Seguridad

Cuaderno Red de Cátedras Telefónica

Universidad de Salamanca

EL DERECHO AL OLVIDO DIGITAL EN LA WEB 2.0

Cátedra Telefónica de la Universidad de Salamanca

Mario Hernández Ramos

No. 11 mayo 2013

www.catedras.telefonica.es
http://catedraseguridad.usal.es

Cátedra de Seguridad Universidad de Salamanca
Dirección y Coordinación:
Prof. Dr. D. Fernando Pérez Álvarez, Profesor titular Derecho Penal. Director Ciencias de la Seguridad (CISE).
Profa. Dra. Dña. Angélica González Arrieta, Profesora titular Ciencias de la Computación e Inteligencia artificial.
Profa. Dra. Dña. Lina Mariola Díaz Cortés. Profesora Ciencias de la Seguridad (CISE).
Coordinación:
Dra (c). María Teresa Heredero Campo. Doctoranda Derecho Civil, Universidad de Salamanca.
Imagen y sonido:
Dr. (c). Pablo Calvo. Profesor Ciencias de la Seguridad (CISE)
Despacho:
291 Facultad de Derecho, Campus Miguel de Unamuno.
Teléfono:
923294400 Ext. 1622
Correo electrónico:
catedratelefonica@usal.es

CISE

Mario Hernández Ramos

Es profesor de Derecho Constitucional adscrito al Departamento de Derecho Público General de la Universidad de Salamanca. Se doctoró Cum Laude, premio extraordinario por la Universidad de Salamanca y mención especial Doctor Europeus con la tesis doctoral titulada "La relevancia del contenido constitucional en la admisión del recurso de amparo. Aportaciones de la experiencia de los casos estadounidense y alemán al caso español". Ha realizado estancias de investigación en las Facultades de Derecho de la Universidad de Bristol (Reino Unido), de la Universidad de Michigan (EE.UU.) y en la Universidad de Ciencias de la Administración Pública de Speyer (Alemania). Autor de varias publicaciones sobre la tutela de los derechos fundamentales y conferenciante sobre diversos temas relativos a los derechos fundamentales, a la justicia constitucional y sus relaciones con el Tribunal Europeo de Derechos Humanos y el Tribunal de Justicia de la Unión Europea. También es cronista de jurisprudencia, y evaluador externo en revistas nacionales e internacionales. En la actualidad dirige el Máster en Democracia y Buen Gobierno de la Universidad de Salamanca

ISSN: 2174-7628

Índice

RESUMEN:

Internet y la web 2.0 supone una herramienta para la mayor efectividad de algunos derechos fundamentales como la libertad de información y la libertad de expresión. Sin embargo, al mismo tiempo, también supone una amenaza para la integridad de otros derechos fundamentales como el derecho al honor, la intimidad, la propia imagen y la protección de datos personales. Los ciudadanos son cada vez más conscientes de estos peligros y demandan del ordenamiento jurídico mecanismos para la tutela de sus derechos fundamentales. El derecho al olvido digital, ejercido principalmente a través del derecho de cancelación y oposición al tratamiento de datos personales por páginas web y buscadores, está cobrando un gran protagonismo. Sin embargo, su ejercicio debe realizarse conforme unos principios y respetando otros derechos fundamentales con los que entra en conflicto. Solo de este modo se podrá seguir garantizando la naturaleza abierta de Internet y el disfrute de una sociedad pluralista y democrática por parte de los ciudadanos.

ABSTRACT:

Internet and the web 2.0 are very useful tools in order to achieve that some fundamental rights like freedom to information and right to freedom of expression are more effective. Nonetheless, at the same time, they implies jeopardy to the integrity of other fundamental rights like right to honor, privacy, own image and personal data processing. Citizens are increasingly more aware of these perils and demand from the legal system tools to protect their fundamental rights. The right to be forgotten implemented by the rights to cancel and to oppose processing data by web pages and browsers, is being considered more and more important. Nonetheless, its implementation must be exercised taking into account the respect to others fundamental rights. Only in this way the open nature of Internet and the enjoyment of a plural and democratic society can be protected.

Palabras clave:

Derecho a la protección de datos personales; Internet; Web 2.0; derecho al olvido digital; derechos de acceso, rectificación, cancelación y oposición.

Keywords:

Right to personal data protection; Internet; Web 2.0.; Right to be forgotten; Right to access, rectification, cancel and opposition.

ABREVIATURAS

AEDP: Agencia Española de Protección de Datos.

Art.: artículo.

Arts.: artículos.

CE: Constitución española de 1978.

