten real, concreta y efectivamente protegidos",⁶⁷ en nuestra opinión el derecho al olvido en internet debe formar parte del contenido esencial del derecho a la protección de datos del art. 18.4 CE pues hace referencia a la facultad del titular de demandar la modificación o cancelación de ciertos datos en posesión de un tercero. Este derecho, por tanto, es parte de este haz de facultades que conforman el contenido esencial del derecho fundamental al que ya se ha aludido a lo largo de este trabajo. Ahora bien, ningún derecho fundamental es absoluto ni ilimitado. Hay que tener en cuenta que esta posibilidad de cancelación puede incidir en el ámbito de protección de otros derechos fundamentales como la libertad de expresión o libertad de información.⁶⁸

Nuestra postura a la hora de afrontar esta problemática no es otra que la de aplicar la doctrina de ponderación de derechos desarrollada en la jurisprudencia constitucional y del TEDH y aplicada sistemáticamente por los tribunales. Esta es precisamente la postura del Alto Tribunal al sancionar el principio de unidad de la Constitución a la hora de interpretar cualquier precepto constitucional. El derecho de protección de datos personales no constituye una excepción y el Tribunal Constitucional ha sentenciado que "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",⁶⁹ pues así lo exige el principio

⁶⁷ STC 11/1981.

⁶⁸ Disponible en: <http://www.publico.es/ciencias/360165/no-queremos-que-se-use-a-google-para-censurar>

⁶⁹ El Derecho Europeo cristaliza la misma hermenéutica y la Propuesta de Reglamento de Protección de Datos relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) COM(2012) 11 final, reconoce que el derecho a la protección de datos personales podría tener incidencia en los siguientes derechos fundamentales consagrados en la CDFUE: la libertad de expresión (artículo 11 de la Carta); la libertad de empresa (artículo 16); el derecho a la propiedad y especialmente a la protección de la propiedad intelectual (artículo 17, apartado 2); la prohibición de toda discriminación, y en particular la ejercida por

de unidad de la Constitución.⁷⁰ Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental."⁷¹

El eventual ejercicio del derecho al olvido debería ser considerado de una forma similar a la ponderación entre derechos fundamentales en conflicto, acudiendo a los criterios utilizados por la jurisprudencia constitucional.

La AEPD ya los ha tenido en cuenta en muchas de sus decisiones para resolver sobre las solicitudes de oposición y cancelación de datos personales. En este sentido, un criterio muy utilizado por la AEPD es la *relevancia pública* de los datos personales,⁷² como por ejemplo la comisión de un delito⁷³ (o su no relevancia).⁷⁴ Así, la AEPD ha razonado que "cabe proclamar que ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la RED sin poder reaccionar ni corregir la inclusión ilegítima 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 incontestada de datos personales podría suponer una insoportable barrera al libre ejercicio de las libertades

razón de raza, orígenes étnicos, características genéticas, religión o convicciones, opiniones políticas o de cualquier otro tipo, discapacidad u orientación sexual (artículo 21); los derechos del menor (artículo 24); el derecho a un alto nivel de protección de la salud humana (artículo 35); el derecho de acceso a los documentos (artículo 42); el derecho a la tutela judicial efectiva y a un juez imparcial (artículo 47).

⁷⁰ SSTC 11/1981, de 8 de abril, FJ 7; 196/1987, de 11 de diciembre, FJ 6; y respecto del art. 18, la STC 110/1984, FJ 5.

⁷¹ STC 292/2000, de 30 de noviembre, FJ 11.

⁷² Surgen así problemas de no poca importancia como los que tratados en BUSTOS Gisbert, R., "*Sobre la publicación en páginas Web de listas de condenados penalmente. Los casos de las listas de pedófilos, maltratadores, torturadores y errores médicos*", *Revista Vasca de Administración Pública*, (62), 2002.

⁷³ Agencia Española de Protección de Datos, Procedimiento N°: TD/01041/2012, RESOLUCIÓN N°.: R/02553/2012, Disponible en:

http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-01041-2012_Resolucion-de-fecha-19-10-2012_Art-ii-culo-16-LOPD.pdf

⁷⁴ Agencia Española de Protección de Datos, Procedimiento N°: TD/00796/2012, RESOLUCIÓN N°.: R/02010/2012. Disponible en:

http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-00796-2012_Resolucion-de-fecha-18-09-2012_Art-ii-culo-34-RD-1720-b-2007.pdf

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 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".⁷⁵

La *exactitud de los datos personales* utilizados es otro de los criterios utilizados por la AEPD,⁷⁶ y debería ser completada con los requisitos para la apreciación de la veracidad en una información, como el descrédito en la consideración de la persona a la que la información se refiere, el respeto a la presunción de inocencia o la condición pública o privada de la persona implicada.⁷⁷ La *antigüedad* de los datos, exigiendo que no sean obsoletos,⁷⁸ es otro criterio utilizado por la AEPD. Por último, la observancia y el respeto por otros derechos fundamentales muy íntimamente relacionados con el derecho a la protección de datos personales, como la intimidad, el honor o la propia imagen, así como la protección de la juventud y de la infancia, también deberían de tenerse en cuenta a la hora de concederse o no el pretendido derecho al olvido en internet.

