

Neutralidad de la red y otros retos para el futuro de Internet

Actas del VII Congreso Internacional Internet,
Derecho y Política. Universitat Oberta de Catalunya,
Barcelona, 11-12 de julio de 2011

Net Neutrality and other challenges for the future of the Internet

*Proceedings of the 7th International Conference on Internet,
Law & Politics. Universitat Oberta de Catalunya,
Barcelona, 11-12 July, 2011*

2011

NEUTRALIDAD DE LA RED Y OTROS RETOS
PARA EL FUTURO DE INTERNET

*NET NEUTRALITY AND OTHER CHALLENGES
FOR THE FUTURE OF THE INTERNET*

© 2011, Los autores

© 2011, Huygens Editorial

La Costa, 44-46, át. 1ª

08023 Barcelona

www.huygens.es

ISBN: 978-84-694-7037-4

Impreso en España



Esta obra está bajo una llicència Attribution-
NonCommercial-NoDerivs 3.0 Unported de Creative Commons.

Para ver una copia de esta licencia, visite

<http://creativecommons.org/licenses/by-nc-nd/3.0/>.

EL DERECHO AL OLVIDO EN INTERNET

Ramón M. ORZA LINARES

Profesor Contratado Doctor de Derecho constitucional. Universidad de Granada

Susana RUIZ TARRÍAS

Profesora Contratada Doctora de Derecho constitucional. Universidad de Almería

ABSTRACT: El acelerado desarrollo de la sociedad de la información y la creciente complejidad técnica de las tecnologías asociadas a su desarrollo plantean nuevos retos en nuestras sociedades democráticas. Estos nuevos retos aparecen en dos líneas relativamente convergentes: por un lado, es necesario la redefinición de derechos tradicionalmente contruidos entre nosotros, sobre todo en lo que se refiere a los derechos relacionados con la libertad de expresión o el derecho a la información y su posibles conflictos con el derecho al honor, a la intimidad personal o a la propia imagen; y, por otro, como respuesta a nuevos peligros que amenacen la libertad de los ciudadanos, es necesario la creación de nuevos derechos que la sigan garantizando, como el derecho al olvido.

Este problema, ligado a la expansión de internet y, en especial de las redes sociales, por lo tanto, afecta, como mínimo, a las personas individuales citadas, a las empresas (por ejemplos, editoras de periódicos), instituciones o personas individuales que han generado la información y a los buscadores de internet que rastrean las páginas web y almacenan su contenido indexado, guardándolos en ocasiones durante un dilatado periodo de tiempo. Problema que existe incluso cuándo es el propio interesado el que suministra o publica información personal.

Finalmente, se reseñan los intentos de la Agencia Española de Protección de Datos para dar contenido a este derecho y las respuestas que se plantean en relación con el derecho al olvido desde la Unión Europea.

PALABRAS CLAVE: Internet, derecho al olvido, derechos fundamentales, datos personales, derecho a la información, buscadores, Directiva 95/46/CE, Unión Europea, Constitución, nuevas tecnologías, privacidad, TIC's.

1. INTRODUCCIÓN

Cuando hablamos del “derecho al olvido” es inevitable no recordar el siniestro Ministerio de la Verdad en el que trabajaba Winston Smith en la conocida novela de George Orwell¹.

Ante la persistencia del pasado, en el Departamento del Registro en el que trabajaba el protagonista, se buscaba minuciosamente toda huella documental anterior para que, al reescribirla, a través de delicadas tareas de falsificación, quedara debidamente alterado el presente.

1 ORWELL, G. (1949) 1984. 1ª edición 1952, Barcelona: Ed. Planeta.

En la era de Internet también nos preocupa la persistencia del pasado. Pero creemos que desde una perspectiva radicalmente diferente. Así, si en la novela de Orwell toda esa ingente tarea se ponía al servicio del Gran Hermano y de su poder, nuestra intención es precisamente establecer y consolidar mecanismos jurídicos que permitan seguir garantizando la libertad de los ciudadanos en una sociedad democrática.

De hecho, cuando una determinada información, que afecta a una persona concreta, es recogida en una página web, la información allí incluida puede ser replicada en otras páginas webs, en los índices de los buscadores e, incluso, en páginas web de repositorios que tienen como finalidad guardar lo que alguna vez se ha publicado en internet, aunque haya desaparecido la página web original².