Derechos ARCO: Derechos de acceso, rectificación, cancelación y oposición.

FJ: Fundamento Jurídico

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos

LSSICE: Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

RLOPD: Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

STC: Sentencia del Tribunal Constitucional

SSTC: Sentencias del Tribunal Constitucional

STEDH: Sentencia del Tribunal Europeo de Derechos Humanos

SSTEDH: Sentencias del Tribunal Europeo de Derechos Humanos

SSTEDH: Sentencias del Tribunal Europeo de Derechos Humanos

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea

TC: Tribunal Constitucional

UE: Unión Europea

1. 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. 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.

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 determinados usos de Internet. En este sentido empieza a cobrar cada vez más importancia el derecho fundamental a la protección de datos. Prueba de ello es la creciente normativa reguladora sobre la materia, tanto nacional como internacional, que se abordará someramente a lo largo de este trabajo.

En España este aumento se evidencia en el número creciente de demandas de protección de datos personales solicitadas a la Agencia Española de Protección de Datos (en adelante AEPD). Según datos de la Memoria del 2011 de la AEPD, 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 AEPD que se aproximan a los 3 millones (2.892.516), con un promedio diario cercano a los 8.000 accesos (7.923). 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.

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 antigüedad de la

Directiva 95/46/CE 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, 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.

En las siguientes páginas se trata de ilustrar, de manera introductoria, el problema de la protección de datos personales a través de demandar su control y su eventual desaparición de Internet por parte de sus titulares. Para ello se comenzará señalando el papel que la web 2.0 ha jugado para la disponibilidad y acceso de datos personales a través de Internet por parte de cualquiera. Se prestará especial atención al derecho fundamental a la protección de datos personales, su objeto, y función, así como los derechos o potestades que otorga a los titulares de los datos personales para controlar su acceso por parte de terceros. Por último, se abordará el significado del derecho al olvido digital, su configuración y los principales retos que plantea su reconocimiento.

2. LA WEB 2.0. NUEVO ESCENARIO DE AMENAZA DE LOS DERECHOS FUNDAMENTALES EN LA RED.

Si bien Internet ha supuesto una verdadera revolución para el desarrollo de imprescindibles derechos fundamentales en democracia como la libertad de expresión y libertad de información, también ha supuesto nuevos riesgos y amenazas para otros derechos fundamentales como el de la intimidad, el honor, la propia imagen y la protección de datos.

Estos riesgos y amenazas se han visto incrementados exponencialmente con la irrupción de la web 2.0. Con la Web 1.0, el *webmaster* controlaba los contenidos de la página web, por lo que podía constituir un filtro a la información, expresiones o datos que los usuarios podrían encontrarse en la web. Con la web 2.0 se incluye la posibilidad de que los usuarios interactúen entre sí, relegando a un segundo plano al *webmaster*. Los ejemplos más definitorios de lo que es la web 2.0 lo constituyen las redes sociales, los blog y las wikis.

> El concepto de web 2.0 "se usa para referirnos a una nueva tendencia en el uso de las páginas Web, en la cual el usuario es el centro de la información y se convierte en generador de contenidos. Supone un cambio en la filosofía, una actitud, una forma de hacer las cosas que identifica el uso actual de Internet que hacen tanto los internautas como las empresas, pasando de ser meros consumidores a productores y creadores de contenidos." (HEREDERO CAMPO)

Como consecuencia de esta evolución (aunque ya se está hablando de la web 3.0, caracterizada por el procesamiento de datos por procesadores de información mediante aplicativos que permiten describir los contenidos y la información presente en la Web, concebida para que las máquinas "entiendan" a las personas y procesen de una forma eficiente la avalancha de información publicada en la Web, MORENO NAVARRETE) la información disponible de cada persona en Internet, publicada por terceros, ha aumentado de manera incontrolada por sus propios titulares, quienes comienzan a demandar un cierto control sobre los mismos. Es cierto que en un principio, los usuarios de Internet podrían estar encantados de aparecer en buscadores o redes sociales. Sin embargo, cada vez más se es consciente que la disponibilidad pública e incondicionada de esa información puede generar ciertos perjuicios y problemas personales. Un ejemplo muy claro en este tema lo constituye el mundo laboral, pues no son pocos los ejemplos de despidos por informaciones publicadas en redes sociales o datos de candidatos a puestos de trabajo obtenidos por las empresas a través de rastrear la Red. Otros ejemplos ya habituales y que protagonizan el surgimiento de la web 3.0 son los estudios por parte de las empresas de todo tipo de datos personales para posteriormente comercializar con ellos. Nada en Internet, aunque lo parezca, es gratis (SALGADO SEGUÍN).

