

**LA CONFIGURACIÓN JURÍDICA
DEL DERECHO AL OLVIDO
EN EL DERECHO ESPAÑOL A TENOR
DE LA DOCTRINA DEL TJUE**

M^a BEGOÑA LÓPEZ PORTAS

SUMARIO

I. LA PROTECCIÓN DE DATOS EN LA RED Y SUS PRINCIPALES PROBLEMAS JURÍDICOS. II. EL MARCO JURÍDICO DEFINIDO EN EL DERECHO INTERNO ESPAÑOL. III. IMPORTANCIA DE LA SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA DE 13 DE MAYO DE 2014. IV. CONCLUSIONES: PECULIARIDADES DE LA REGULACIÓN EN VIGOR.

Fecha recepción: 23.02.2015

Fecha aceptación: 4.05.2015

LA CONFIGURACIÓN JURÍDICA DEL DERECHO AL OLVIDO EN EL DERECHO ESPAÑOL A TENOR DE LA DOCTRINA DEL TJUE

M^a BEGOÑA LÓPEZ PORTAS

Profa. Contratado-doctora, Universidad de Santiago de Compostela

I. INTRODUCCIÓN: PRINCIPALES PROBLEMAS JURÍDICOS QUE PLANTEA LA PROTECCIÓN DE DATOS EN LA RED

La privacidad, entendida por WARREN y BRANDEIS como el «derecho a que te dejen en paz o el derecho al olvido»¹, se ha descrito como el más com-

¹ WARREN, S. D. y BRANDEIS, L. D. «The Right to Privacy», *Harvard Law Review*, Vol. IV, n° 5, diciembre, Boston, 1890, p. 213. Debemos destacar, sin embargo, que la teoría de WARREN y BRANDEIS no fue unánimemente aceptada en Estados Unidos si no que dio lugar a distintos debates doctrinales sobre los supuestos de responsabilidad que abarcaría el concepto de *Privacy* interpretado por los jueces. Así, fue el caso de las posturas de PROSSER, KALVEN y BLOUSTEIN. Por un lado, PROSSER estableció cuatro categorías de *torts* —intrusiones a la intimidad— sin que se produjesen este tipo de actos en el caso de la difusión pública de hechos privados (Cfr. PROSSER, W. L.: «Privacy», en *California Law Review*, vol. 48, UC Berkeley, California, 1960, pp. 63-67). Por su parte, KALVEN manifestó ciertas dudas sobre el interés realmente protegido por la *Privacy* y criticó la tendencia a sustituir las acciones de libelo y difamación por la protección derivada del *right to privacy* (Cfr. KALVEN, H. Jr.: «Privacy in a tort law. Where Warren and Brandeis wrong?», en *Law and Contemporary Problems*, n° 31, (spring) Duke Law School, Duke University, Carolina del Norte, 1966, pp. 326-341, <http://scholarship.law.duke.edu/lcp/vol31/iss2/7>). Finalmente, BLOUSTEIN fue más allá y entendió la existencia de una afectación a la inviolabilidad de la persona cuando se revelan ciertos aspectos de la vida privada que resultan sometidos a la opinión pública y recondujo los *torts* de PROSSER a una única categoría fundamentada en la protección de la dignidad personal (Cfr. BLOUSTEIN, E. J.: «Privacy as an aspect of human dignity: as an answer to

pleto de los derechos y el más valorado por los hombres civilizados. Sin embargo, en los últimos años esta percepción puede haber cambiando en el contexto de la sociedad de la información. La proliferación de nuevos sistemas tecnológicos ha ampliado los umbrales de la tolerancia pública ante la intromisión en la esfera privada y personal, más aún cuando se configuran páginas *webs* inteligentes, las denominadas *webs 3.0*². Esta nueva plataforma tecnológica no sólo permite una comunicación multidireccional entre los internautas sino también facilita la acumulación de grandes cantidades de información sobre los mismos sin ningún tipo de control. Las *webs* inteligentes 3.0 o programas inteligentes presentan un nuevo reto jurídico al permitir la creación de grandes bases de datos sobre las preferencias de los usuarios configuradas a partir de la información guardada de sus búsquedas personalizadas. A suerte de un panóptico digital³, los buscadores y administradores de datos en Internet actúan no sólo almacenando reseñas de los ciudadanos sino también orientando de forma individualizada sus búsquedas en la red. Esto facilita la elaboración de perfiles digitales de los cibernautas que inciden directamente sobre su intimidad y, al mismo tiempo, que el vigilante incomunicado pueda orientar su escrutinio en función de sus apreciaciones personales, sus intereses económicos, perjuicios o valores.

Dean PROSSER», en *New York University Law Review*, vol. 39, diciembre, New York University, New York, 1964, pp. 964-1007, <http://heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/nylr39&div=71&id=&page=>). Para un estudio más exhaustivo sobre esta discusión doctrinal debe consultarse MARTÍNEZ MARTÍNEZ, R.: *Una aproximación crítica a la autodeterminación informativa*, Estudios de protección de datos, Thomson Civitas, Madrid, 2004, pp. 73-78). Hoy en día, como veremos, la interpretación de BLOUSTEIN centrada en la dignidad personal resulta esencial para la protección de la intimidad ante las nuevas tecnologías como destaca la jurisprudencia española y europea.

² El neologismo *web 3.0* surge en el año 2006 a raíz de un artículo de un estudioso de los estándares *web* como superación al concepto de *web 2.0* que había comenzado a emplearse en el año 2004 para referirse a las páginas de Internet que permiten interactuar a los ciudadanos en tiempo real y de una forma pública bien con fines profesionales o particulares a través de motores de búsqueda, de las redes sociales, compartiendo imágenes o vídeos (cfr. ZELDMAN, J., «Web 3.0», *Published in JavaScript, Business, Industry, Usability*, 95 Comments, January 17, 2006 (<http://alistapart.com/article/web3point0>)).

³ A partir del concepto anglosajón de la actual panoptización social —basado en la extensión del modelo penitenciario establecido en la obra de Jeremy BENTHAM «El panóptico»—, Lyall KING en el año 2001 definió el término de panóptico electrónico como el conjunto de los actuales sistemas de control tecnológico ejercido en los países desarrollados por las empresas privadas o los estados sobre las actividades informáticas cotidianas de ingresar en un portal de Internet o pagar con una tarjeta de crédito (cfr. KING, L., «Information, Society and Panopticon», *The Western Journal of Graduate Research*, 2001, vol. X (1), Ontario, Canadá, p. 45).

Así, una de las mayores preocupaciones que amenazan la libertad de comunicación en la red es el control de su potencial manipulación⁴. Los servidores o los responsables del tratamiento de datos automatizados, al chequear las páginas *web* a las que accede el usuario a través del registro de las *cookies* y direcciones *IPs*, pueden elaborar perfiles personales que inciden directamente sobre su privacidad. Al mismo tiempo, Internet ha permitido que los ciudadanos se hayan convertido en el origen y el destino de la información que circula en la misma, lo que complica la diferenciación entre la voluntad de informar y la publicidad de los datos. Este hecho redundante en una menor protección de sus derechos personalísimos, al ser sus propios titulares los que exponen datos íntimos sin valorar en su totalidad las repercusiones que implican en términos de publicidad. El empleo de dispositivos electrónicos como los móviles o las *tablets* logra captar y subir fotos o grabaciones en tiempo real a la red. Esta difusión inmediata de elementos correspondientes a su vida privada, que permiten el rastreo e identificación del usuario que compartió la información en la *web*, posibilita articular un derecho de oposición o corrección con ciertas peculiaridades. Finalmente, otro de los rasgos destacados que definen este nuevo contexto digital es que la información vertida no conoce de fronteras ni límites espacio temporales, el espacio y el tiempo se difuminan en la red. Por este motivo, en la medida en que la difusión de los datos es inmediata, la censura se ve condicionada como mecanismo de prevención de daños sobre la intimidad personal. El posible control o la corrección de la publicación en este ámbito es *a posteriori* y se centra básicamente en identificar al usuario que la facilitó, pero difícilmente puede suponer la definitiva eliminación de los datos.

⁴ Se abre así un peligroso campo de indefensión jurídica, la posibilidad del establecimiento de detallados perfiles de los usuarios con diversos fines. De este modo, podemos señalar que se configuran perfiles que buscan ajustar la oferta publicitaria bien mediante el control contenido existente en el dispositivo electrónico (cfr. «Twitter recaba información de las aplicaciones instaladas por los usuarios» noticia publicada en el periódico *La Voz de Galicia*, con fecha de 27 de noviembre de 2014, disponible en Internet <http://www.lavozdeg Galicia.es/noticia/vidadigital/2014/11/27/twitter-recaba-informacion-aplicaciones-instaladas-usuarios/00031417069222437167401.htm>) o bien en función de la localización geográfica (Cfr. «Facebook cambia la privacidad y guardará los datos bancarios» noticia publicada en el periódico *El País*, con fecha de 13 de noviembre de 2014, disponible en Internet http://tecnologia.elpais.com/tecnologia/2014/11/13/actualidad/1415890898_584637.html). E, incluso, cabe subrayar que se llega a la experimentación emocional de los internautas mediante el procedimiento de los *A/B testing* (cfr. «Facebook experimentó con 689.000 usuarios sin su consentimiento», publicada en el periódico *El País*, con fecha de 30 de junio de 2014, disponible en Internet http://tecnologia.elpais.com/tecnologia/2014/06/30/actualidad/1404108700_038585.html); o «La polémica por la manipulación emocional de Facebook», publicada por la BBC, ese mismo día 30 de junio de 2014, disponible en la dirección http://www.bbc.co.uk/mundo/noticias/2014/06/140630_tecnologia_facebook_experimento_emociones_criticas_lv.shtml).

Bajo cierta controversia jurídica, el legislador español adopta distintas soluciones que pretenden hacer frente a esos obstáculos con los que se encuentra la censura en el ámbito digital. Es el caso de la disposición final cuadragésimo tercera incluida en la Ley 2/2011, de 4 de marzo, de economía sostenible que modifica la Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y comercio electrónico. La conocida como *Ley Sinde* permitió el cierre y la retirada de contenidos de las *webs* por decisión unilateral de la sección segunda de la Comisión de propiedad intelectual dependiente del Ministerio de Cultura, previa autorización de los tribunales contencioso administrativos. Esta medida preventiva de censura, sin embargo, conlleva una serie de problemas jurídicos tan relevantes como el relativo a la garantía jurídica de los derechos fundamentales ya que ignoraba la exigencia establecida en el artículo 81.1 de la Constitución. La limitación de las libertades informativas y el respeto al derecho a la tutela judicial efectiva se realizaba mediante una Ley ordinaria y no a través de una Ley orgánica.