Este es un problema que no sólo afecta a las personas individuales citadas, sino también a las empresas (por ejemplo, editoras de periódicos), instituciones o personas individuales que han generado la información y a los buscadores que rastrean las páginas web y almacenan su contenido indexado, guardándolo –y poniéndolo a disposición de todos– en ocasiones durante un dilatado periodo de tiempo.

Por poner un único ejemplo, muchos de los periódicos tradicionalmente editados en papel, y que ahora también están presentes en internet, han volcado sus hemerotecas históricas en la red, por lo que en este momento es perfectamente posible, con la ayuda de los buscadores, encontrar noticias que afectan a personas concretas, incluso de muchos años atrás. Con el inconveniente de que al ser estas noticias antiguas, no suelen estar actualizadas, por lo que pueden contener detalles o aspectos que se han quedado obsoletos o que, simplemente, eran erróneos e inexactos ya cuando se publicaron³. Pero, sin embargo, al ser recuperados por los buscadores, aparecen registrados de manera inmediata, poniéndolos de nuevo de actualidad.

Como en tantas otras ocasiones, este no es un problema que no haya sido abordado por las legislaciones con anterioridad. De hecho, en todos los países existen normas sobre la prescripción de los delitos, sobre la cancelación de antecedentes penales que constan en los Registros Públicos o sobre la cancelación de informaciones sobre aspectos económicos que pudieran afectar a las personas (quiebras, insolvencias, etc.). De hecho, es posible encontrar resoluciones jurisdiccionales en diversos países sobre el «derecho al olvido», sobre todo en lo atinente a cuestiones penales⁴.

2 Es el caso de la página <http://www.archive.org/index.php> que ha llegado a archivar billones de páginas webs que ya han dejado de estar operativas o <http://groups.google.com/> que almacena millones de mensajes expuestos en los grupos de noticias/discusión de Usenet [Consulta: 10 de mayo de 2011].

3 Piénsese por ejemplo, en la cantidad de informaciones que suelen recoger los diarios sobre detenciones de presuntos delincuentes que, años más tarde, tras los correspondientes procesos judiciales, pueden quedar exentos de toda responsabilidad penal. La noticia suele recoger el momento de la detención policial, pero es raro que se actualice años más tarde con el resultado de los procedimientos jurisdiccionales.

4 Cfr. PACE, A. (1998) «El derecho a la propia imagen en la sociedad de los *mass media*» *Revista Española de Derecho Constitucional*, núm. 52, pags. 33-52. En especial, la pág. 48 y la nota núm. 50. No

De hecho, en el contexto europeo ha sido creciente la preocupación por la protección de datos de las personas físicas en relación con los ficheros automatizados y la divulgación de estos datos a través de Internet. Y, aunque no ha existido hasta ahora una regulación específica para garantizar que las informaciones publicadas en internet puedan suponer perjuicios para la vida de las personas, es cierto que, en parte, se pueden aplicar a estas informaciones la regulación garantista presente en las legislaciones sobre protección de datos personales.

La base actual de la regulación de casi todas las legislaciones europeas la proporciona el contenido de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos⁵.

No obstante, el marco jurídico europeo ha resultado profundamente transformado más recientemente en relación con la protección de los derechos fundamentales con la entrada en vigor del Tratado de Lisboa⁶ y de la Carta de los Derechos Fundamentales de la Unión Europea⁷. Esta última, en su artículo 8 reconoce como derecho autónomo el derecho a la protección de datos de carácter personal, afirmando que “toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan” (apartado 1); que estos datos “se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley”, y que toda persona tiene derecho “a acceder a los datos recogidos que le conciernan y a obtener su rectificación” (apartado 2).

Pero este reconocimiento expreso en el ordenamiento originario europeo del derecho a la protección de datos como derecho fundamental no toma en cuenta la rapidez en la

obstante el autor se muestra bastante pesimista sobre la posibilidad de que un afectado pueda impedir que los medios de comunicación vuelvan a publicar noticias o informaciones de su vida pasada, si vuelve a ser relevante.

5 *Diario Oficial (en adelante, DOL)* n° L 281 de 23/11/1995 p. 0031 - 0050. El texto completo se puede consultar en <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML> [Consulta: 10 de mayo de 2011]

6 *Diario Oficial de la Unión Europea (en adelante, DOUE)* C 306, de 17 de diciembre de 2007. El texto completo del Tratado se puede consultar en <http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:es:HTML> [Consulta: 10 de mayo de 2011]. Concretamente, el artículo 16 del Tratado de Funcionamiento de la Unión Europea dispone que

“1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea”.