Tomando como ejemplo las redes sociales, MORENO NAVARRETE, señala tres fases en las que los derechos fundamentales de los usuarios pueden quedar más desprotegidos. En primer lugar, señala el registro en la red social, momento en el que se introducen datos personales de toda índole y que, a pesar de que esa introducción es consentida por el usuario y de que se otorga la posibilidad de restringir el acceso de terceros a esos datos, pueden ser utilizados para otros fines diferentes al registro en la red social. En segundo lugar, el desarrollo de actividades en la red social, donde el usuario continúa introduciendo nuevos datos, como su vida diaria, su grupo de amigos, información multimedia, imágenes y vídeos, propios y con aparición de terceros. En esta segunda fase, los derechos de terceros pueden quedar al descubierto y accesibles a otras personas para lo que sus titulares no han emitido consentimiento alguno. Por último, al darse de baja del servicio, surge la problemática de la conservación de los datos del usuario, así como los que hubieran podido introducirse por la actividad diaria en la red social de terceros. Además,

teniendo en cuenta la dinámica de la Web 2.0, hay que tener en cuenta que a través de su actividad en la red, el usuario aumenta la información de su perfil y se hace más precisa, contribuyendo a ello sin duda la información que sobre éste aportan otros usuarios del entorno

Esta actividad supone una amenaza clara a los derechos de intimidad, honor y propia imagen (art. 18.1 CE) tanto del usuario como de otras personas sobre las que se ha añadido información de cualquier tipo. Estos derechos forman parte de los derechos de la personalidad, y como tal, conforme a la jurisprudencia del Tribunal Constitucional, garantiza el ámbito de libertad de una persona respecto de sus atributos más característicos, propios e inmediatos como son la imagen física, la voz o el nombre, cualidades definitorias del ser propio y atribuidas como posesión inherente e irreductible a toda persona.

Respecto del derecho a la propia imagen, como afirma el Alto Tribunal, en la medida en que la libertad de las personas se manifiesta en el mundo físico por medio de la actuación de su cuerpo y las cualidades del mismo, es evidente que con la protección de la imagen se salvaguarda el ámbito de la intimidad y, al tiempo, el poder de decisión sobre los fines a los que hayan de aplicarse las manifestaciones de la persona a través de su imagen, su identidad o su voz.

El derecho a la intimidad, por su parte, limita la intervención de otras personas y de los poderes públicos en la vida privada. Esta intervención puede incidir también en la propia imagen, manifestándose tanto respecto de la observación y captación de la imagen y sus manifestaciones como de la difusión o divulgación posterior de lo captado.

El derecho al honor protege tanto la dignidad como la reputación de una persona en la sociedad. La palabra 'honor' parece un poco trasnochada; sin embargo, es algo plenamente vigente en nuestra sociedad (y más desde que existen las nuevas tecnologías). Como enfatiza SALGADO SEGUÍN, con el auge de Internet, éste es uno de los derechos más atacados hoy en día, pues con frecuencia se publican comentarios o informaciones sobre personas a las que se insultan o acusan de hechos que en muchas ocasiones resultan inciertos y que menoscaban su imagen pública. Este tipo de comportamientos son espoleados por el aparente anonimato que ofrece la Red. Además, esto se acrecienta con la enorme capacidad de los buscadores (especialmente de

Google) para referenciar e indexar toda esta información y mostrárnosla por orden de relevancia, ocasionando que al ser buscado el nombre de una persona en un buscador, el resultado de la búsqueda suelan ser críticas, insultos e informaciones dudosas sobre la misma. Esto daña enormemente su reputación tanto a nivel privado como profesional.

Lo más importante que ha de destacarse a los efectos de este trabajo, es que estos derechos, como expresión de la persona misma, disfrutan de la más alta protección en nuestra Constitución y constituyen un ámbito exento capaz de impedir o limitar la intervención de terceros contra la voluntad del titular. En esta línea se elaboraron la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, y en el ámbito de Internet, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) cuyo art. 8.1 afirma que "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 [...] 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 y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social[...]".

Estos derechos, por tanto, son irrenunciables en su núcleo esencial y por ello, aunque se permita autorizar su intromisión o divulgación, será siempre con carácter revocable (STC 117/1994, de 25 de abril, FJ 3). La información o datos aportados por el usuario, de manera consciente y voluntaria o inconsciente e involuntaria tienen un régimen jurídico constitucional claro: los derechos fundamentales, y más si cabe los derechos de la personalidad, son irrenunciables, inalienables e imprescriptibles.