Una inseguridad jurídica a la que pretendió hacer frente el *Reglamento Wert* al establecer un procedimiento que en el caso de la infracción del derecho de propiedad intelectual se dirige contra el administrador de la página *web* de enlaces. El Real Decreto 1889/2011, de 30 de diciembre por el que se regula el funcionamiento de la Comisión de propiedad intelectual, estableció un procedimiento administrativo-judicial con el fin de asegurar el equilibrio entre la defensa de los derechos de propiedad intelectual en la red y otros derechos fundamentales como la protección de los datos personales, la libertad de expresión o el derecho a la información. Esta norma reservaba la competencia de decisión que afectase a estos derechos a la jurisdicción contencioso administrativa y no a la jurisdicción civil. De este modo, la falta de consenso entre los tribunales civiles se pretende solucionar mediante la atribución de la competencia sobre estos asuntos a otra jurisdicción a la que esta materia resulta extraña. Por otro lado, la complejidad y rigidez del procedimiento establecido en el Real Decreto puede ser otra de las cuestiones criticables de la norma. Y, finalmente, debemos subrayar que la indefinición de una posible sanción del usuario, que condicionan la necesidad de una nueva reforma la Ley de propiedad intelectual, agrava todavía más la sensación de inseguridad jurídica⁵.

⁵ Cfr. MINERO ALEJANDRE, G.: «Análisis comparado de las soluciones normativas y jurisdiccionales para la lucha frente a la piratería en Internet en España, y los países de nuestro entorno» en VV. AA *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Cuadernos y Debates n.º 215, Centro de Estudios Político Constitucionales, Madrid, 2013, pp. 231-232.

En definitiva, por la propia naturaleza de los datos íntimos disponibles en Internet, el ejercicio del derecho de oposición por el individuo resulta muy difícil y los derechos de información, de acceso, de rectificación y cancelación revisten características singulares. En este ámbito emerge en el contexto europeo el derecho al olvido como un nuevo derecho ligado a la defensa de la privacidad de los ciudadanos en el ámbito de Internet y relacionado con la *censura a posteriori*. En los últimos años el derecho al olvido digital surge como una reacción a la atemporalidad de los datos personales en la red, es decir, como una garantía personal frente a su tratamiento masivo y descontrolado⁶. Este derecho abarca tanto a la oposición al tratamiento ilegítimo de los datos personales o su supresión y como la facultad de que terceros recuerden hechos veraces desactualizados, carentes de notoriedad pública en el presente. El reconocimiento jurídico de la existencia de un derecho al olvido de la información no relevante contenida en la *web* por parte de los buscadores como *Google* puede ser el primer paso a la hora de garantizar la privacidad de los datos de los internautas en este nuevo contexto tecnológico. Ahora bien, este derecho tendrá unos límites distintos en función de la tradición jurídica del país que lo regule. En *estados civilistas*, su configuración y su aplicación genera menos problemas lo que favorece a su reconocimiento por sus agencias de protección de datos⁷. Este es el caso de Francia, Italia o España. Al respecto Cotino Hueso nos recuerda que, en el conflicto de libertades públicas y protección de datos, la articulación legal de los límites de los supuestos señalados no es obligatoria pues dicha limitación proviene directamente de la Constitución española. En cualquier caso, aunque la Ley orgánica de protección de datos personales no especifica las posibles restricciones de la protección de datos a favor de la libertad de expresión, este problema que se ha amortiguado por los tribunales a través de la interpretación que realiza del artículo 6.1 de

⁶ Cfr. SIMÓN CASTELLANO, P.: «El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos», en VV. AA *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Cuadernos y Debates nº 215, Centro de Estudios Político Constitucionales, Madrid, 2013, p. 452.

⁷ En cambio en los países que siguen la tradición jurídica del *Common law*, al participar de una cultura en la que la difusión y el acceso a la información prima sobre las condenas penales, puede presentar ciertas dificultades reconocer la existencia de un derecho que hace prevalecer la protección de datos frente el derecho a informar (Cfr. SIMÓN CASTELLANO, P.: «El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos», en VV. AA *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Cuadernos y Debates nº 215, Centro de Estudios Político Constitucionales, Madrid, 2013, pp. 453-454).

la citada ley en el que se determina la necesidad del consentimiento inequívoco del afectado⁸.

En consecuencia, aun cuando los perfiles jurídicos que definen el objeto de análisis están pendientes de una regulación definitiva a través de un Reglamento europeo específico⁹, cobra urgencia su estudio dada la relevancia que adquiere el reciente pronunciamiento efectuado por el Tribunal de Justicia de Estrasburgo en este contexto. Una respuesta jurídica acotada que pretende hacer frente a un atentado global e ilimitado a los bienes y derechos en la red¹⁰. Una preocupante paradoja que plantea un nuevo reto para los ordenamientos jurídicos nacionales y supranacionales, el de su reglamentación jurídica. Por ello, dados los peligros reales de una utilización abusiva de este espacio por los gigantes de las telecomunicaciones, así como del riesgo de control social o político, apremia una ordenación jurídica de sus límites. A partir de su contextualización en el Derecho interno español, este trabajo se detendrá en el análisis de los avances producidos en este ámbito a raíz de Sentencia de 13 de mayo de 2014 si bien destacará asimismo algunos de los principales problemas carentes todavía de una precisa concreción normativa.

II. EL MARCO JURÍDICO DEFINIDO EN EL DERECHO INTERNO ESPAÑOL

La dignidad humana es el punto de arranque, lógico y ontológico, del reconocimiento de los demás derechos¹¹. Como valor jurídico, la dignidad garantiza el derecho de toda persona a definir libremente su proyecto de vida sin que los

⁸ Así, sobre la posibilidad de que artículo 20 de la Constitución española permita el tratamiento de datos sin necesidad del consentimiento del afectado debe atenderse a la interpretación judicial realizada por la Audiencia Nacional —es el caso de las sentencias de 12 de enero de 2001, 2 de febrero de 2006 y de 16 de marzo de 2006— y por la Agencia Española de Protección de Datos —de manera particular, en las resoluciones E/00742/2007, E/01022/2006, E/01504/2007 o E/00500/2008, entre otras—. (Cfr. Sobre el cómo se realiza dicha ponderación, COTINO HUESO, L.: «Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público» en VV. AA. *Comentario a la ley orgánica de protección de datos de carácter personal*, TRONCOSO REIGADA, A. (dir.), Civitas Thomson Reuters, Madrid, 2010, pp. 308-316).

⁹ En concreto, el artículo 17 del borrador de proyecto de Reglamento europeo prevé de manera pacífica el derecho al olvido como la mera supresión de los datos no necesarios o cuando no atiendan al a finalidad para la que fueron recogidos o tratados.

¹⁰ Cfr. PÉREZ LUÑO, A.: «Internet y Derechos Humanos», *Derecho y Conocimiento*, vol.2, Facultad de Derecho, Universidad de Huelva, Huelva, 2002, p. 105.

¹¹ Cfr. STC 53/1985 en su fundamento jurídico 3.

derechos reconocidos en el artículo 18 de la CE¹² puedan verse alterados por la acción recordatoria de terceros sobre hechos acontecidos en el pasado. La auto-determinación informativa recogida en el apartado 4 de dicho artículo surge así como el derecho personal que permite el control sobre datos íntimos que, en su vertiente de difusión de informaciones pasadas, pueden afectar el desarrollo vital de un ciudadano, el denominado el derecho al olvido.

La universalidad de la información, la potencial interceptación de las comunicaciones y los riesgos de acceso, difusión o alteración de los datos por parte de terceros son una constante preocupación para la normativa española. En un primer intento para evitar la publicación en Internet de la información privada, se atiende a la regulación de los derechos de acceso, rectificación y cancelación de los datos privados que constasen en bases públicas o privadas. De manera que el derecho al olvido coincide así con el derecho de cancelación de datos. Una equiparación que presenta ciertos inconvenientes, sobre todo en lo que se refiere a la cancelación o rectificación de bases de datos oficiales —al ser éstas excluida de la regulación general¹³—, en lo referente al problema de los antiguos datos difundidos o publicados en diarios o periódicos digitales, o a la dificultad que entraña la aplicabilidad de la normativa nacional a empresas o servidores de Internet domiciliados fuera de las fronteras europeas¹⁴.

De modo específico, respecto al acceso, oposición y cancelación de datos en la *web*, debemos indicar que en virtud del artículo 9 de la Ley de protección de datos y de los Reales Decretos-ley 994/1999 y 195/2000 —que trasponen la previsión del artículo 17 de la Directiva 95/46/CE¹⁵— se establece la obligación

¹² Sobre la existencia del vínculo intrínseco entre los derechos de la personalidad, reconocidos en el artículo 18 de la Constitución española, y la dignidad, contemplada en el artículo 10 de la CE, puede consultarse el fundamento jurídico 3 de la STC 231/1988. Nos encontramos ante un tipo de derechos amparan a la persona en cuanto tal al asegurarle una esfera de autonomía esencial e individual y cuya existencia y garantía es consustancial a la propia personalidad (cfr. BLANCO VALDÉS, R. L.: *La Constitución de 1978*, Alianza editorial, Madrid, 2011, pp. 285-286).

¹³ Bases de datos que están expresamente excluidas de la regulación general a tenor de lo dispuesto en los artículos 2 y 23 de la Ley orgánica 15/1999, de protección de datos de carácter personal.

¹⁴ Sobre la problemática para la cancelación de noticias recogidas por los servidores de Internet a partir de las hemerotecas de los periódicos digitales y la interpretación efectuada por la AEPD recientemente, debe consultarse ORZA LINARES, R. M.: «Derecho al olvido en Internet: algunos intentos para su regulación legal», en VV. AA *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Cuadernos y Debates nº 215, Centro de Estudios Político Constitucionales, Madrid, 2013, pp. 478-487.

¹⁵ A la espera de la aprobación de un futuro Reglamento sobre protección de datos, la Directiva 95/46/CE del Parlamento europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las físicas se configura como la piedra angular sobre la que descansa la normativa

del responsable del tratamiento de aplicar las medidas técnicas de organización adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental o la alteración, la difusión o el acceso no autorizados, en particular, cuando el tratamiento incluya la transmisión de datos en una red.

Siguiendo el mismo precepto de la Directiva 95/46/CE y en virtud de los artículos 4 y 5 de la Directiva 2002/58/CE, la Ley 32/2003, de 3 noviembre General de Telecomunicaciones en sus los artículos 33 y 34 define las medidas técnicas o de gestión precisas para garantizar un nivel de seguridad adecuado y determina el deber de informar a los abonados y usuarios sobre cualquier riesgo especial, sobre todo cuando se trate de un tratamiento ilícito de datos personales¹⁶.