Dado el amplio alcance que el tratamiento de datos personales en internet puede llegar a tener y su incidencia en otros derechos fundamentales, las instituciones europeas están llevando a cabo un proceso de unificación y modernización de normas jurídicas, queriendo establecer un marco más sólido y coherente en materia de protección de datos en la UE, a partir de

⁷⁵ Procedimiento N°: TD/00796/2012 RESOLUCIÓN N°.: R/02010/2012.

⁷⁶ AEPD, Procedimiento N°: TD/01041/2012, RESOLUCIÓN N°.: R/02553/2012.

⁷⁷ STC 21/2000, de 31 de enero, FJ 6.

⁷⁸ RESOLUCIÓN N°.: R/02010/2012

un nuevo Reglamento⁷⁹ y una nueva Directiva de protección de datos de carácter personal.⁸⁰

El proyecto de Reglamento consagra en el art. 17 el pretendido derecho al olvido. Este consistiría en que el interesado puede demandar al responsable del tratamiento de datos personales que los suprima y se abstenga de darles más difusión en caso de que ya no sean necesarios para los fines para los que fueron recogidos o tratados de otro modo, de que los interesados hayan retirado su consentimiento para el tratamiento, de que se opongan al tratamiento de datos personales que les conciernan o de que el tratamiento de sus datos personales no se ajuste de otro modo a lo dispuesto en el Reglamento. El derecho al olvido sería particularmente pertinente si los interesados hubieran dado su consentimiento siendo niños, cuando no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quisieran suprimir tales datos personales especialmente en internet.

Sin embargo, la misma Propuesta de Reglamento establece que se puede autorizar la conservación de los datos cuando sea necesario para fines de investigación histórica, estadística y científica, por razones de interés público en el ámbito de la salud pública, para el ejercicio del derecho a la libertad de expresión, cuando la legislación lo exija,⁸¹ o en caso de que existan motivos para restringir el tratamiento de los datos en vez de proceder a su supresión.⁸²

Por último, y con el fin de reforzar el "derecho al olvido" en internet, el derecho de supresión también debe ampliarse de tal forma que los responsables del tratamiento que hayan hecho públicos los datos

⁷⁹ Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), COM (2012) 9 final.

⁸⁰ Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las autoridades competentes a efectos de la prevención, investigación, detección y enjuiciamiento de infracciones penales o la ejecución de sanciones penales, y a la libre circulación de estos datos, COM (2012) 10, final.

⁸¹ Art. 17.3 Propuesta de Reglamento COM (2012) 9 final.

⁸² Art. 17.4 Propuesta de Reglamento COM (2012) 9 final.

personales deben estar obligados a informar a los terceros que estén tratando tales datos de que un interesado les solicita que supriman todo enlace a tales datos personales, o las copias o réplicas de los mismos.⁸³ Para garantizar esta información, el responsable del tratamiento debe tomar todas las medidas razonables, incluidas las de carácter técnico, en relación con los datos cuya publicación sea de su competencia. Se comenzaría de esta forma a dar respuesta al problema planteado por Google y la AEPD, exigiendo a las páginas web que introdujeron los datos en primer lugar que den el primer paso para su cancelación y se pongan en contacto con otros operadores de internet que estén utilizándolos, sean páginas web o buscadores, como Google.

A modo de conclusión

El derecho fundamental a la protección de datos personales está alcanzando una relevancia cada vez mayor en la medida en que internet ha cobrado un indiscutible protagonismo en nuestras vidas, tanto a nivel personal como profesional. Por ello, es imprescindible delimitar claramente el contenido esencial de este derecho, las facultades que otorga a los titulares de los derechos personales y sus límites. Sin embargo, internet es una realidad que supera, casi a diario, las previsiones normativas y jurídicas que tratan de regularlo. Un ejemplo de esta realidad lo constituye el llamado "derecho al olvido en internet", que pretende la desaparición de todos los datos identificativos de una persona de ese medio, en relación con los derechos de oposición y cancelación que asisten a los ciudadanos. Sin embargo, para ello sería necesario abordar la actuación de los operadores en internet, tanto páginas web como buscadores, que contribuyen a la realización de otros derechos fundamentales esenciales para nuestra sociedad y Estado democrático, como la libertad de expresión y de información. La ponderación, por tanto, entre los intereses jurídicamente protegidos y derechos fundamentales en conflicto supone el instrumento clave utilizado, no solo por el Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos, sino por la nueva normativa europea que

⁸³ Art. 17.2 Propuesta de Reglamento COM (2012) 9 final.

pretende dar una respuesta más actualizada a la problemática suscitada. No obstante estos esfuerzos legislativos, la realidad de la sociedad de la información y de internet siempre continuará superando con una gran rapidez a la normativa que trata de regularla. Es en este tipo de situaciones cuando la existencia de una clara y firme jurisprudencia constitucional cobra una importancia esencial para que los derechos fundamentales, sea cual sea el escenario en el que tengan que ser aplicados, sean disfrutados a su máximo nivel por los ciudadanos.