Sin embargo, un análisis de los derechos fundamentales amenazados por el escenario creado a raíz de la web 2.0, por muy introductorio que sea como es éste, no estaría completo si no abordáramos el estudio del derecho a la protección de datos (art. 18.4 CE).

Como ha señalado de manera constante el Tribunal Constitucional 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 derechos 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" (STC 254/1994, de 9 de mayo, FJ 6).

Por tanto, el art. 18.4 CE consagra, por un lado, un derecho fundamental al ciudadano y por otro un mandato al legislador, diferente del resto de los derechos contenidos en el art. 18 CE.

3. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL: DELIMITACIÓN CONCEPTUAL.

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 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".

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". 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. Aquí es donde entra a operar el derecho fundamental a la protección de datos (art. 18.4 CE).

3.1 Diferenciación del derecho a la protección de datos de los clásicos derechos al honor, intimidad propia y familiar y a la propia imagen.

Está fuera de toda duda la diferencia que estableció el Tribunal Constitucional en la STC 292/2000 entre los derechos fundamentales clásicos del art. 18.1 CE y el derecho a la protección de datos del art. 18.4 CE (véase la reciente STC 29/2013 de 11 de febrero, FJ 6). El Alto Tribunal señala que "el constituyente quiso garantizar mediante el actual art. 18.4 CE no sólo un ámbito de protección ***específico*** sino también más ***idóneo*** que el que podían ofrecer, por sí mismos, los derechos fundamentales" del honor, intimidad y propia imagen (art. 18.1 CE).

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. En consecuencia, el Tribunal Constitucional ha sentenciado que el derecho fundamental a la intimidad (art. 18.1 CE) concebido únicamente como facultades negativas, 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 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" (STC 11/1998, de 13 de enero, FJ 4).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.

> La peculiaridad del derecho fundamental a la protección de datos respecto del derecho fundamental a la intimidad, radica, pues, en su distinta **función**, lo que apareja, por consiguiente, que también su **objeto** y **contenido** difieran.

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 voluntad (STC 144/1999, de 22 de julio, FJ 8). 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. 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.

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 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 solo 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." (STC 292/2000, de 30 de noviembre)

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 (SSTC 73/1982, de 2 de diciembre, FJ 5), 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.

> Esto 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 uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales" (STC 292/2000, de 30 de noviembre, FJ 6).

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.

3.2 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 (STC 11/1981, de 8 de abril, FJ 8), tanto por su naturaleza jurídica o "el modo de concebir o de configurar cada derecho", como por sus bienes o intereses jurídicamente protegidos.

> 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 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, ***saber*** de los mismos, con pleno conocimiento de la ***finalidad*** para la que se recogen esos datos y para la que se van a emplear (STC 29/2013 de 11 de febrero).

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.

Estas facultades forman parte también del contenido esencial del derecho de protección de datos de carácter personal (STC 292/2000, de 30 de noviembre, FJ 10) y deben de integrar la 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".

Como no podía ser de otra manera, este contenido esencial va en la línea del 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 (Arts. 5,6,7, 8 y 11); 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; el art. 16 del Tratado de Funcionamiento de la Unión Europea, introducido por el Tratado de Lisboa;, 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 UE (*Tribunal de Justicia de la UE, sentencia de 9.11.2010 en los asuntos acumulados C-92/09 y C-93/09, VolkerundMarkusSchecke y Eifert, Rec. 2010, p. I-0000*), 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. 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". 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. 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 (SSTC 110/1984 y 143/1994).

El 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 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, aplicable también al tráfico de datos de carácter personal, reconociendo que pudiera tener *límites* como la seguridad del Estado (*STEDH caso Leander, de 26 de marzo de 1987, §§ 47 y ss*) o la persecución de infracciones penales (*Mutatis mutandis, SSTEDH, casos Z, de 25 de febrero de 1997, y Funke, de 25 de febrero de 1993*) 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 (*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).

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." Es importante insistir de nuevo 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 (STC 292/2000, de 30 de noviembre). 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.

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. De hecho, el art. 3 de la Ley Orgánica de Protección de Datos solo incluye en el ámbito de aplicación de la misma "la información concerniente a personas físicas".

4. EL DERECHO AL OLVIDO DIGITAL

4.1 El origen del derecho al olvido digital: el poder de disposición de los datos personales y los derechos ARCO: acceso, rectificación cancelación y oposición.

Hasta el momento se ha dejado claro que todo ciudadano ha de tener el control y disposición sobre sus propios datos personales. La plasmación jurídica de este poder en el art. 18.4 CE se desarrolla tanto en forma de un ***derecho fundamental*** de los ciudadanos, como de un ***mandato al legislador*** para que el disfrute de los 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". 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 derecho a la protección de datos de carácter personal.