La última aportación legislativa española destacable sobre la privacidad individual en Internet en el campo de las comunicaciones electrónicas es el Real Decreto-ley 13/2012, de 30 de marzo por el que se trasponen las directivas en materia de mercados interiores de electricidad y gas y en el ámbito de las comunicaciones electrónicas. En concreto, nos referimos a la Directiva 2009/136/CE sobre la privacidad de este tipo de comunicaciones. En relación con las *cookies* y la esfera privada de los usuarios, este Real Decreto modificó, con algunas deficiencias, el artículo 22 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información. De manera que, en esta norma se refuerzan las obligaciones de información al exigir la obtención previa del consentimiento de los destinatarios como requisito necesario para la legitimidad de la instalación de

europaea en lo que respecta al tratamiento de datos personales y a su libre circulación. Esta Directiva fija una detallada regulación sobre la protección de datos centrada en el contenido del derecho a la intimidad sin que ello suponga excluir la concurrencia de otros derechos fundamentales. El ámbito de aplicación de la esta norma es más restringido que el del Convenio 108 del Consejo de Europa pues sólo se aplica al tratamiento total o parcialmente automatizado de datos personales y al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. La Directiva 95/46 articula específicamente el derecho de acceso a los datos así como el ejercicio del derecho de rectificación y de oposición al tratamiento de datos por el interesado y autoriza la transferencia de datos personales de un Estado miembro a un tercer país si garantiza un nivel de protección adecuado. Ahora bien, el derecho de oposición no se reconoce con carácter general en la Directiva 95/46/CE pero, como señala GUERRERO PICÓN, vistos los términos en los que se pronuncia esta norma, tampoco se puede concluir que se circunscribe a los dos supuestos de datos que enuncia en los artículos 7.e) y 7.f) y al tratamiento de sus datos destinado a la prospección. (Cfr. GUERRERO PICÓ, M^a del C.: «El Derecho fundamental a la protección de los datos de carácter personal en la Constitución Europea», *Revista de Derecho Constitucional Europeo*, n^o 4, julio-diciembre, Facultad de Derecho de la Universidad de Granada, Granada, 2005, pp. 305-3006. <http://www.ugr.es/~redce/REDCE4/articulos/12guerrero.htm>).

¹⁶ Cfr. BALLESTEROS MOFFA, L. Á.: *La privacidad en Internet. Internet en el centro de protección*, monografías n^o 413, Tirant lo Blanch, 2005, p. 154

las *cookies*. Sin embargo, no se determina con claridad quién será el responsable de avisar sobre las *cookies* a los internautas —sí los editores o los prestadores de servicios— y tampoco se especifica quién será el encargado del tratamiento ni de la gestión de los datos personales obtenidos o qué consecuencias se prevén en caso de incumplimiento¹⁷.

A partir de la configuración de un nuevo marco jurídico europeo —compuesto por la Directiva 2009/136/CE, sobre los Derechos de los Usuarios, y la Directiva 2009/140/CE para una Mejor Regulación—, se ha avanzado un paso más en la protección de datos en este campo. Así, en la Ley general de telecomunicaciones 9/2014, de 9 de mayo se introducen una serie de medidas destinadas a crear un ámbito adecuado para la realización de inversiones en el despliegue de redes de nueva generación. Estas disposiciones pretenden que los operadores ofrezcan servicios innovadores y tecnológicamente más adecuados a las necesidades de los ciudadanos y, al mismo tiempo, garanticen el cumplimiento de los objetivos de la Agenda digital para Europa. En su Título I, esta Ley excluye de su regulación la prestación de servicios sobre las redes de telecomunicaciones que no consistan principalmente en el transporte de señales a través de las mismas, remitiéndose en este caso a la regulación contenida en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Motivo por el que, a la espera de la modificación de esa Ley 34/2002 —que hace responsable al prestador de servicios¹⁸—, las deficiencias de técnica legislativa señaladas se han ido corrigiendo en la práctica¹⁹ sobre todo por la interpretación jurisprudencial y por la acción de la Agencia Española de Protección de Datos.

Recordemos que la privacidad se presenta como un concepto jurídico más amplio que el de la intimidad, pues en sí misma engloba un mayor número de facetas de la personalidad que, aunque consideradas aisladamente pudieran care-

¹⁷ Cfr. MARTÍNEZ PASTOR, E. y MÚÑOZ SALDAÑA, M.: «En busca de equilibrio entre la regulación y la autorregulación de la publicidad comportamental en línea», *Estudios sobre el mensaje periodístico*, vol.19, marzo, Universidad Complutense, Madrid, 2013, p. 292 (<http://revistas.ucm.es/index.php/ESMP/article/viewFile/42036/40017>).

¹⁸ Cfr. El apartado quinto de la Disposición final 2ª de la Ley 9/2014, de 9 de mayo, de telecomunicaciones.

¹⁹ Así, en enero del 2013, el director de la Agencia Española de Protección de Datos resuelve sancionar a dos empresas españolas por infracción de la normativa de las *cookies* en lo que constituye el primer expediente sancionador incoado en España y uno de los primeros impuestos a nivel internacional en esta materia. A raíz de esta Resolución se plantea la necesidad por parte del titular de la página *web* de realizar no sólo un análisis previo y exhaustivo de las *cookies* para identificar a los terceros que puedan usarlas si no también deberá actualizar la política de *cookies* implantadas en la *web* así como de los sistemas de información y obtención del consentimiento de los usuarios (cfr. la Resolución de la AEPD de 14 de enero de 2013, R/02990/2013).

cer de significación, entrelazadas conformarían un retrato de la personalidad del individuo²⁰. Las libertades informativas, configuradas como la piedra angular sobre la que se asienta una opinión pública y libre esencial en un Estado democrático, no son elemento suficiente para legitimar la intromisión producida cuando colisionan con la protección de datos o la veracidad de la información. El interés público actualizado, el contexto en el que se produce la información y la proporcionalidad de la medida limitadora del derecho son los criterios manejados por la jurisprudencia constitucional²¹ para dirimir este conflicto entre libertades informativas y derecho al olvido²².

A partir de ahí, podemos precisar que el Tribunal Constitucional español interpreta la necesidad de favorecer a un bien jurídico positivo como es la privacidad, de la que derivan facultades de control sobre los datos e informaciones del individuo —como recogen, entre otras, las sentencias 254/1993, 11/1998, 94/1998, 104/1998 ó 44/1999—. Es decir, en el caso de privacidad electrónica nos encontramos ante una situación de desprotección de los usuarios de Internet lo que revierte directamente en el ámbito de la dignidad individual. En el marco específico de las nuevas tecnologías, debemos remitirnos a la doctrina asentada en la Sentencia 292/2000 en la que el máximo intérprete de la Constitución protege a la libertad informática al entender que dicha libertad posee una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad; esto se traduce en un derecho de control sobre los datos relativos a la propia persona. Además, el Tribunal Constitucional establece tanto una distinción entre el derecho a la protección de datos y el derecho a la intimidad como la necesidad de que el afectado conozca quién dispone de sus datos personales, qué datos dispone y con qué fin.

De este modo, el derecho a la protección de datos persigue el garantizar al individuo un poder de control sobre sus datos personales, no sólo desde el punto de vista de su uso sino también de su destino, con el fin de impedir una lesión de nuestra dignidad y derechos. Al mismo tiempo, este derecho supone garan-

²⁰ Cfr. El Auto de la Audiencia Provincial de Madrid de 21 de enero de 2004.

²¹ Véanse, entre otras, las sentencias del Tribunal Constitucional 9/2007, 192/1999, 110/2000 —sobre la necesidad de encontrar un equilibrio entre las libertades informativas y los derechos de la personalidad—; las sentencias 6/1988, 105/1990, 240/1992 ó 139/2007 —respecto a la relevancia pública de los hechos como límite interno a las libertades informativas—; y, en concreto, debe destacarse la Sentencia 139/2007 referida al interés público como criterio fundamental para justificar la publicación de la información a pesar del no consentimiento del titular.

²² Cfr. SIMÓN CASTELLANO, P.: «El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos» en VV. AA *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Cuadernos y Debates n.º 215, Centro de Estudios Político Constitucionales, Madrid, 2013, pp. 459-463).

tizar a los ciudadanos un poder de disposición sobre los datos personales e imponer a los terceros un deber de hacer respecto a los mismos. Es decir, el derecho a la protección de datos se distingue del derecho a la intimidad por el hecho de que sus garantías se extienden tanto sobre la intimidad —constitucionalmente protegida en el artículo 18.1— como sobre los datos íntimos —entendidos como tales cualquier información personal disponible por el afectado aunque sea público—. Mientras que el derecho a la autodeterminación informativa, contenido en el artículo 18.4 de la Constitución Española, atribuye a su titular un conjunto de poderes jurídicos cuyo ejercicio se impone como deberes ante terceros con un carácter instrumental ya que pretende garantizar a los ciudadanos el pleno ejercicio de sus derechos, todos ellos, no sólo los del artículo 18.1. Esos deberes, que conforman un grupo de instrumentos o poderes de disposición de datos por el interesado, son el de exigir el consentimiento del afectado en su recogida, el de informarle sobre el uso y destino de sus datos y el de establecer la facultad de obtención, acceso, rectificación y cancelación sobre los mismos.

El poder de disposición y control de los datos personales definido por la Carta Magna española se concreta jurídicamente tanto en la facultad de consentir sobre la recogida de los datos, su obtención y acceso como en la facultad de tratamiento, almacenamiento y uso posible por terceros, sean el Estado o los particulares. Pero al mismo tiempo, el Tribunal Constitucional subraya la existencia de unos complementos esenciales a esos poderes, como son la facultad de saber en todo momento quién dispone de esos datos, qué uso le daría y el poder de oponerse a esa posesión y uso. Por lo tanto, el derecho a ser informado de quién almacena los datos y el fin que les confiere y de los derechos de rectificación y cancelación, si proceden, se aúna un deber del tercero responsable de los mismos de informar sobre los datos que posee y el destino que les otorga²³.

El problema será entender si los datos identificativos de un titular o de una terminal telefónica que facilita el acceso a Internet se integran dentro del derecho a la intimidad personal —en concreto, en el ámbito de la protección de datos del artículo 18.1 de la Constitución española— o si forman parte del derecho al secreto de las comunicaciones del artículo 18.3 de nuestra Carta Magna. Estos dos derechos emergen con un carácter previo de protección al ciudadano, en el momento inicial del acopio de los datos tecnológicos. La intrusión producida posteriormente se articula con un carácter reparatorio a través del *Habeas Data* del 18.4 de la CE y mediante el reconocido como el derecho al olvido o derecho

²³ Cfr. «La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad», en LUCAS MURILLO DE LA CUEVA, P. y PIÑAR MAÑAS, J. L.: *El derecho a la autodeterminación informativa*, Fundación coloquio Europeo, Madrid, 2009, p. 38.

a la supresión de datos. En este sentido, precisaremos que el Tribunal Constitucional dos años más tarde se hace eco de la doctrina *Malone* asentada por el Tribunal de Estrasburgo de Derechos Humanos²⁴ al entender en la Sentencia 123/2002 que el secreto de las comunicaciones protegido por el artículo 18.3 de la Constitución y 8 del Convenio Europeo de Derechos Humanos alcanza no sólo a la confidencialidad de las comunicación en sí y de su contenido si no también a la identidad de los conferenciantes y a los datos externos de la conexión telefónica —como son, entre otros, el momento, la duración o el destino.

La doctrina del Tribunal Constitucional comentada se completa por la interpretación jurídica del Tribunal Supremo. Este órgano judicial fue más allá al diferenciar las comunicaciones telefónicas tradicionales —amparadas por el secreto de las comunicaciones— del acceso telefónico a Internet —pues las claves identificativas, *Internet Protocols (IPs)*, registran sólo al ordenador mientras que para poder conocer el número de teléfono²⁵ y el titular del contrato del mismo es necesaria previa autorización judicial—. De manera que, respecto al rastreo de internautas por la Policía, el Tribunal Supremo, en su Sentencia 236/2008, determina que los usuarios de Internet de un programa *P2P*, como el del supuesto enjuiciado EMULE, asumen que sus datos se convierten en públicos. Así pues, los cibernautas conocen o deberían conocer esta circunstancia²⁶. Es decir, estos

²⁴ Cfr. La Sentencia del Tribunal de Estrasburgo de Derechos Humanos de 2 de agosto de 1984, asunto 8691/79 —caso *Malone v. Reino Unido*—.