7 *DOUE* C 303, de 14 de Diciembre de 2007. El texto completo se puede consultar en <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:Es:PDF> [consulta: 10 de mayo de 2011]

evolución tecnológica y la globalización en la difusión y tratamiento de los datos de carácter personal, lo que ha llevado a la Comisión Europea a proponer la necesidad de hacer frente, en términos más específicos, a la resolución de retos no contemplados inicialmente en la Directiva 95/46/CE, planteando la posibilidad de una reforma de la misma.

En este contexto, las siguientes páginas se dedicarán a analizar el estado actual de la protección del derecho al olvido, dentro de la regulación general de la protección de datos, y las posibles líneas de evolución en esta materia.

2. EL DERECHO AL OLVIDO EN INTERNET

2.1. Antecedentes

Como antecedente más remoto, podemos encontrar que, ya en 1931, en la Corte de California se resolvió el caso denominado *Melvin v. Reid*. Se trataba de un asunto en el que la víctima, tras un pasado como prostituta y haber sido acusada de homicidio, había conseguido rehacer su vida, hasta que una película, realizada y exhibida por el demandado bajo el título «*The Red Kimono*» desveló su pasado, con su nombre real y le arruinó la vida. La Corte consideró que se había producido una lesión en su privacidad al traer de nuevo a la actualidad aspectos de la vida de la demandante que ya habían quedado olvidados⁸.

Más recientemente, una primera respuesta legal a esta persistencia de los datos, con la aparición de los primeros ordenadores, fue la regulación de los derechos de acceso, rectificación y cancelación de los datos personales que pudieran constar en las bases de datos públicas o privadas⁹.

De este modo el derecho al olvido podía hacerse coincidir simplemente con el derecho de cancelación de los datos¹⁰, no sin dificultades, especialmente en lo que se refería a determinadas bases de datos que recogían datos de solvencia de los ciudadanos. Y siempre teniendo en cuenta que las bases de datos oficiales (policía, hacienda, etc.) normalmente son excluidas de la regulación general y suelen presentar numerosas dificultades a la hora de cancelar o, simplemente, de rectificar los datos recogidos¹¹.

8 Cfr. CORRAL TALCIANI, H. (2000) «Configuración jurídica del derecho a la privacidad II: Concepto y delimitación». *Revista Chilena de Derecho*, vol. 27 núm. 2, págs. 331-355, en especial, la pág. 337.

9 Especialmente en lo que se refiere a las bases de datos de solvencia patrimonial, las primeras que fueron objeto de una regulación específica. Cfr., entre otros, FERRANDO VILLALBA, M^a L. (2000), *La información de las Entidades de Crédito. Estudio especial de los informes comerciales bancarios Valencia*, Ed. Tirant lo Blanch; DUBIÉ, P. (2003) «Protección de datos y derecho al olvido», *Derecho de los negocios*, Año nº 14, Nº 154-155, págs. 1-16

10 GARRIGA DOMÍNGUEZ, A. (2004) *Tratamiento de datos personales y derechos fundamentales*. Madrid, Dykinson, pág. 40

11 De hecho estas bases de datos están especialmente excluidas de la regulación general. Vid. el artículo 2 de la *Ley Orgánica 15/1999, de protección de datos de carácter personal, que excluye de la aplicación*

Pero, además, con el vertiginoso desarrollo de las nuevas tecnologías de la información y de la comunicación, estas garantías pueden que ya no sean ya plenamente eficaces. Por un lado nos encontramos con el problema de que los datos difundidos o publicados pudieran ser correctos, aunque antiguos, lo que impediría, en ocasiones, el ejercicio de los derechos de corrección o cancelación: es el caso de la mayoría de las noticias publicadas por los diarios. Por otro, también nos podemos encontrar con que las empresas o servidores de internet en los que están alojados estos datos no se encuentren en el país del afectado o cuyas leyes queramos aplicar, dificultando de manera extrema las posibilidades de hacer efectivos esos derechos.

2.2. La actividad de la Agencia Española de Protección de Datos en relación al derecho al olvido

Así, en España, la Agencia Española de Protección de Datos, en sus primeras Resoluciones sobre estas materias, de fecha 9 de julio de 2007 —reafirmada tras el recurso de reposición del recurrente, el día 10 de septiembre de 2007¹²— y de 26 de enero de 2009¹³, ha abordado

de esta ley a los ficheros sometidos a la normativa sobre protección de materias clasificadas, a los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada y, entre otros, a los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad. Y aunque el artículo 22.2 del mismo texto legal señala que: “2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad”, lo cierto es que para este tipo de ficheros, según el artículo 23: “Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando”.