Este conjunto de derechos, que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales solo 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 salvaguardia del derecho fundamental (STC 290/2000, de 30 de noviembre, FJ 7) 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 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos, (en adelante LOPD) y su Reglamento de desarrollo aprobado por el Real Decreto 1720/2007, de 21 de diciembre (en adelante RLOPD). A raíz de la LOPD se ha creado la Agencia Española de Protección de Datos (en adelante AEDP), prevista y regulada en su Título VI, así como por el RLOPD, con la finalidad de controlar la creación y utilización de ficheros de datos. 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", debiendo añadir el derecho fundamental a la propia imagen por el aumento de la utilización de redes sociales como Facebook, Tuenti, Tweeter o Youtube.

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 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.

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***. Esta facultad ha sido cristalizada en los derechos de consulta al Registro General de Protección de Datos (art. 14 LOPD) y de acceso a los datos personales utilizados (art. 15 LOPD).

> 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 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). 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. La cancelación dará lugar al bloqueo de los datos objeto de demanda y sólo podrán conservarse 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. Una vez cumplido este plazo deberá procederse a la supresión de los datos (art. 16.3 LOPD).

El procedimiento para instar por el titular la oposición, rectificación o cancelación de sus datos personales se regula en el art. 17 LOPD, que remite al art. 25 RLOPD. En caso de que la página web deniegue al afectado el ejercicio de su derecho de cancelación podrá denunciarlo ante la AEPD y enfrentarse a una elevada multa pecuniaria pues constituye una infracción grave prevista por la LOPD (art. 18 LOPD).

4.2 La consolidación del derecho al olvido digital.

Parafraseando a SIMÓN CASTELLANO, referente de esta materia en nuestro país, el derecho al olvido digital podría definirse "como un derecho que exige que los datos de las personas dejen de ser accesibles en la web, por petición de las mismas y cuando estas lo decidan; como un derecho a retirarse del sistema y eliminar la información personal que la red contiene. Más concretamente, se trata de un derecho de la ciudadanía a cancelar y oponerse al tratamiento de sus datos personales cuando estos han dejado de ser útiles o necesarios para el propósito con el que fueron recabados o publicados."

Debido al aumento de demandas de protección de datos al que se ha hecho ya referencia en la introducción, la AEPD con su actividad diaria ha desempeñado un papel esencial para el reconocimiento del derecho al olvido digital. Son varias ya las ocasiones en las que la AEPD ha afirmado que ningún ciudadano que no sea objeto de un hecho noticiable de relevancia pública tiene que resignarse a que sus datos se difundan en Internet sin poder reaccionar ni corregir su inclusión (véase, por ejemplo, su Resolución TD/266/2007). La AEPD configura este derecho, por un lado, como la posibilidad de ejercitar el *derecho de* ***cancelación*** de los datos que la red conserva cuando estos no se contengan en una fuente accesible al público ni exista una finalidad legítima que proteja la publicación —libertades informativas, finalidad cultural e histórica, etc (art. 3.j LOPD); por otro lado, reconoce el *derecho de* ***oposición*** frente al tratamiento que los buscadores web realizan de los datos personales, es decir, además de la cancelación —la desindexación por parte de los motores de búsqueda de la información pasada—, se exige que el buscador encuentre medios para que la información no vuelva a aparecer en el futuro (Resolución de la AEPD TD/00463/2007).

Ambas acciones, la cancelación de algunos datos y la oposición frente al tratamiento de los buscadores, no están exentas de problemas relevantes, pues pueden impedir el ejercicio legítimo de otros derechos fundamentales, como la libertad de expresión o la libertad de información. Es importante, por ello, detenerse brevemente en su estudio y perfilar aún más el ámbito de actuación del derecho al olvido digital.

4.3 Problemas en torno al derecho al olvido digital.

A) – Buscadores o motores de búsqueda en Internet. La cuestión prejudicial al TJUE por la confrontación entre Google y la AEPD.

Conforme al art. 3 LOPD, el tratamiento de datos en Internet puede ser llevado a cabo por páginas web o por buscadores, conforme a la definición de "responsable de fichero o tratamiento de datos".

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, . (LSSICE) 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 amplia 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.