²⁵ Sobre la consideración de los números de teléfono como dato personal a tenor de la interpretación efectuada por la AEPD en su Informe 285/2006 y por las sentencias de la Audiencia Nacional de 26 de enero de 2005 (Recurso 1258/2002) y de 17 de septiembre de 2008 (Recurso 353/2007), debe consultarse PIÑAR MAÑAS, J. L.: «Concepto de dato de carácter personal» en VV. AA *Comentario a la ley orgánica de protección de datos de carácter personal*, TRONCOSO REIGADA, A. (dir.), Civitas Thomson Reuters, Madrid, 2010, pp. 203-204.

²⁶ A partir de la jurisprudencia del Tribunal Supremo, la interceptación de las comunicaciones telefónicas y telemáticas es objeto de atención en el proyecto de Ley orgánica de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica aprobado por el Consejo de Ministros el 13 de marzo de 2015. Mediante un nuevo capítulo que se integraría en el Título VIII del Libro II de la Ley de Enjuiciamiento Criminal se pretende colmar el vacío legal existente. En la futura regulación se pretende autorizar la intervención y registro de las comunicaciones de cualquier clase que se realicen a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual siempre que se adopte una decisión jurisdiccional de intervención. Entre las principales novedades que se introducirían podemos destacar como las siguientes: la admisión de la figura del agente encubierto para la persecución determinados delitos en el ámbito telemático previa autorización judicial; el registro de dispositivos informáticos de almacenamiento masivo y el registro remoto de equipos informáticos; la posibilidad de identificar a los terminales mediante la captación de códigos de identificación del aparato o sus componentes, tales como la numeración IMSI o IMEI y la imposición de un sistema de sellado o firma electrónica que garantice la infor-

datos públicos en Internet no se hallan protegidos ni por el artículo 18.1 ni por el artículo 18.3 de la Constitución por lo que pueden ser conocidos por la Policía sin necesidad de autorización judicial cuando el usuario de la red deja registrada su huella al acceder a una información ilegítima o irregular mediante estos programas.

El problema sobre la protección jurídica en este ámbito se agrava si consideramos el hecho de que cualquier búsqueda que realizamos en la *web* deja una impronta digital que permite a los servidores y buscadores elaborar un perfil del usuario con el que pueden comercializar. Elementos de búsqueda a los que no les damos apenas importancia y que, sin embargo, facilitan una reseña detallada e individualizada de los internautas a servidores como *Google*, *Yahoo!*, *ask.com*, *Microsoft Search*, *bing*, etc. Hasta tal punto que algún autor ha llegado a subrayar que *Google* conoce más de nosotros de lo que cada uno sobre sí mismo podría recordar o identificar²⁷. Una información valiosa de los ciudadanos que incide directamente sobre sus derechos personales y de la que no es consciente. Datos que pueden ser almacenados durante períodos de tiempo indeterminados y que, incluso, pueden permitir a los Estados el crear bancos de datos digitales²⁸ cuyos usos pueden ser cuestionados desde un punto de vista jurídico en función no sólo de su titular —privado o público— si no también de su fin.

Como acabamos de subrayar, Internet emerge como uno de los futuros retos que se presentan a la hora de garantizar el cumplimiento del artículo 18.4 de la Constitución española. La dimensión universal de la red dificulta la aplicación de la normativa jurídica, en concreto, en el caso español de las leyes 25/2007 u 11/2007 y de su interpretación jurisprudencial. Con el fin de alcanzar un pro-

moción volcada desde el sistema central. Sobre el objeto principal de estudio en este trabajo, podemos subrayar que el artículo 588 *bis k* del proyecto de Ley orgánica determina que una vez que se ponga término al procedimiento mediante resolución firme se ordenará el borrado y eliminación de los registros que consten en los sistemas electrónicos e informáticos si bien se conservará una copia bajo custodia del secretario judicial durante cinco años computables desde que la pena se hubiera ejecutado o desde que el delito o la pena hubieran prescrito. De manera específica, el artículo 588 *ter j* se refiere a las informaciones obrantes en archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, que podrán ser cedidos e incorporados al proceso previa autorización judicial siempre que la naturaleza de los mismos precise que deban ser conocidos y existan razones que justifiquen su cesión.

²⁷ Cfr. MAYER-SCHÖNBERGER, V.: *Delete: The virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton and Oxford, Princeton, 2011, p. 20.

²⁸ El potencial empleo de este tipo de información para elaborar grandes bases de datos, no es un tema reciente, sino que ya había sido avanzado en la década de los setenta por algún autor, es el caso de MILLER, A.: *The Assault on Privacy: Computers, Data Banks and Dossiers*, Ann Arbor, University of Michigan Press, 1971.

tección más eficaz de los derechos de los internautas, la Agencia Española de Protección de Datos Personales (AEPD) —como autoridad administrativa reguladora de la autodeterminación informativa ante el abuso de la informática— ha potenciado en los últimos años un nuevo mecanismo de protección jurídica, el derecho al olvido.

La AEPD ha sido clara en este sentido pues ha señalado que los ciudadanos pueden ejercer un derecho de oposición frente al tratamiento de datos personales en Internet por parte de los buscadores *web*, así como su cancelación y la adopción medios que eviten que la información reaparezca en el futuro o pueda ser indexada por los motores de búsqueda²⁹. De manera que la AEPD interpreta que el derecho al olvido se integra dentro del Derecho fundamental a la protección de datos³⁰ al entender que nos encontramos ante elementos que identifican a personas físicas y cuyo tratamiento automatizado permite su recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación conforme a los artículos 3.a) y 3.c) de la Ley orgánica de protección de datos y 5.1.f) de su

²⁹ Cfr. Entre otras, las resoluciones de la Agencia de Protección de Datos Personales TD/00463/2007, TD/01424/2012, TD/01753/2012, TD/01569/2013, TD/01544/2013 o TD/01270/2013 en las la AEPD no sólo advierte la necesidad de que cese de forma definitiva el tratamiento de los datos en la página *web* si no que también entiende que debe adoptarse medidas alternativas que lo aseguren. El empleo del protocolo denominado «robots.txt» como método válidos para el borrado de informaciones o el hecho de que los propios medios de comunicación, por falta de interés legítimo, eviten en su *webmaster* la indexación de la noticia por los motores de búsqueda en Internet permiten un adecuado ejercicio de los derechos de cancelación y oposición de los ciudadanos conforme el actual estado de la tecnología.

³⁰ La importancia de la acción de la Agencia de Protección de Datos española como precursora de la interpretación que actualmente realiza el Tribunal de Justicia de la Unión Europea debe ser destacada. La Agencia española sigue las interpretaciones realizadas por sus homólogas francesa e italiana. Así, para la *Commission nationale de l'informatique et des libertés* los datos personales tratados deben ser exactos, actualizados y procesados limpiamente y legalmente y recogidos para objetivos especificados, explícitos y legítimos. Mientras que, la *Garante per la Protezione dei Dati Personali* va un paso más allá al entender que el derecho al olvido implica el derecho de cancelar los datos personales cuando no fuesen útiles para el objetivo para los que habían sido procesados. Ahora bien, la acción de la Agencia española extiende los contornos que delimitan la defensa de este derecho al ser la primera en definir el derecho al olvido. En concreto, las resoluciones de la Agencia de Protección de Datos Personales TD/01335/2008 y específicamente TD/01164/2008 y TD/00627/2009 determinan que nos encontramos ante un derecho reconocido a todo ciudadano de reaccionar y corregir una inclusión ilegal de sus datos en Internet cuando el sujeto no tiene el estatus de personaje público ni se trata de un tema o noticia de relevancia de dicha índole (cfr. SIMÓN CASTELLANO, P.: «A test for Data Protection rights effectiveness: charting the future of the 'Right to be forgotten' under European Law», en *The Columbia Journal Law online*, The European Legal Studies Center, Columbia Law School, Invierno, 2013. <http://www.cjel.net/wp-content/uploads/.../Castellano-edited-and-rev.pdf>)

correspondiente Reglamento de desarrollo. La extensa interpretación efectuada sobre estos artículos³¹, como veremos, permite incluir de manera limitada en nuestro ordenamiento jurídico la protección del derecho al olvido frente a la actividad de los motores de búsqueda *web*.

Una identificación del derecho al olvido con la cancelación de datos que no está exenta de algunos problemas, lo que supondría un cambio de doctrina de la Agencia de Protección de Datos. En sus primeras resoluciones datadas en el 2007 la AEPD no había apreciado la responsabilidad del servidor, sin embargo, dos años más tarde, observaría con claridad la existencia de esa obligación de borrado por parte del buscador *web*. Ahora bien, el importante incremento de demandas presentadas por los ciudadanos ante la AEPD supuso la necesidad de introducir algunos filtros. Así, a partir del año 2010 comienza a requerirse el cumplimiento de ciertos requisitos por los recurrentes para poder admitir su recurso³². Esto no impidió que recientemente se hayan abierto numerosos procedimientos contra *Google Spain SL* con el fin de que eliminase datos correspondientes a los reclamantes. Un pronunciamiento de la AEPD sobre la posible responsabilidad de *Google* que fue objeto de recurso por la compañía ante la Audiencia Nacional y que motivó, finalmente, el pronunciamiento del Tribunal

³¹ La inclusión del derecho al olvido dentro de la protección constitucional a los datos personales efectuada por la AEPD se sustenta en una amplia interpretación de los conceptos tanto de los datos personales, que engloba a toda información identificable de personas físicas, como de su tratamiento —al entender que se trata de cualquier operación o procedimiento técnico automatizado o no, que permita su recogida, grabación, elaboración, conservación, modificación, bloqueo, cancelación— (cfr. SIMÓN CASTELLANO, P.: *El régimen constitucional del derecho al olvido digital*, colección monografías, n.º 815, Tirant lo Blanch, Valencia, 2012, pp. 139-140).

³² Así, debe subrayarse que la AEPD en sus resoluciones del 2007 dio prioridad al derecho a la información en el caso de noticias antiguas publicadas en páginas *web* sin que constituyesen datos personales ni que se responsabilizase a los buscadores al entender que simplemente cumplían una labor de intermediación —sirvan de ejemplo los procedimientos TD/00463/2007, TD00266/2007 ó TD/00299/2007—. Dos años más tarde la interpretación de AEPD cambió radicalmente al apreciar la existencia de responsabilidad en los buscadores por los datos que éstos tratan por lo que deberían evitar la recuperación de las informaciones desactualizadas volcadas en las hemerotecas de los periódicos —es el caso del procedimiento TD/01654—. La doctrina específica asentada por la AEPD en estos supuestos es comentada por COTINO HUESO (cfr. COTINO HUESO, L.: «Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público» en VV. AA. *Comentario a la ley orgánica de protección de datos de carácter personal*, TRONCOSO REIGADA, A. (dir.), Civitas Thomson Reuters, Madrid, 2010, pp. 317-319). Sobre la importancia de la labor realizada por la AEPD al respecto, también puede consultarse ORZA LINARES, RAMÓN M.: «Derecho al olvido en Internet: algunos intentos para su regulación legal», en VV. AA. *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Cuadernos y Debates n.º 215, Centro de Estudios Político Constitucionales, Madrid, 2013, pp. 480-483.

de Justicia de las Comunidades Europeas a favor del reconocimiento del derecho al olvido que, por su importancia, analizaremos más adelante.