Y por lo que se refiere a los datos recogidos en los ficheros de hacienda, el artículo 23.3 determina que “Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras”.

- 12 El texto de estas Resoluciones, se pueden consulta en las siguientes direcciones electrónicas: https://www.agpd.es/portalweb/resoluciones/tutela_derechos/tutela_derechos_2007/common/pdfs/TD-00299-2007_Resolucion-de-fecha-09-07-2007_Art-ii-culo-16-LOPD.pdf , y la reposición en: https://www.agpd.es/portalweb/resoluciones/recursos_reposicion/tr_sobre_tutela_de_derechos/common/pdfs/REPOSICION-TD-00299-2007_Resolucion-de-fecha-10-09-2007_Art-ii-culo-16-LOPD.pdf [Consulta: 10 de mayo de 2011]
- 13 Los hechos denunciados en esta ocasión se referían a la publicación en la página web del periódico El País, de una noticia ya publicada el 25 de junio de 1987. El texto de la resolución puede verse en: https://www.agpd.es/portalweb/resoluciones/tutela_derechos/tutela_derechos_2009/common/pdfs/TD-01164-2008_Resolucion-de-fecha-26-01-2009_Art-ii-culo-17-LOPD_Recurrida.pdf [Consulta: 10 de mayo de 2011]

la cuestión de las noticias antiguas publicadas en las páginas web de los diarios, con las siguientes características:

En ellas, con un razonamiento sustancialmente similar, por un lado, la Agencia considera que la publicación de informaciones relevantes y veraces entra dentro del ejercicio legítimo del derecho a la información y, por lo tanto, su publicación es correcta, quedando además el análisis de los posibles conflictos con otros derechos constitucionales (honor, intimidad o protección de la propia imagen), fuera de las competencias de la Agencia, remitiendo para su enjuiciamiento a los Tribunales ordinarios.

Y, por otro, por lo que se refiere a la publicación en internet de las noticias, a través de la puesta a disposición de los internautas el archivo o hemeroteca del periódico, la Agencia también considera que no constituye la publicación de dato personal alguno, ya que la hemeroteca no es una base de datos susceptible de tratamiento y, por lo tanto, su cancelación o modificación queda fuera del ámbito de aplicación de la legislación de protección de datos.

Además, por último, y en lo que respecta a la responsabilidad concreta del buscador Google (directamente denunciado también), como servicio de intermediación, la Agencia, en las Resoluciones del año 2007, considera que tampoco tienen responsabilidad por la publicación de esos datos ya que «los buscadores tipo «Google», «Yahoo», «MSN Search», «AOL Search», etc., realizan la localización de información en Internet, con base en unos criterios que le son señalados por el usuario, buscando ocurrencias en textos o documentos publicados en la red y ofreciendo enlaces a los mismos». Así, «la información no se encuentra ubicada en los servidores o máquinas de los prestadores de los servicios de búsqueda, sino en las máquinas hacia las cuales apuntan los enlaces que ofrecen los buscadores, por lo que, la cancelación de los datos, si procede, deberá ejercitarse ante los responsables de las máquinas que contienen la información». De tal modo que los prestadores de estos servicios, en tanto facilitan los denominados «servicios de intermediación de la Sociedad de la Información», no son responsables por la información a la que dirijan a los destinatarios de sus servicios¹⁴.

Sin embargo, en lo que respecta a este último aspecto, el criterio de la Agencia en relación a la responsabilidad de los buscadores, cambia radicalmente. un par de años más tarde. Así, ahora considera a éstos como responsables de los datos que tratan. Concretamente señala que «la libertad de información no impone que los datos personales del reclamante figuren en los índices que utiliza Google para facilitar al usuario el acceso a determinadas páginas, ni tampoco preceptúa que figuren en las páginas que Google conserva temporalmente en memoria «caché»», al no ser la de buscar contenidos en internet «una actividad amparada por la libertad de información, sin que exista, una disposición legal o constitucional en contra del ejercicio del derecho de oposición frente a Google». Concluyendo por tanto que Google, es responsable y, por lo tanto debe evitar que los datos personales del recurrente puedan recuperarse cuando se utilice el mencionado buscador¹⁵.