Como afirma RALLO, en "los últimos tiempos la generalización de las prestaciones y uso de estos servicios está comportando importantes consecuencias al activar y permitir el acceso de

cualquiera a datos personales que con anterioridad eran difícilmente localizables, por encontrarse dicha información alojada en sitios web que posibilitan su captación y acceso a través de la indexación que realizan los buscadores." Por ello, en el ámbito de los buscadores, adquiere especial importancia la tutela de los derechos de aquellas personas a cuyos datos pueden ser accedidos a raíz de las búsquedas realizadas. La AEPD defiende que el ejercicio de los derechos de cancelación y oposición debería estar asociado a un ejercicio correlativo de tales derechos frente a los responsables de estos sitios web, que son quienes, en origen, permiten el acceso a la información personal, teniendo en cuenta que la actividad de los buscadores consiste en vincular los términos de búsqueda a las web en las que consta la información.

Sin embargo, hay una tipología de casos que está huérfana de solución, esto es, cuando la página web que aloja la información no puede borrar los datos porque está amparada legalmente o cuando entra en conflicto con otro derecho fundamental. La indexación por parte de los buscadores provocaría una difusión masiva de la información personal a la que todo el ciudadano con un motivo legítimo se opone. Este tipo de casos recibidos por la AEPD se tratan principalmente de demandas contra la indexación y recuperación por buscadores de Internet de datos personales contenidos en boletines oficiales y ediciones digitales en medios de comunicación. A juicio de la AEPD, a pesar de que los responsables de las web pueden tener impedido terminar el tratamiento de los datos, en virtud de exigencia legal, o al encontrarse amparado a mantener la información, esta obligación o amparo no es exigible o aplicable al responsable del servicio de búsqueda. Lo que la AEPD busca con la efectividad del derecho de oposición del tratamiento de datos del buscador es limitar el efecto divulgativo multiplicador que se produce a través de estos motores de búsqueda indeseado por los titulares de los derechos vulnerados.

> Por tanto, el derecho de oposición 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.

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. 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; y, por otro lado, 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. 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.

Es imprescindible señalar que Google ha impugnado sistemáticamente ante la jurisdicción contencioso-administrativa las resoluciones de la AEPD que le instaban a desindexar ciertos datos. Esta situación 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 de sitios web, las competencias de las Autoridades de protección de datos y la posibilidad de evitar la indexación de la información personal.

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.

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.

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.

3) Por último, los magistrados de la Sala de lo Contencioso peguntan 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 perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?"

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 viene utilizado la AEPD para fundamentar algunas de sus resoluciones

B) Los requisitos y límites del derecho al olvido digital: principios reguladores y necesaria ponderación frente a otros derechos fundamentales.

> Ningún derecho fundamental es absoluto ni ilimitado. El derecho al olvido no escapa a esta categórica afirmación, pues la pretensión del ejercicio de cancelación u oposición puede chocar con los derechos, por ejemplo, de libertad de información o expresión de otras personas.

Para la resolución de estos conflictos, es necesario atender en primer lugar a dos principios que vertebran el tratamiento legítimo de los datos personales en Internet, esto es, el principio del consentimiento y el principio de la finalidad. En segundo lugar, la AEDP ha utilizado para sus resoluciones la doctrina dictada por el Tribunal Constitucional y el Tribunal Europeo de Derechos Humanos en materia de ponderación entre derechos del ámbito de la información en conflicto, como el honor, intimidad y propia imagen frente a la libertad de expresión y de información.

- ***Principio del consentimiento.***

En todos los derechos fundamentales del ámbito de la información, el consentimiento es un elemento esencial. Para no vulnerar el derecho contenido en el art. 18.4 CE es imprescindible que todo tratamiento de datos personales se realice contando con el previo consentimiento inequívoco del afectado (art.6.1 LOPD). Además, conforme a la doctrina del Tribunal Constitucional señalada anteriormente, el consentimiento puede ser revocado cuando exista causa justificada (art. 6.3 LOPD).

> La misma LOPD define consentimiento como "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le concierne." (art. 3.h) LOPD).

Como señala SIMÓN CASTELLANO, el principio del consentimiento del afectado, a efectos del derecho al olvido, es aplicable en un supuesto doble. En primer lugar, cuando una persona consiente o él mismo publica una información que contiene datos personales en la red. En este caso, el interesado puede revocar su consentimiento y exigir que aquello que antes permitió —la divulgación de fotos, videos, comentarios, etc. en Internet— desaparezca. Esta posibilidad es especialmente útil en las plataformas de vídeo (por ejemplo, Youtube) o en redes sociales. En segundo lugar, puede que un tercero haya publicado información que contenga datos personales como comentarios, imágenes, vídeos, etc, sin el consentimiento del interesado. Ante esta

situación, esta persona puede oponerse a la información publicada, con la excepción de si esa información entra dentro del ámbito protegido de alguno de los derechos fundamentales de libertades informativas. Por último, existe una tercera situación en la que la LOPD reputa como innecesario o irrelevante el consentimiento del interesado titular de los datos personales: cuando estos estén contenidos en fuentes de carácter público, como los diarios y boletines oficiales (art. 11.2.b) LOPD). Este principio de consentimiento se complementa con el principio de finalidad.