La Agencia Española de Protección de Datos entiende que el derecho al olvido digital se sustenta sobre dos principios recogidos en la Ley orgánica de protección de Datos. Por un lado, el artículo 6 de la LOPD, que traspone el artículo 7.a) de la Directiva 95/46/CE, regula el principio de consentimiento inequívoco del afectado y la existencia de un interés público actual como requisitos necesarios para el tratamiento de los datos. Por otro lado, el artículo 4.5 de la LOPD establece el principio de finalidad como límite a la conservación de los datos registrados o recabados. Ahora bien, la acción de estos principios puede verse acotada y su fundamentación es diferenciada respecto al derecho de olvido digital. Así, el consentimiento del afectado no va a ser obligado en el caso de que los datos personales aparezcan contenidos en una fuente de acceso público —como son diarios y boletines oficiales, como reza el artículo 11.2.b) de la LOPD— y, al encontrarnos ante un concepto jurídico indeterminado, su tratamiento conforme a la existencia de un interés legítimo requiere ser valorado de forma individualizada. En todo caso, los demás derechos y libertades del afectado deberán ser respetados. De manera específica, la Sentencia del Tribunal Supremo de 8 de febrero de 2012³³ concreta todavía más la interpretación de este principio al subrayar la necesidad de que se demuestre por parte del responsable del tratamiento de datos que concurre el interés legítimo y su prevalencia sobre otros derechos e intereses existentes para que prime sobre el consentimiento inequívoco del sujeto afectado. Por este motivo, puede afirmarse que el principio del consentimiento en sí mismo no sustenta al derecho al olvido digital.

En cambio, el artículo 4.5 de la LOPD determina la obligada cancelación de los datos si estos dejan de ser necesarios o pertinentes para el fin por el que hubieran sido recabados o registrados. Es decir, el principio de finalidad *per se* permite la supresión de aquellas informaciones personales pasadas sometidas a un tratamiento automatizado que dejan de ser indispensables para el objeto por las que fueron obtenidas. La AEPD considera que en estos supuestos los afectados

³³ Dada la imposibilidad competencial del Tribunal Supremo para derogar un Ley orgánica, cabe destacar la importancia de la Sentencia del Tribunal Supremo de 8 de febrero de 2012 porque plantea una cierta paradoja normativa al declarar nulo el artículo 10.2.b) del Reglamento de desarrollo de la Ley orgánica de protección de datos por entenderlo contrario al artículo 7.f) de la Directiva 95/46/C. La Directiva europea simplemente contemplaba la necesaria satisfacción del interés legítimo con independencia de la fuente accesible o no al público en la que figuren los datos personales mientras que el Reglamento de desarrollo de la Ley orgánica de protección de datos exigía que los datos figurasen en fuentes accesibles al público, un requisito no previsto en la normativa europea pero sí añadido por el artículo 6.2 de la LOPD.

tienen razones legítimas para oponerse al tratamiento efectuado sobre sus datos personales por los motores de búsqueda *web*, incluso en aquellos casos en dichas informaciones que apareciesen recogidas en noticias carentes de relevancia pública actual y fuesen objeto de un tratamiento en hemerotecas digitales³⁴. De este modo, la AEPD, siguiendo los pasos de sus homólogas italiana y francesa, reconoce la existencia de un derecho al olvido digital en el marco del principio de finalidad que inspira la protección de datos.

El olvido digital se entiende como un derecho a controlar los datos personales propios que permitan el desarrollo del proyecto vital, amparándose en la dignidad humana, y que encuentra su fundamento en el derecho a la autodeterminación informativa, cuyo bien jurídico protegido sería más amplio que el bien jurídico protegido por el derecho a la protección de datos³⁵. Como destaca la AEPD, los ciudadanos podrán ampararse en la legislación de protección de datos para oponerse y cancelar aquellos datos personales pasados que no respondan a un interés público y cuyo tratamiento pueda suponer una violación de la legislación de protección de datos. Un posición que, además, resulta compatible con el principio de proporcionalidad preventivo aplicable por los gestores de las hemerotecas particulares y los buscadores. En el caso de los primeros señalados, esto se produce al tener que valorar la necesidad de incluir el dato personal en el medio de comunicación y, en el segundo de los supuestos, al verse obligados a configurar sistemas que reduzcan la visibilidad de la información y su indexación a lo necesario y al establecer mecanismos automáticos de anonimización aplicables a los datos desactualizados³⁶.

A pesar de todo lo expuesto, la AEPD como órgano de garantía no jurisdiccional ofrece a los usuarios de la red una protección jurídica limitada que debe completarse no sólo con lo previsto en la legislación y por la interpretación de la misma realizada por los órganos jurisdiccionales españoles, como hemos destacado, sino por la generada en el marco de la Unión Europea. Al ser la red un ámbito abierto necesitado de una regulación jurídica común que asegure la intimidad de los ciudadanos y que desconoce de fronteras estatales, un estudio completo de su problemática jurídica real nos obliga a considerar el marco nor-

³⁴ Cfr. Las resoluciones de la Agencia de Protección de Datos Personales TD/01164/2008, TD/01540/2008, TD/00627/2009 o TD/01887/2009, entre otras.

³⁵ Cfr. SIMÓN CASTELLANO, P.: *El régimen constitucional del derecho al olvido digital*, colección monografías, n.º 815, Tirant lo Blanch, Valencia, 2012, pp. 151-152.

³⁶ Cfr. COTINO HUESO, L.: «Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público» en VV. AA. *Comentario a la ley orgánica de protección de datos de carácter personal*, TRONCOSO REIGADA, A. (dir.), Civitas Thomson Reuters, Madrid, 2010, p. 321.

mativo europeo existente. Un nuevo contexto jurídico que se caracteriza por su evolución en los últimos treinta años y su reciente revisión tras la Sentencia emitida por el Tribunal de Justicia de la Unión Europea el 13 de mayo de 2014.

La extraordinaria importancia que ha tenido el pronunciamiento judicial señalado en la definición de los perfiles jurídicos de la protección de la intimidad de los internautas nos obliga a considerar los principales términos de dicha resolución para comprender la reconfiguración jurídica que, en la actualidad, experimenta el derecho al olvido en el ordenamiento español.

III. IMPORTANCIA DE LA SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA DE 13 DE MAYO DE 2014

El Tribunal de Justicia de la Unión Europea ha jugado un papel decisivo a la hora de fijar los parámetros que conforman el derecho a la protección de datos. Su Sentencia de 13 de mayo supone una nueva redefinición de este derecho. Una vez más este Tribunal adquiere un relevante protagonismo en el tema objeto de estudio que exige una reflexión específica.

Con carácter previo, este órgano judicial había vinculado estrechamente la protección de datos con el respeto de la vida privada y familiar establecido en el artículo 7 de la Carta de los Derechos fundamentales de la Unión Europea, y lo integra dentro del derecho a la intimidad, tal y como reconocía el apartado primero del artículo 1 de la Directiva 95/46/CE. Ahora bien, no es un derecho absoluto. El Tribunal Europeo admite la posibilidad de que se puedan introducir limitaciones a su ejercicio siempre que estén determinadas por la ley, no vulneren su contenido esencial, respeten el principio de proporcionalidad, sean necesarias y respondan a un interés general reconocido por la Unión Europea o a la necesidad de proteger los derechos y las libertades de los demás³⁷.

Sobre el tratamiento de datos personales y con arreglo al artículo 13 de la Directiva 95/46/CE, este tribunal de justicia establece que todo tratamiento de datos personales debe ser conforme no sólo con los principios relativos a la calidad de datos —enunciados en el artículo 6 de la norma señalada— si no también atender a los principios que determinan la legitimación del tratamiento de datos³⁸ —principios que se recogen en el artículo 7 de la misma—. Además,

³⁷ Véase al respecto la doctrina asentada por el Tribunal de Justicia de la Unión Europea en la sentencias de 9 de noviembre de 2010 en los asuntos acumulados C-92/09 y C93/09 —casos *Volmer und Markus Schecke y Eifer*.

³⁸ Cfr. La STJUE de 20 de mayo de 2003, asunto C-465/00 —caso *Rechnungshof*— en la que también se establece que las disposiciones de la Directiva 95/46/CE, al regular el tratamiento de

el TJUE amplía los supuestos aplicables. Este órgano judicial entiende que la protección de datos relativos a personas físicas regulada en la Directiva 95/46/CE —conforme al artículo 8 del Convenio Europeo de Derechos Humanos— también es extensible a los datos referentes a ciertas categorías de personas, como son los empresarios individuales —ya que en sus relaciones profesionales pueden acceder a informaciones personales del trabajador sin llegar a menoscabar su intimidad personal.

De manera específica, sobre la publicación de datos personales en Internet y el concepto de transferencia de esa información a terceros países, el Tribunal de Justicia de la Unión Europea³⁹ señala que la Directiva 95/46/CE fija unos principios esenciales relativos a la calidad del tratamiento de datos personales —en el sentido de que sean sólo datos adecuados, pertinentes y no excesivos en rela-

datos personales que pueden atentar contra las libertades fundamentales, deben ser interpretadas a la luz de los derechos fundamentales que forman parte de los principios generales del Derecho cuyo respeto garantiza este Tribunal. Partiendo de la jurisprudencia asentada por el Tribunal Europeo de Derechos Humanos, en esta Sentencia el TJUE expone los criterios fundamentales de interpretación del artículo 8.2 del Convenio Europeo de Derechos Humanos a los casos de comunicación de datos sobre determinados ingresos de funcionarios a terceros y la difusión pública del dato personal del salario. Así pues, el Tribunal de Justicia de la Unión Europea delimita el objetivo perseguido —mantener ciertos salarios dentro de unos límites razonables para garantizar una utilización óptima de los fondos públicos— y el aspecto más problemático de la medida adoptada —la amplia divulgación de los datos personales—. Ahora bien el Tribunal reserva a la jurisdicción nacional la valoración particularizada en cada caso de si la normativa austriaca atiende plenamente a dichas exigencias (cfr. MIGUEL ASENSIO, P. A. de: «La protección de datos personales a la luz de la reciente jurisprudencia del TJCE», *Revista de la Facultad de Derecho de la Universidad de Granada*, 3ª época, nº 7, Granada, 2004, pp. 402-403).