14 Resolución de fecha 10 de septiembre de 2009, ya citada.

15 Resolución de fecha 26 de enero de 2009, ya citada. No obstante, como la denuncia solo se plantea contra Google, se puede dar el paradójico resultado de que, al no modificarse la página origen de

En la Resolución de 26 de enero de 2009, la Agencia también realiza una serie de reflexiones sobre el hecho de que los periódicos vuelquen en la red su hemeroteca. Considera que «los medios de comunicación deberían valorar la necesidad de que su actuación se dirija a conciliar en mayor medida, el derecho a la libertad de información con la aplicación de los principios de protección de datos personales». De tal forma que debieran ponderar «escrupulosamente» la relevancia pública de la identidad de las personas afectadas por el hecho noticiable, «para, en el caso de que no aporte información adicional, evitar la identificación mediante la supresión del nombre e incluso, si fuera necesario, de las iniciales o cualquier referencia suplementaria de la que pueda deducirse la identificación, en el caso de que el entorno sea limitado». Y, además, teniendo en cuenta que el desarrollo de Internet y la implantación generalizada de motores de búsqueda «suponen una actualización y divulgación exponencial y permanente de la información en prensa así como de los datos personales incluidos en la misma como la identidad de las personas», los medios de comunicación debería reflexionar «sobre la trascendencia que tiene mantener de manera permanente una absoluta accesibilidad de los datos contenidos en noticias cuya relevancia informativa probablemente es inexistente en la actualidad», así como «tener en cuenta la trascendencia sobre la privacidad de las personas que puede derivar de ello»¹⁶.

Esta última línea de actuación, que pasa por obligar a los buscadores, o al menos a los buscadores que son denunciados, a evitar la publicación de datos personales de los ciudadanos, ha sido confirmada en numerosas Resoluciones de la Agencia¹⁷, incluso cuando esos datos provienen de fuentes oficiales¹⁸.

Esta línea de actuación de la Agencia Española de Protección de Datos le ha llevado hasta el momento a abrir cerca de un centenar de procedimientos contra el buscador “Go-

la información (la del periódico), éste buscador no refleje ese resultado en sus búsquedas, pero sí lo continúen haciendo otros como Yahoo, Msn, Ask o cualquier otro que no haya sido afectado por la decisión de la Agencia.

- 16 Y continúa señalando que «En este sentido los medios de comunicación debieran usar medidas informáticas para que, en el caso de que concurra interés legítimo de un particular y la relevancia del hecho haya dejado de existir, se evite desde su webmaster la indexación de la noticia por los motores de búsqueda en Internet. De esta forma, aún manteniéndola inalterable en su soporte —no se borraría de sus archivos ni de sus históricos— se evitará su divulgación indiscriminada, permanente y, en su caso, lesiva» (*Fundamento de Derecho Décimo*). Resolución de fecha 26 de enero de 2009, ya citada.
- 17 Entre otras, las Resoluciones de fecha 17 de julio de 2008, 31 de julio de 2008, 3 de septiembre de 2008, 4 de noviembre de 2008, 29 de diciembre de 2008. Asimismo también existen otras muchas resoluciones en las que obliga a páginas webs privadas que eliminen datos personales obtenidos sin consentimiento. Todas las resoluciones de la Agencia Española de Protección de Datos pueden consultarse en <https://www.agpd.es/portalweb/resoluciones/index-ides-idphp.php> [Consulta: 10 de mayo de 2011]
- 18 Resolución de 30 de noviembre de 2010, que se refería a datos que aparecían publicados en la página web del Boletín Oficial del Estado: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00754-2010_Resolucion-de-fecha-30-11-2010_Art-ii-culo-16-LOPD.pdf [Consulta: 10 de mayo de 2011].

ogle” en el que le insta a eliminar de sus resultados de búsquedas los datos correspondientes a los reclamantes¹⁹.