- ***Principio de finalidad.***

El art. 11.1 LOPD señala tajantemente que "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". A juicio de SIMÓN CASTELLANO, "el principio de finalidad podría constituir una base sólida para el derecho al olvido digital, al establecer que los datos personales serán eliminados o borrados una vez que estos hayan dejado de ser útiles a la finalidad con la que se registraron". Así lo establece el art. 4.5 LOPD al afirmar que "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."

> El citado académico prosigue afirmando que "el derecho al olvido digital actuaría como un instrumento que persigue el efectivo cumplimiento del principio de finalidad, que exige que los datos personales sólo puedan utilizarse para la finalidad concreta para la que fueron registrados, y una vez ya no son necesarios a tal efecto se produciría su cancelación. No obstante, no en todos los casos la cancelación es posible, especialmente si los datos personales están contenidos en fuentes que tiene la consideración de accesibles al público."

Este principio de finalidad ha sido uno de los principales argumentos sobre los que la AEPD ha basado su constante demanda a los buscadores para que limitar la divulgación de informaciones pasadas que contienen datos personales sin una autorización para su tratamiento.

Respecto a la ponderación de derechos, ha de insistirse en que el derecho a la protección de datos personales no constituye una excepción al carácter limitado de los derechos fundamentales. Es pertinente enfatizar la afirmación constante del Tribunal Constitucional sobre los límites inherentes a todo derecho fundamental de que "aunque la Constitución no imponga expresamente límites específicos a un derecho fundamental determinado, 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 11/1981, de 8 de abril, FJ 7; respecto del art. 18 CE, STC 110/1984, FJ 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental." (STC 292/2000, de 30 de noviembre, FJ 11).

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 las solicitudes de oposición y cancelación del tratamiento de datos personales.

En este sentido, un criterio muy utilizado por la AEPD es la ***relevancia pública*** de los datos personales, como por ejemplo la comisión de un delito (Procedimiento Nº: TD/01041/2012, resolución Nº: R/02553/2012) (o su no relevancia: Procedimiento Nº: TD/00796/2012, RESOLUCIÓN Nº: R/02010/2012). Es adecuado aquí volver a insistir en la afirmación de la AEPD de 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 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 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" (Procedimiento Nº: TD/00796/2012, resolución Nº.: R/02010/2012).

La ***exactitud de los datos personales*** utilizados es otro de los criterios utilizados por la AEPD (Procedimiento Nº: TD/01041/2012, Resolución Nº.: R/02553/2012), 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*** (STC 21/2000, de 31 de enero, FJ 6). La ***antigüedad de los datos***, exigiendo que no sean obsoletos (Resolución Nº.: R/02010/2012), 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.

4.4 POSITIVACIÓN DEL DERECHO AL OLVIDO POR EL LEGISLADOR EUROPEO: PROPUESTAS DE REGLAMENTO Y DIRECTIVA

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 un nuevo Reglamento (*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*) y una nueva Directiva de protección de datos de carácter personal (*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*).

El proyecto de Reglamento consagra en el art. 17 el pretendido derecho al olvido. Éste 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 (art. 17.3 Propuesta de Reglamento COM (2012) 9 final), o en caso de que existan motivos para restringir el tratamiento de los datos en vez de proceder a su supresión (art. 17.4 Propuesta de Reglamento COM (2012) 9 final).

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 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 (art. 17.2 Propuesta de Reglamento COM (2012) 9 final). 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 no podía ser de otra manera, la Propuesta de Reglamento de Protección de Datos tiene muy en cuenta la ponderación de derechos fundamentales. En lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, reconoce que el derecho a la protección de datos personales podría tener incidencia en los siguientes derechos fundamentales consagrados en la Carta de Derechos Fundamentales de la Unión Europea: la libertad de expresión (art. 11); la libertad de empresa (art. 16); el derecho a la propiedad y especialmente a la protección de la propiedad intelectual (art. 17.2); la prohibición de toda discriminación, y en particular la ejercida por 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).