³⁹ Cfr. La STJUE de 6 de noviembre de 2003, asunto C-101/01 —caso *Göta hovrätt contra Bodil Lindqvist*—. En esta Sentencia el TJUE define con claridad los criterios aplicables a una página *web*, al entender que el concepto de tratamiento de datos del artículo 1 de la Directiva 95/46/CE comprende tanto la comunicación por transmisión como la difusión o cualquier otra operación que facilite el acceso a los datos personales. Además, esta Sentencia señala que el conflicto entre el derecho a la protección de datos personales y la libertad de expresión o el derecho de información ha de ser resuelto por la autoridad o juez nacional competente. Esto en la práctica supondría la posible existencia de algunas divergencias en la interpretación del alcance de los derechos fundamentales afectados lo que redundaría en una limitación de la uniformización jurídica comunitaria (cfr. MIGUEL ASENSIO, p. A. de: «La protección de datos personales a la luz de la reciente jurisprudencia del TJCE», *Revista de la Facultad de Derecho de la Universidad de Granada*, 3ª época, nº 7, Granada, 2004, p. 410). Sobre la importancia de esta Sentencia en el ámbito de la protección de datos y las obligaciones para los medios de comunicación puede consultarse RALLO LOMBARTE, A. y MARTÍNEZ MARTÍNEZ, R.: «Protección de datos personales y redes sociales: obligaciones para los medios de comunicación», *Quaderns del Consell de l'Audivisual de Catalunya, Internet a la deriva?*, nº 37, vol XIV (2), diciembre, Generalitat de Catalunya, Barcelona, 2011, pp. 42-43 (<http://www.cac.cat.es>).

ción con las finalidades que pretenden—. El TJUE subraya que estos principios son directamente aplicables, es decir, pueden ser invocados por los particulares ante los órganos jurisdiccionales nacionales con el fin de que el régimen de protección de datos sea equivalente en todos los Estados miembro. De este modo, se evita el restringir ciertas transferencias internacionales de datos⁴⁰.

Ahora bien, el carácter uniformizador normativo alcanzado por la Directiva 95/46/CE y precisado jurisprudencialmente por el Tribunal Europeo en los términos comentados, sin embargo, se manifiesta como un medio jurídico insuficiente ante el desarrollo de nuevas plataformas tecnológicas que manejan un gran volumen de datos personales. Resulta evidente la necesidad de una ulterior reformulación jurídica. El pasado año el Tribunal de Justicia de la Unión Europea ha dado el primer paso en este sentido.

A partir de la recopilación de la dispersa doctrina jurídica europea sobre el tema⁴¹, la Sentencia del TJUE 13 de mayo de 2014 responde a una cuestión prejudicial presentada por la Audiencia nacional española⁴² que pretende corregir la imprecisión jurídica del concepto de derecho al olvido a la espera de una reformulación jurídica específica⁴³. Con el fin de actualizar la regulación normativa en aras de una mejor defensa de los derechos de los ciudadanos, esta Senten-

⁴⁰ En este sentido, se ha subrayado que la Directiva 95/46/CE supone un ejemplo de progreso en la uniformización jurídica, dado que sus normas han tenido un destacable impacto en las legislaciones nacionales sobre todo en este ámbito de transferencia de datos a terceros estados dentro del marco de la libre circulación de datos personales. (Cfr. MIGUEL ASENSIO, P. A. de: «La protección de datos personales a la luz de la reciente jurisprudencia del TJCE», *Revista de la Facultad de Derecho de la Universidad de Granada*, 3^a época, n.º 7, Granada, 2004, pp. 408-409).

⁴¹ Cfr. Entre otras normas, la Directiva 95/46/CE sobre protección de datos —que sirve de parámetro jurídico para valorar la Sentencia comentada—; la Directiva 2002/58/CE sobre la privacidad; la Directiva 2006/24/CE sobre la conservación de datos, el Dictamen 1/2008 de 4 de abril sobre cuestiones relativas a la protección de datos relacionadas con motores de búsqueda emitido por el GT29 —en el que ya se consideraba a las búsquedas personalizadas a través de la lectura de las *cookies* del ordenador como tratamiento de datos—.

⁴² En los últimos años, hasta la Audiencia Nacional española han llegado unos doscientos casos que presentan como elementos comunes el hecho de que se trataba de datos publicados en el Boletín Oficial del Estado, posteriormente recogidos de forma lícita en un periódico pero cuya información había sido desnaturalizada en la red por falta de actualización o descontextualización. Por este motivo, con el fin de darle una respuesta jurídica adecuada, la Audiencia Nacional en un Auto de 27 de febrero de 2012 presentó una cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea en la que se planteó como cuestiones esenciales: la definición de la normativa aplicable en la garantía de estos derechos, las competencias de las autoridades de protección de datos, la responsabilidad de los buscadores y titulares de las páginas *web* y la posibilidad de evitar registros de la información personal.

⁴³ Con carácter previo, el 26 de febrero 2013 el Tribunal de Justicia de la Unión Europea celebró una audiencia pública para conocer las posturas de *Google*, España y otros Estados miembro

cia ha ido un poco más allá. Esta resolución judicial materializa el posible ejercicio del derecho de oposición ante un operador que realiza un tratamiento de datos. Bajo la premisa de que este derecho sólo sería aplicable *ad casum*, el Tribunal de Justicia trata de dilucidar varios términos de gran relevancia jurídica que requerían de una precisión inmediata:

- a) En primer lugar, este órgano judicial se pronuncia sobre la posibilidad de aplicar territorialmente la Directiva 95/46/CE a *Google* cuyo domicilio empresarial se localiza fuera de la Unión Europea.
- b) En segundo lugar, la Sentencia intenta definir si los buscadores *web* a través de las «arañas de búsqueda» toman como recurso a medio término los datos disponibles por los servidores, es decir, se plantea la posible aplicación del artículo 8 del Convenio Europeo de Derechos Humanos que asienta el marco jurídico sobre la protección de datos.
- c) En tercer lugar, se busca identificar si la actividad realizada por los buscadores puede ser incluida dentro del concepto de tratamiento de datos, de manera que la Agencia Española de Protección de Datos puede controlar, actuar y responsabilizar a los mismos sobre la información y el contenido disponible en su *web*.
- d) Finalmente, en último caso, la resolución judicial pretende establecer cuáles son los derechos de los ciudadanos y cómo pueden llegar a ejercitarse.

Debemos comentar que la Sentencia *Google Inc v. Agencia Española de Protección de Datos* resuelve afirmativamente la cuestión relativa a la aplicación territorial. El TJCE determina que el artículo 4.1.b) de la Directiva 95/46/CE despliega sus efectos sobre la filial *Google Spain* al ser un establecimiento permanente ubicado en la Unión Europea y vinculado con el buscador *Google* al que permite personalizar la publicidad que ofrece. Sobre el ámbito material de aplicación de la Directiva, subrayaremos que el Tribunal distingue entre el trato entre editar —que implica la mera inclusión de información en la página *web*— de la actividad del buscador —que almacena, trata, organiza, muestra y facilita el acceso a los datos—. A partir de ahí, el TJUE señala que la actividad de motor de búsqueda debe calificarse como de tratamiento de datos personales en el sentido que es descrito en el artículo 2.b) de la Directiva 95/46/CE. Esta actividad del buscador permite crear un perfil estructural de la persona con la mera introducción de su nombre y apellidos por lo que *Google* tiene que asumir ciertas respon-

sobre el derecho al olvido, con el fin de aclarar la normativa de protección de datos aplicable a buscadores de Internet.

sabilidades en base al artículo 12 de la norma señalada, un artículo que regula el derecho de oposición cuando los datos fuesen incompletos o inexactos. Además, el Tribunal entiende que el exigir un determinado hacer a los usuarios, si estos no quieren que un dato sea indexado, no constituye una garantía suficiente y establece la obligación de asegurar el borrado de datos en determinados supuestos. En este sentido, ha de subrayarse que, por primera vez, se define la necesidad de que los buscadores establezcan un procedimiento que atienda a los derechos de los ciudadanos y se fijan una serie de criterios que permiten ponderar si se cumplen esas garantías jurídicas. Por un lado, debe verificarse la naturaleza de la información si pública o privada, su idoneidad y actualidad así como el medio en el que se publica, en este caso el BOE. Por otro lado, el carácter de público o no del sujeto pasivo será otro elemento determinante a la hora de definir el interés que pueda suscitar la información difundida en la red.

Respecto a la conservación de los datos y al ejercicio de los derechos de acceso y oposición frente a la actividad del motor de búsqueda, a tenor de lo regulado en los artículos 6, 7, 12 y 14 de la Directiva europea destacada, el TJUE señala que los Estados miembros dispondrán que los datos personales sean conservados en una forma que permita su identificación por los interesados y durante un período de tiempo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. En todo caso, los responsables del tratamiento están encargados de garantizar estas previsiones así como de favorecer a la rectificación, supresión o el bloqueo de los datos que no se ajusten a las disposiciones de la Directiva 95/46/CE, más aún si son inexactos o incompletos. Además, los Estados miembros han de reconocer al interesado el derecho a oponerse, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernen sean objeto de tratamiento. Al ser una oposición justificada, el tratamiento efectuado por el responsable no puede referirse a esos datos. Ahora bien, como recuerda el TJUE, el artículo 12 deja la puerta abierta a alguna excepción ya que admite la posibilidad de que la legislación nacional disponga específicamente otra cosa.

La resolución judicial comentada concreta además cuales son los poderes que corresponden a la autoridad pública encargada de vigilar la aplicación de estas disposiciones. Así, conforme al artículo 28 de la Directiva 95/46/CE, el Tribunal reconoce a esta autoridad de control su capacidad de intervención a la hora de ordenar el bloqueo, la supresión, la destrucción de los datos o la prohibición provisional o definitiva de su tratamiento. Incluso, con el fin de garantizar la máxima protección de los derechos y libertades, se determina no sólo que esta autoridad pública deberá entender de las solicitudes presentadas por cualquier ciudadano o asociación que le represente si no también que sus decisiones pueden

ser objeto de recurso jurisdiccional si fuesen lesivas de derechos. Para completar su actuación y con el fin de cumplir sus funciones, en TJUE establece, además, un deber de cooperación entre las distintas autoridades de control, sobre todo en el ámbito del intercambio de información útil, y la posibilidad de que puedan ser instadas a ejercer sus poderes por autoridad externa correspondiente a otro Estado miembro.

En último término, de una forma clara el Tribunal de Justicia reconoce el derecho al olvido en el marco de los derechos contemplados en los artículos 12.b) y 14.1.a) de la Directiva 95/46/CE. En virtud de esta resolución judicial el gestor de un motor de búsqueda está obligado a suprimir de la lista de resultados aquellas informaciones indexadas a partir del nombre de la persona y vinculadas a páginas *webs* publicadas por terceros. Esa eliminación debe realizarse incluso a pesar de que ese nombre o esa información no se hubieran borrado previa o simultáneamente a la página *web* y aunque la publicación fuese lícita. El interesado tiene de este modo reconocido el derecho a que la información relativa a su persona ya no esté ligada a su nombre por una lista de resultados. Ahora bien, el TJUE precisa que la apreciación de ese derecho no presupone que la inclusión de sus datos en la lista de resultados cause un perjuicio para el mismo. En este sentido, en todo caso, el Tribunal aclara que el derecho del interesado a solicitar la no inclusión de sus datos en la lista de resultados disponible al público general prevalece no sólo sobre el interés económico del gestor del motor de búsqueda si no también sobre el interés general del público en acceder a esa información. Destacaremos que, sin embargo, la resolución judicial admite una vieja excepción a la protección absoluta de los datos: la injerencia en los derechos fundamentales señalados se entiende justificada por el interés general preponderante cuando se trata de un personaje público, una circunstancia que debe verificarse de manera concreta en los términos descritos en líneas anteriores.