Sin embargo, “Google Spain S.L.” ha recurrido estas resoluciones ante la Audiencia Nacional por cuanto considera que la responsabilidad de mantener esos datos accesibles al público es de terceros ajenos. Así, en el curso del procedimiento ordinario 211/2009 que se sigue a su instancia contra la Agencia Española de Protección de Datos, se ha dictado una Providencia de fecha 22 de febrero de 2011 en el que la Sala de lo Contencioso Administrativo (Secc. 1) de la Audiencia Nacional acuerda el planteamiento de una cuestión prejudicial de interpretación ante el Tribunal de Justicia de la Unión Europea para que este Tribunal declare, entre otras cuestiones “Si la actividad de GOOGLE, como buscador de contenidos de terceras personas, puede considerarse un tratamiento de datos” y, por lo tanto, debe garantizar los derechos de cancelación y oposición, “Si la AEPD ... puede requerir a GOOGLE para que cancele o bloquee la información, aun cuando su mantenimiento en la página de origen sea lícita, pero el solicitante considere que su aparición en los resultados de búsqueda atenta a su privacidad, dignidad o al derecho al olvido “ y, en definitiva, “si la AEPD ... puede requerir directamente al buscador, sin dirigirse previa o simultáneamente al webmaster para exigir la retirada de la información”. En la actualidad este procedimiento todavía no ha concluido.

Pero también existen nuevas aplicaciones como «Street View», también de Google, que permite acceder a imágenes de las calles de las principales ciudades del mundo o «Google Health» que pretende elaborar un banco de datos sanitarios, que han alertado a los responsables de las Agencias de Protección de Datos²⁰. De hecho, la Agencia Española de Protección de Datos ha publicado en su página web que «ha obtenido garantías por parte de Google de que “Street View”... contará con un sistema que anonimizará los rostros y matrículas de vehículos para evitar que los ciudadanos puedan ser identificados»²¹.

2.3. Derecho al olvido y redes sociales

Otra perspectiva del problema del anonimato en la red lo presenta la participación en las redes sociales, tipo Facebook o Tuenti. En este último caso la diferencia más significativa consiste en que en estas redes sociales los que ponen a disposición de otros sus datos personales son los propios internautas. De este modo nos encontramos con un principio de

19 La última Resolución es de fecha 7 de abril de 2011. Cfr. http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-01239-2010_Resolucion-de-fecha-07-04-2011_Art-ii-culo-16-LOPD.pdf [Consulta: 10 de mayo de 2011]

20 En un grado más incipiente de desarrollo parece encontrarse otros servicios de geolocalización como los vinculados a determinados dispositivos móviles (Iphone, entre otros).

21 Agencia Española de Protección de Datos, Nota informativa. 21 de abril de 2008. Localización: https://www.agpd.es/portalweb/revista_prensa/revista_prensa/2008/notas_prensa/common/abril/210408_np_edpnp-google.pdf [Consulta: 10 de mayo de 2011]

consentimiento otorgado expresa o tácitamente por la misma persona a la que se refieren sus datos personales.

No obstante, se ha podido observar una utilización de esos datos mucho más intensa que la prevista inicialmente, que era la de relacionarse con otras personas en un ámbito más o menos cerrado. De tal modo que datos e información suministrada directa y personalmente por las personas interesadas en sus propias cuentas personales dentro de estas redes sociales, con una finalidad de que sólo fueran accesibles a un círculo reducido de sus conocidos, han sido finalmente accesibles a todo el mundo sin restricciones, con consecuencias diversas para sus propietarios, bien por propia torpeza del usuario a la hora de configurar la privacidad de sus datos, o bien por dificultades inherente a la dinámica de la propia página de internet utilizada. Así, se han referido casos de utilización de estos datos para seleccionar demandantes de empleo, para la divulgación de fotografías personales de personajes conocidos²², o incluso, para la comisión de determinados delitos.

Ello ha llevado a que los responsables de las agencias de protección de datos hayan hecho diversas recomendaciones a los propietarios de esas redes sociales para limitar el daño que pudiera causarse a los ciudadanos por la proliferación de sus datos personales en este tipo de redes. Así, por ejemplo, se ha recomendado que los responsables de estas páginas extremen el cuidado sobre el diseño de esas páginas, para garantizar al máximo la confidencialidad de los datos publicados, facilitar y divulgar entre los usuarios cuáles son los permisos de acceso a los mismos y su capacidad para modificarlos, sobre la posibilidad de que los usuarios puedan borrar con facilidad los datos o imágenes publicadas o, incluso, cancelar todo su perfil o su cuenta, que los motores de búsquedas no puedan acceder a los datos personales publicados, etc.