3. Fuentes de consulta

DÍEZ PICAZO, L.M. "*Sistema de derechos fundamentales*", 3ª ed., Navarra, Thomson Civitas, 2008.

Legislación:

Constitución Española, aprobada el 31 de octubre de 1978, ratificada el 6 de diciembre de 1978.

Carta de Derechos Fundamentales de la Unión Europea 210/C, 30 de marzo de 2010.

Convenio del Consejo de Europa para la Protección de Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, 28 de enero de 1981.

Convenio Europeo de Derechos Humanos, revisado en conformidad con el protocolo número 11, entrada en vigor el 1 de noviembre de 1998.

Ley Orgánica de Protección de Datos de Carácter Personal, 15/1999, de fecha 13 de diciembre de 1999.

Propuesta del Reglamento del Parlamento Europeo y del Consejo relativo a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación (Reglamento General de

Protección de Datos), Bruselas 25 de enero de 2012, COM (2012) 11 final.

Sentencias del Tribunal Constitucional Español consultables en:

Tribunal Constitucional Español: www.tribunalconstitucional.es.

STC 11/1981, de 8 de abril, FJ 8.

SSTC 73/1982, de 2 de diciembre, FJ 5; 110/1984, de 26 de noviembre, FJ 3; 89/1987

STC 110/1984, FJ 5.

SSTC 110/1984 y 143/1994.

STC 231/1988, de 2 de diciembre, FJ 3.junio, FJ 3; 231/1988, de 2 de diciembre, FJ 3; 197/1991, de 17 de octubre, FJ 3.

STC 254/1993, de 9 de mayo, FJ 7.

STC 254/1993, de 20 de julio, FJ 7.

STC 143/1994, de 9 de mayo, FJ 7.

STC 254/1994, de 9 de mayo, FJ 6.

STC 11/1998, de 13 de enero, FJ 4.

SSTC 94/1998, de 4 de mayo, FJ 6.

SSTC 11/1998, FJ 4; 143/1994, FJ 7.

SSTC134/1999, de 15 de julio, FJ 5;

STC 144/1999, de 22 de julio, FJ 8.

SSTC 202/1999, de 8 de noviembre; FJ 2.

SSTC144/1999, de 22 de julio,

SSTC 98/2000, de 10 de abril, FJ 5;

STC 292/2000, de 30 de noviembre, FJ 4.

STC 292/2000, de 30 de noviembre, FJ 5.

SSTC115/2000, de 10 de mayo, FJ 4.

SSTC115/2000, de 10 de mayo.

STC 292/2000, de 30 de noviembre, FJ 6.

STC 292/2000, de 30 de noviembre, FJ 6

STC 290/2000, de 30 de noviembre, FJ 7.

SSTC 290/2000, de 30 de noviembre, FJ 7.

STC 292/2000, de 30 de noviembre, FJ 7.

STC 292/2000, de 30 de noviembre, FJ 2.

STC 292/2000, de 30 de noviembre, FJ 10.

STC 292/2000, de 30 de noviembre, FJ 11.

SSTC 292/2000, de 30 de noviembre FJ 5.

Recurso de Reposición N° RR/00188/2012. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/recursos_reposicion/rr_sobre_tutela_de_derechos/common/pdfs/REPOSICION-TD-01364-2011_Resolucion-de-fecha-25-06-2012_Art-ii-culo-16-LOPD-34-RD-1720-b-2007.pdf

RESOLUCIÓN N°.: R/02557/2012. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-01118-2012_Resolucion-de-fecha-02-11-2012_Art-ii-culo-16-LOPD.pdf

RESOLUCIÓN N°.: R/01609/2012. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-00396-2012_Resolucion-de-fecha-19-06-2012_Art-ii-culo-16-LOPD-34-RD-1720-b-2007.pdf

RESOLUCIÓN N°.: R/02010/2012. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-00796-2012_Resolucion-de-fecha-18-09-2012_Art-ii-culo-34-RD-1720-b-2007.pdf

RESOLUCIÓN N°.: R/02553/2012, Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-01041-2012_Resolucion-de-fecha-19-10-2012_Art-ii-culo-16-LOPD.pdf

RESOLUCIÓN N°.: R/02010/2012. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-00796-2012_Resolucion-de-fecha-18-09-2012_Art-ii-culo-34-RD-1720-b-2007.pdf