De todo lo expuesto se deduce que el Tribunal de Justicia de la Unión Europea reconoce de forma limitada la existencia del derecho al olvido amparándose en su jurisprudencia anterior, la normativa europea y, sobre todo, en el trabajo procedente del GT29. Como resultado de su interpretación, la protección de la intimidad en la red está acotada materialmente por varias razones. Entre los principales rasgos que configuran el actual reconocimiento jurídico del derecho al olvido han de subrayarse los siguientes: su ámbito territorial sólo extensible al espacio europeo; su valoración *ad casum* que admite la existencia de excepciones a su reconocimiento y su aplicabilidad limitada al borrado de la indexación de datos en las páginas *web* de búsqueda pero no en la fuente originaria.

En definitiva, se observa que el empleo de recursos analógicos como respuesta jurídica ante los nuevos retos que plantea la difusión de datos en la *web* se caracteriza por ser restrictiva⁴⁴. Es decir, una vez más se plantea el inconveniente de ofrecer soluciones que estén a la altura de los nuevos problemas jurídicos emergentes en el ámbito digital lo cual requiere el desarrollo de normas específicas. La sociedad actual definida por el empleo de la información como fuente de poder a través de las nuevas tecnologías, especialmente de Internet como motor inmediato⁴⁵, exige el desarrollo de una regulación en la materia. La información presenta en este nuevo contexto en el que circula, el universo 3.0, una serie de particularidades como son su perennidad, su descontextualización, su desactualización y el problema de identificar el responsable de su difusión. Características que determinan la necesidad de una nueva normativa a la hora de configurar los perfiles que definen la intimidad de los sujetos en Internet⁴⁶. Un tratamiento jurídico que presenta ciertas peculiaridades, como veremos a continuación, y que ha de superar las deficiencias detectadas con el fin de que la dignidad personal pueda desarrollarse plenamente y con las garantías suficientes en la red.

IV. CONCLUSIONES: PECULIARIDADES DE LA REGULACIÓN EN VIGOR

El derecho a la protección de datos sitúa en una posición peculiar a los poderes del Estado ya que, por un lado, convierte a algunos de sus órganos en respon-

⁴⁴ Cfr. FERNÁNDEZ ESTEBAN, M^a L.: «Limitaciones constitucionales e inconstitucionales a la libertad de expresión en Internet», en *Revista Española de Derecho Constitucional*, n^o 53, mayo-agosto, Centro de Estudios Políticos Constitucionales, Madrid, 1998, pp. 283-311. (http://bibliotecadigital.inap.es/Datos/Publicaciones_Periodicas/REDC/53/REDC_053_281.pdf)

⁴⁵ BALLESTEROS MOFFA afirma que el aumento y socialización de la información como valor social, económico y jurídico, hizo evolucionar la forma de vida asentada en los bienes físicos y la energía, propios, de la era industrial, en una sociedad imbuida por el conocimiento y la información. La aspiración a constituir una aldea global se convierte en un claro desafío para los Estados. En esos términos, la potenciación del valor de la información y el presente orden cosmopolita sólo alcanza la intensidad que hoy tienen a partir de los espectaculares avances producidos en el ámbito de las comunicaciones electrónicas, especialmente Internet. Así, la indefensión de los ciudadanos frente a la utilización de sus datos personales se configura como una patología inmanente a la e-sociedad y que las nuevas tecnologías privan al tiempo y al espacio de su función protectora natural (cfr. BALLESTEROS MOFFA, L. Á.: *La privacidad en Internet. Internet en el centro de protección*, monografías n^o 413, Tirant lo Blanch, 2005, pp. 34-37, y 40-41).

⁴⁶ Cfr. MARTÍNEZ MARTÍNEZ, R.: *Una aproximación crítica a la autodeterminación informativa*, Estudios de protección de datos, Thomson Civitas, Madrid, 2004, pp. 51.

sables directos de los ficheros que almacenan⁴⁷ la información, y por otro lado, encomienda a un órgano *sui generis* la vigilancia y el control de la aplicación de las normas que lo regulan. Como responsable de un fichero, el poder público está obligado a respetar y a cumplir los principios de calidad y las medidas de seguridad⁴⁸ y a dar respuesta al ejercicio de los derechos de acceso, cancelación y oposición que se ejerciten ante él atendiendo el procedimiento establecido. Junto a esta protección ordinaria, la legislación española⁴⁹ prevé un mecanismo singular de tutela en el caso de que se produzca una actuación contraria a la LOPD o si se le negase al interesado los derechos de acceso, rectificación, cancelación y oposición. La Agencia Española de Protección de Datos Personales es la autoridad estatal de control independiente que se encarga de esta función en España, sus actuaciones también se despliegan en el caso de los buscadores de Internet. El reconocimiento del derecho al olvido como derecho personalísimo nace en Europa sobre todo a partir de las contribuciones de las diferentes agencias estatales de control sobre la materia. La fundamentación de este Derecho propuesta por la AEPD es la más ambiciosa de ellas al interpretar que el derecho al borrado de la información se sustenta tanto sobre el principio del consentimiento como sobre el principio de finalidad y que comprende tanto el derecho de cancelación como el de oposición⁵⁰.

La Sentencia *Google Inc v. Agencia Española de Protección de Datos* no crea un nuevo derecho si no que confirma las disposiciones normativas anteriores⁵¹. La principal novedad que introduce la resolución judicial comentada es el establecimiento de un medio jurídico específico para exigir su tutela ante el responsable

⁴⁷ Cfr. SERRANO PÉREZ, M^a M.: «Los derechos al honor, a la intimidad personal y familiar y la propia imagen. La inviolabilidad del domicilio y la protección de datos», en AA. VV. *Los derechos fundamentales. La vida, la igualdad y los derechos de libertad*, GARCÍA GUERRERO, J. L. (dir.), monografía n.º 35, Tirant lo Blanch, Valencia, 2013, pp. 491-492.

⁴⁸ Cfr. Los artículos del 79 al 114 del Reglamento de protección de datos, el Real Decreto-ley 1720/2007, de 21 de diciembre.

⁴⁹ Cfr. Los artículos 18 de la LOPD y 117, 118 y 119 de su Reglamento de desarrollo, el Real Decreto-ley 1720/2007, de 21 de diciembre.

⁵⁰ Sobre las distintas interpretaciones y dudas planteadas por otras agencias estatales europeas respecto a este derecho y la importancia de extensa interpretación de la AEPD sobre su tutela debe consultarse SIMÓN CASTELLANO, P.: *El régimen constitucional del derecho al olvido digital*, colección monografías, n.º 815, Tirant lo Blanch, Valencia, 2012, pp. 162 y ss.).

⁵¹ Hasta el punto de que llega a afirmarse por el Abogado General de la Unión Europea, que este derecho fundamental emerge como una mera reafirmación del acervo de la Unión Europea y del Consejo de Europa en la materia, que simplemente pone énfasis en la importancia de la protección de datos personales pero que no añadiría ningún novedoso elemento significativo a la interpretación de la Directiva 95/46/CE (cfr. <http://curia.europa.eu/juris/documents.jsf?num=C-131/12>)

del tratamiento de los datos en la *web*. A la espera de un Reglamento europeo⁵² que de manera específica se refiera a la supresión de datos, el Tribunal de Justicia de Unión Europea se ha visto en la necesidad de redefinir las características que identifican el ámbito jurídico relativo al derecho sobre la intimidad de usuarios de Internet. Éste es el primer asunto en el que se solicita al dicho Tribunal que interprete la Directiva de protección de datos en relación con los motores de búsqueda en Internet⁵³. La Sentencia 13 de mayo de 2014 entiende que el derecho al olvido presenta unos amplios contornos dentro de la protección de datos pero al mismo tiempo limita su contenido.

⁵² Así, la propuesta de la Comisión de Reglamento general de protección de datos presentado el 25 de enero de 2012 ya establece en su artículo 17 un derecho al olvido, en cuya formulación incluye no sólo la obligación del responsable del tratamiento que haya difundido los datos personales de informar a los terceros sobre la solicitud del interesado de suprimir todos los enlaces a los datos personales, copias o réplicas de los mismos, sino que también integra el derecho a que se restringiese el tratamiento en determinados casos, evitando así la ambigüedad del término «bloqueo» (cfr. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf). El 21 de octubre de 2013, la Comisión LIBE —Comité del Parlamento Europeo de Libertades Civiles, Justicia y Asuntos de Interior— logra un acuerdo sobre el texto que debería ser consensuado entre el Parlamento, el Consejo y la Comisión en el 2014, pero la problemática suscitada ante el bloqueo británico y la oposición alemana a dicha propuesta de Reglamento parece retrasar la aprobación de una normativa consensuada en este ámbito, actualmente en la fase de primera lectura del procedimiento legislativo ordinario. (Cfr. La Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la 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)0011 –C7-0025/2012– 2012/0011(COD), <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=ES&ring=A7-2013-0402>). Sobre los límites del derecho al olvido digital previstos en el artículo 17.3 de la propuesta de Reglamento debe señalarse, en especial, la falta de criterios de ponderación para dirimir el conflicto entre derecho al olvido digital y la libertad de expresión lo que conlleva a acudir una vez más al principio de proporcionalidad y los criterios tradicionales que permiten resolver los conflictos suscitados entre las libertades informativas y el derecho fundamental a la protección de datos (cfr. SIMÓN CASTELLANO, P.: «El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos», en VV. AA *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Cuadernos y Debates n° 215, Centro de Estudios Político Constitucionales, Madrid, 2013, pp. 456-459).

⁵³ Recordemos que, en esta Sentencia, el TJUE toma como punto de partida, principalmente, la Directiva 95/46/CE, a la vez que continúa la línea jurisprudencial que había iniciado en materia de protección de datos en Internet —definida por las sentencias como la *Lindqvist*, *Österreichischer Rundfunk*, *Satakunnan Markkina pörssi Oy* y *Satamedia Oy* y *Volker und Markus Schecke y Eifert*— y las consideraciones emitidas en los últimos años por el GT 29 a través de numerosos dictámenes —entre los que destacan el Dictamen 1/2008, el Dictamen 2/2010 y el Dictamen 4/2012.

En este contexto, el derecho al olvido emerge como una respuesta jurídica caracterizada por su relatividad⁵⁴, al ser sólo aplicable en el territorio europeo y no en todos los supuestos. En la resolución judicial destacada el Tribunal de Justicia no establece una censura respecto a la información personal disponible en red si no que respeta la prevalencia del *Habeas Data* frente el Derecho de información en determinados casos. Esto no implica que los datos deban ser suprimidos si no que lo que se ha de ser eliminado es la indexación del nombre de la persona, es decir, el enlace resultado de la búsqueda de la información. Por lo tanto, los problemas de la perennidad, descontextualización y desactualización de esos datos perviven. El acceso a la información siempre será posible por otras vías. Además, como se ha puesto de manifiesto en esta sentencia, al tratarse de un derecho sólo reconocido en Europa⁵⁵ nos hallamos ante un grave obstáculo que dificulta su protección e imposibilita su control dada la naturaleza global que caracteriza Internet. Es decir, nos encontramos ante un derecho personalísimo de alcance territorial limitado cuyo reconocimiento es diferenciado en tanto a los sujetos pasivos —sólo si se trata de cibernautas europeos— y activos —exigible a responsables del tratamiento de datos localizados en el territorio europeo.