Llama la atención, además, algunas recomendaciones, como la efectuada por la Agencia Española de Protección de Datos en orden a «limitar la posibilidad de etiquetado de los usuarios dentro de la red, de tal forma que cualquier persona etiquetada con su nombre, reciba automáticamente una solicitud de aceptación o rechazo, impidiendo en este caso la publicación y tratamiento de datos no autorizados»²³. Tal etiquetado se realiza con gran asiduidad en relación a las fotografías subidas a las cuentas de los usuarios de las distintas redes sociales, de tal modo que, con gran facilidad, no sólo se puede acceder a los datos de personas concretas, sino también a su imagen, incluso sin su conocimiento o consentimiento²⁴.

22 Incluso con relevancia política, como fue el caso de la publicación de los datos y fotografías del futuro responsable del servicio secreto inglés. Más información en la página de la BBC (en línea): http://www.bbc.co.uk/mundo/ciencia_tecnologia/2009/07/090706_1328_mi6_facebook_sao.shtml [Consulta: 10 de mayo de 2011]

23 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2009) *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line*. Madrid, Instituto Nacional de Tecnologías de la Comunicación y la AEPD, pág. 149. Puede consultarse en la siguiente dirección: https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf [Consulta: 10 de mayo de 2011]

24 Hay que señalar que, aunque hay algunos intentos en este ámbito, los buscadores de internet todavía no pueden buscar directamente en las imágenes, sino que lo hacen en el texto asociado a las mismas.

Estas nuevas exigencias derivadas de la evolución de las tecnologías asociadas a la sociedad de la información, ha llevado necesariamente a la necesidad de reformar la regulación básica de estas materias que se contemplaba en la Directiva del año 1995.

3. LA POSIBLE REFORMA DE LA DIRECTIVA 95/46/CE DE 24 DE OCTUBRE DE 1995 Y SU REPERCUSIÓN EN RELACIÓN CON EL “DERECHO AL OLVIDO”

Como hemos señalado, la adopción de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de datos, supuso un importante paso adelante en cuanto a la normalización de la legislación europea en relación a la protección de datos²⁵, aun cuando mantuvo sustanciales diferencias respecto del Convenio 108 del Consejo de Europa²⁶. El objeto de la misma, según disponía su artículo 1 consistía en reconocer la obligación de los Estados miembros de “garantizar”, en primer término, la protección de las libertades y de los derechos fundamentales de las personas físicas y, en particular, el derecho a la intimidad en lo que respecta a los datos personales y, en segundo lugar, la libre circulación de los datos personales entre los Estados miembros.

El contenido de la Directiva 95/46/CE se ha complementado con la regulación establecida en el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la

Así el etiquetado, que puede incluso estar hecho por terceros, es un elemento imprescindible para localizar imágenes relacionadas o en las que aparecen personas concretas.

- 25 Entre los estudios relativos a esta Directiva, pueden citarse, sin pretensión de exhaustividad: ALONSO BLAS, D. (1996): “El futuro de la protección de datos a nivel europeo”, en DAVARA RODRIGUEZ, M.A. (Coord.) *“Encuentros sobre Informática y Derecho (1995-1996). Pamplona: Aranzadi*; BELLO JANEIRO, D. (2001): *“La protección de datos de carácter personal en el Derecho comunitario”, Anuario de la Facultad de Derecho de la Universidad de la Coruña*, nº 5; BRU CUADRADA, E. (2007): *“La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad”, Revista de Internet, Derecho y Política*, nº 5; GUERRERO PICÓ, M^a C. (2006): *“El impacto de internet en el derecho fundamental a la protección de datos de carácter personal”, Thomson-Civitas*; HEREDERO HIGUERAS, M. (1997): *“La Directiva comunitaria de protección de los datos de carácter personal (Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos)”*. Pamplona: Aranzadi; HERRÁN ORTIZ, A.I. (2001): *“La protección de datos de carácter personal en el marco de la Unión Europea”, en REDI*, nº 39; PRIETO GUTIÉRREZ, J.M^a. (1997): *“La Directiva 95/46/CE como criterio unificador”, Poder Judicial*, nº 48; SÁNCHEZ BRAVO, A. (1998): *“La protección del derecho a la libertad informática en la Unión Europea”*. Sevilla: Universidad de Sevilla; VIGURI PEREA, A. (1999): *“Intimidad versus informática (La protección de datos de carácter personal: perspectiva desde el derecho comparado)”*, *La Ley*, Tomo de Jurisprudencia 2/

- 26 Vid., al respecto la Memoria de la Agencia Española de Protección de Datos de 1995.

libre circulación de estos datos²⁷, con lo dispuesto en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas²⁸, y con la Decisión del Consejo Europeo nº 2008/977/JHA de 27 de noviembre de 2008, sobre la protección de los datos personales en el ámbito de la cooperación policial y judicial en materias penales²⁹.