5. A modo de conclusión

Internet ha supuesto una revolución total en cualquiera de los ámbitos en los que haya hecho acto de presencia. En el mundo de las relaciones sociales la web 2.0 ha posibilitado un acceso y tratamiento de datos personales prácticamente ilimitado. Tras un inicio en el que los usuarios no eran muy conscientes de los riesgos que este comportamiento entrañaba, cada vez más se demanda por parte de los usuarios un poder de controlar el acceso y tratamiento de los datos personales. De esta manera surge la configuración del derecho al olvido digital, a partir principalmente de los derechos de cancelación y oposición de los datos personales frente a páginas web y motores de búsqueda. El ejercicio de estos derechos incide en el ámbito de protección de otros derechos fundamentales, y puede implicar su restricción. Corresponde al mundo del Derecho establecer garantías que protejan los derechos de las personas de los nuevos riesgos que plantean las nuevas tecnologías. Por ello, es necesario, sin duda alguna, arbitrar medidas que aseguren el necesario equilibrio entre el carácter abierto de Internet y la protección de otros derechos fundamentales como base de las sociedades democráticas en las que vivimos. Desde el punto de vista del Derecho, este desafío no ha hecho más que comenzar.

6. BIBLIOGRAFÍA

BOIX PALOP, A., "Libertad de expresión y pluralismo en la red", *Revista Española de Derecho Constitucional*, nº 65, 2002, pp. 133-180.

BOIX REIG, J., (Dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010.

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*, 2002, nº. 62.

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

HEREDERO CAMPO, Mª. T., "Web 2.0: Afectación de derechos en los nuevos desarrollos de la web corporativa", *Cuadernos Red de Cátedras Telefónica*, nº 6, mayo 2012.

MORENO NAVARRETE, M.A., "Aspectos jurídico privados de las tecnologías Web 2.0 y su repercusión en el derecho a la intimidad", en BOIX REIG (Dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010, pp. 335-360.

RALLO LOMBARTE, A., "El derecho al olvido y su protección", *TELOS, Cuadernos de comunicación e innovación*, nº 85, Octubre - Diciembre 2010.

SALGADO SEGUÍN, V.A., "Intimidad, privacidad y honor en Internet", *TELOS, Cuadernos de Comunicación e Innovación*, nº 85, Octubre-Diciembre, 2012.

SIMÓN CASTELLANO, P., *El régimen constitucional del Derecho al Olvido Digital*, Tirant lo Blanch, 2012.

SIMÓN CASTELLANO, P., "El derecho al olvido en el universo 2.0", *Textos Universitaris de Biblioteconomia i Documentació*, nº 28, junio 2012.

LEGISLACIÓN Y DOCUMENTACIÓN JURÍDICA

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

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

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

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.

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.

Convenio Europeo de Derechos Humanos.

Carta de Derechos Fundamentales de la Unión Europea.

Tratado de Funcionamiento de la Unión Europea.

Decisión Marco 2008/977/JAI, 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).

Eurobarómetro especial (EB) 359, *Data Protection and Electronic Identity in the EU* (Protección de datos e identidad electrónica en la UE, 2011): http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf; así como el *Comparativestudyondifferentapproachesto new privacychallenges, in particular in the light of technologicaldevelopments, enero de 2010* http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

Dictamen 5/2009 sobre las redes sociales en línea, Comisión Europea, Grupo de Trabajo sobre Protección de Datos del artículo 29.

JURISPRUDENCIA

- STC 11/1981, de 8 de abril
- STC 73/1982, de 2 de diciembre
- STC 110/1984, de 26 de noviembre
- STC 89/1987, de 3 de junio.
- STC 196/1987, de 11 de diciembre
- STC 231/1988, de 2 de diciembre
- STC 197/1991, de 17 de octubre
- STC 254/1993, de 20 de julio
- STC 143/1994, de 9 de mayo
- STC 254/1994, de 9 de mayo,
- STC 11/1998, de 13 de enero.
- STC 94/1998, de 4 de mayo
- STC 134/1999, de 15 de julio
- STC 144/1999, de 22 de julio
- STC 166/1999, de 27 de septiembre.
- STC 202/1999, de 8 de noviembre
- STC 98/2000, de 10 de abril,
- STC 115/2000, de 10 de mayo.
- STC 127/2000, de 16 de mayo
- STC 292/2000, de 30 de noviembre.
- STEDH, *caso X e Y*, de 26 de marzo de 1985
- STEDH *caso Leander*, de 26 de marzo de 1987,
- STEDH *caso Gaskin*, de 7 de julio de 1989
- STEDH *caso Funke*, de 25 de febrero de 1993.
- STEDH *caso Z*, de 25 de febrero de 1997.
- STJUE 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