En conclusión, el reconocimiento del derecho al olvido ha supuesto un relativo avance en la garantía de los derechos de los usuarios de Internet. Desde el punto de vista material, la información personal disponible en la *web* debe presentar los elementos señalados de licitud, pertinencia y actualización. En caso contrario, sólo es posible eliminar su indexación pero no borrar los datos de la fuente principal. Además de los condicionamientos subrayados que caracterizan este derecho, destaremos que han surgido nuevos problemas jurídicos específicos

⁵⁴ Como destaca SIMÓN CASTELLANO, el derecho al olvido se configura como un derecho relativo, no absoluto, a tenor de los límites jurídicos que hemos analizado y que se entienden previstos en la propuesta europea de Reglamento de protección de datos personales. Su fundamento jurídico es el derecho a la protección de datos motivo por el cual, junto a sus límites propios, estaría acotado por los correspondientes a la libertad de información, el deber de conservación de datos de interés histórico, estadístico o científico, o por las leyes que autorizan la conservación de los datos personales a pesar de la falta de consentimiento o la negativa explícita del titular de los datos (cfr. SIMÓN CASTELLANO, P.: «El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos» en VV. AA *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Cuadernos y Debates nº 215, Centro de Estudios Político Constitucionales, Madrid, 2013, pp. 456-465).

⁵⁵ Para hacer frente al problema del ámbito territorial de la aplicación de la Directiva 95/46/CE, el Grupo del artículo 29 propone en su Dictamen 8/2010 de 16 de diciembre que en la legislación futura sobre la protección de datos en el ámbito europeo tenga en cuenta la oportuna orientación hacia las personas en lo que se refiere a los responsables del tratamiento que no están establecidos en la Unión Europea (cfr. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf).

en nuestro ordenamiento jurídico a raíz de su actual reconocimiento jurisprudencial. La exigencia de su articulación *ad casum*⁵⁶ y a la configuración de nuevos mecanismos extrajurídicos por el responsable de la difusión en la *web* complican el procedimiento de garantía que articula la protección de datos en la red.

En concreto, la solución ideada por *Google* a raíz del reciente pronunciamiento judicial ha sido la de establecer un formulario a través del cual los internautas pueden solicitar el borrado de referencias a un Comité de Expertos⁵⁷. Una solución que resulta cuestionable por su restringido alcance. Por un lado, este mecanismo sólo es aplicable a ciudadanos de la Unión Europea —lo que plantea problemas desde el punto de vista del principio de igualdad—, sólo puede solicitarlo el afectado y requiere que se alegue una explicación de las causas que motivan su petición. Por otro lado, aun atendiendo a la demanda presentada por el internauta, el resultado de su petición se ciñe exclusivamente al borrado de los enlaces asociados que no resulten relevantes. Debemos añadir, que este medio

⁵⁶ En sentido contrario al que posteriormente se pronuncia el TJUE, el Abogado General de la Unión Europea, Nilo Jääskinen, en sus conclusiones en el asunto C-131/12 presentadas el 25 de junio de 2013 propone que no se considerase al proveedor de servicios «responsable del tratamiento» de tales datos personales, en el sentido del artículo 2, letra d), de la Directiva 95/46 —a excepción de los contenidos del índice de su motor de búsqueda, siempre que el proveedor del servicio no indexase o archivase datos personales en contra de las instrucciones o las peticiones del editor de la página *web*— y que los derechos de cancelación y bloqueo de datos y el derecho de oposición —establecidos en los artículos 12 y 14 de la Directiva 95/46 e interpretados a la luz del artículo 7 de la Carta de Derecho de la Unión Europea— no se extiendan a la creación de un nuevo derecho, el derecho al olvido. El Abogado General entiende que la Directiva 95/46/CE no establece un derecho general al olvido sobre intereses subjetivos si no que la finalidad del tratamiento y fines a los que sirve serían criterios a aplicar cuando se procesan datos sin el consentimiento del interesado. Y, finalmente, Nilo Jääskinen desaconseja al Tribunal de Justicia que estos intereses en conflicto pudiesen equilibrarse de modo satisfactorio en cada situación concreta sobre una base casuística, dejando la decisión en manos del proveedor de servicios de motor de búsqueda en Internet (cfr. <http://curia.europa.eu/juris/documents.jsf?num=C-131/12>). Sin embargo, el TJUE no atiende a esta última recomendación. Motivo por lo que se impone la necesidad de establecer unos estándares mínimos de garantías jurídicas en este ámbito. De lo contrario, puede producirse un menoscabo de los derechos de los ciudadanos ya que la ponderación de derechos se debe realizar caso a caso, con la consecuente falta de seguridad jurídica, y, a demás, los buscadores pueden aprovechar esa indeterminación para variar el tipo de información que publican sin atender a criterios uniformes.

⁵⁷ Actualmente este Comité de expertos está integrado por el expresidente de *Google*, el director de *Wikipedia*, el relator especial de la ONU para la Protección del Derecho a la Libertad de Expresión, tres profesores de las Universidades de Oxford, Lovaina y CEU San Pablo, y el antiguo director de la Agencia Española de Protección de Datos. Este Comité tiene como función principal la de la evaluación caso a caso cada una de las solicitudes presentadas, que, a fecha de 1 de septiembre de 2014, ascienden a ciento veinte mil y afectan a un total de cuatrocientas cincuenta y siete mil URL.

implantado para dar respuesta a la demanda ciudadana genera una grave de incertidumbre jurídica en el Derecho español pues el tiempo de respuesta del Comité de expertos con dificultad puede ajustarse al plazo de diez días que establece la Ley de protección de datos y su correspondiente Reglamento de desarrollo⁵⁸. De manera que, en todo caso, el interesado si entendiese que su solicitud no es atendida por *Google* puede dirigirse a la Agencia Española de Protección de Datos como último recurso.

Más allá de la discusión jurídica suscitada sobre el alcance del derecho a la intimidad en Internet, el derecho al olvido plantea de nuevo la urgente necesidad de encontrar un equilibrio entre los intereses públicos y privados en este campo así como la exigencia de fijar unas directrices que permitan actuar sobre este derecho⁵⁹ con carácter global y eficaz no sólo en el ámbito jurídico si no también cultural y social. El empleo de la propia tecnología digital puede limitar temporalmente las informaciones compartidas en la red⁶⁰ mas, con carácter previo, debe solucionarse una tarea pendiente tan esencial como es la formación de una conciencia social. Sólo mediante la denominada alfabetización del usuario⁶¹ o alfabetización digital⁶² podrá valorarse si el cibernautas presta o no su consentimiento o si decide revocarlo posteriormente a través de los instrumentos articulados por el legislador en el universo 3.0.

El ciudadano debe ser totalmente consciente de la importancia que tiene asegurar su intimidad personal también en la *web* y de la obligación de los poderes públicos en su eficiente protección. Hoy en día, una tutela jurídica global acorde con los tiempos que corren se impone así como imprescindible en la configuración de dignidad de los internautas ante el imparable avance tecnológico.

⁵⁸ Cfr. Los artículos 16 de la Ley orgánica 15/1999, de 13 de diciembre de protección de datos y los artículos 32.2 y 32.3 Real Decreto-ley 1720/2007, de 21 de diciembre.

⁵⁹ Con este fin, el 23 de julio de 2014, el GT29 se reúne en Bruselas con los principales buscadores *web* para obtener información completa del proceso que están llevando a cabo para aplicar la Sentencia comentada y, al mismo tiempo, para trasladarles las inquietudes que le suscita la adopción de determinadas medidas que no se adecuan a las exigencias del fallo.

⁶⁰ Cfr. MAYER-SCHÖNBERGER, V.: *Delete: The virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton and Oxford, Princeton, New Jersey, 2011, pp. 169 y ss.

⁶¹ Cfr. MARTÍNEZ PASTOR, E. y MUÑOZ SALDAÑA, M.: «En busca de equilibrio entre la regulación y la autorregulación de la publicidad comportamental en línea», *Estudios sobre el mensaje periodístico*, vol. 19, marzo, Universidad Complutense, Madrid, 2013, p. 295 (<http://revistas.ucm.es/index.php/ESMP/article/viewFile/42036/40017>).

⁶² Cfr. JARAMILLO, Ó.: «El futuro de la vida pública y privada en las redes sociales» en *VV. AA Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, Cuadernos y Debates n° 215, Centro de Estudios Político Constitucionales, Madrid, 2013, p. 413.

Title:

THE RIGHT TO BE FORGOTTEN IN SPANISH LAW DUE TO THE CJEU DOCTRINE

Summary:

I.—Data Protection in the Internet and its more important juridical problems. II.—The juridical frame of Data Protection in Spanish Law. III.—The magnitude of Sentence Google Spain SL, *Google Inc v. Agencia Española de Protección de Datos*. IV.—Conclusions: Legal peculiarities in present time.

Resumen:

En la sociedad de la información el control de los datos adquiere una gran relevancia en el ejercicio de poder. El derecho al olvido surge como una respuesta jurídica peculiar en el ámbito de Internet. Este trabajo pretende ofrecer un análisis de los perfiles que definen su actual configuración en el Derecho español a partir de la STJUE de 13 de abril de 2014 sin perder la perspectiva de su origen y los retos futuros que plantea. Así, el Tribunal de Justicia de la Unión Europea reconoce de forma limitada la existencia del derecho al olvido amparándose en la jurisprudencia anterior, la normativa europea y, sobre todo, en la actividad previa del GT29. Como resultado de su interpretación surgen nuevos problemas jurídicos en nuestro ordenamiento que requieren el desarrollo de normas específicas en la materia.

Abstract:

In the information society, Control of becomes increasingly more important in the exercise of power. The Right to be forgotten appears as a peculiar juridical answer in Internet context. This work tries to offer an analysis of the profiles that define its configuration in Spanish Law from the Court of Justice of European Union's Sentence of May 13th 2014 —*Google Inc v. Agencia Española de Protección de Datos*— without losing the perspective of its origin and the future challenges that it presents. This way, the Court of Justice of the European Union recognizes of limited form the existence of the Right to be forgotten seeking protection in the previous jurisprudence, in the European Law and, especially, in the job of the Data Protection Working Group (WP29). As result of its interpretation, new juridical problems come into Spanish Law that will have to need the development of specific rules.

Palabras clave:

Webs 3.0 «webs inteligentes»; Protección de Datos; Ley Orgánica 15/1999, de 13 de diciembre; Derecho al olvido; STJUE 13 de mayo de 2014.

Key Words:

3.0 Webs «intelligent webs»; Data Protection; Bill of Data Protection 15/1999; Right to be forgotten; Sentence of the Court of Justice of European Union of May 13th 2014.