Quince años después de la aprobación de la Directiva 95/46/CE, la Comisión Europea, a través de la Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones, titulada “Un enfoque global de la protección de los datos personales en la Unión Europea”³⁰, reconoce que si bien el objetivo al que respondía “sigue teniendo vigencia”, y los principios que consagra “siguen siendo válidos”, lo cierto es que la rápida evolución tecnológica y la globalización “han modificado profundamente nuestro medio y han lanzado nuevos retos” en materia de protección de datos personales.

Al mismo tiempo, “los métodos de recogida” de los datos personales son cada vez más complejos y se detectan con mayor dificultad, siendo utilizados tanto por organizaciones y/o empresas privadas como públicas.

Tales consideraciones plantean, a juicio de la Comisión, la cuestión acerca de si la legislación actual de la Unión Europea en materia de protección de datos personales permite hacer frente “plena y eficazmente” a estos nuevos retos.

Con objeto de responder a esta cuestión, la Comisión inició un estudio del marco jurídico actual a través de una Conferencia de alto nivel en mayo de 2009, seguida de una consulta pública hasta finales de ese mismo año. Por otro lado, a lo largo de 2010 tuvieron lugar consultas más específicas y la Vicepresidenta Viviane Reding presidió una reunión de alto nivel con las partes interesadas, celebrada en Bruselas el 5 de octubre de 2010, además de consultar al Grupo de Trabajo del Artículo 29³¹, tomando en consideración, así mismo,

27 DO L 8/1 de 12.1.2001.

28 DO L 201 de 31.7.2002, p. 37. Modificada por la Directiva 2009/136/CE (DO L 201 de 18.12.2009, p.11).

29 DO L 350/60 de 30.12.2008.

30 COM (2010) 609 final.

31 Dicha consulta concluyó con la elaboración del Documento sobre “El futuro de la privacidad” (WP 168) y el Dictamen 3/2010, sobre el principio de responsabilidad, de 13 de julio (00062/10/ES) GT 173.

En dicho Dictamen se plantea la necesidad de “progresar de la teoría a la práctica” en el ámbito de la protección de datos personales, sugiriendo a la Comisión la introducción del “principio de responsabilidad” en la posible revisión de la Directiva de protección de datos, lo que, a juicio del Grupo de Trabajo del Artículo 29, contribuiría a reforzar “el papel del responsable del tratamiento de datos”, aumentando sus competencias (vid., pg. 3). El texto puede consultarse en:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_es.pdf [Consulta: 10 de mayo de 2011].

el *Study on the economic benefits of privacy enhancing technologies*³² y el *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*³³.

Entre otros aspectos, la Comunicación de la Comisión “Un enfoque global de la protección de los datos personales en la Unión Europea”, plantea la necesidad de clarificar el denominado “derecho a ser olvidado”, que define como “el derecho de las personas a que sus datos no se traten y se supriman cuando dejan de ser necesarios con fines legítimos”, es decir, en el caso en que la persona “retira su consentimiento al tratamiento de datos” o de que “haya expirado el plazo” de conservación de los mismos³⁴.

De entre los numerosos documentos dirigidos a la Comisión por parte de particulares, entidades y organizaciones privadas e instituciones públicas de los Estados de la Unión Europea³⁵, la mayoría de aquellos que entran a valorar este aspecto coinciden en reconocer la necesidad de clarificar jurídicamente el denominado “derecho al olvido”, aunque con algunas matizaciones respecto a la necesidad de que dicho esclarecimiento requiera, necesariamente, la reforma de la Directiva 95/46/CE.

A este respecto, y sin pretensión de exhaustividad, puede destacarse la Contribución de la Agencia Española de Protección de Datos (AEPD), encargada de ejercer las funciones que le encomienda el artículo 37.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. En su opinión, la aplicación conjunta del principio según el cual todo consentimiento “puede ser revocado” y el contenido de los artículos 6.1.c)³⁶, 12.b)³⁷ y 14³⁸ de la Directiva 95/46/CE, constituyen mecanismos que, “adecuadamente

32 London Economics, julio de 2010. http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf [Consulta: 10 de mayo de 2011].

33 Enero de 2010. http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf [Consulta: 10 de mayo de 2011].

34 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones “Un enfoque global de la protección de los datos personales en la Unión Europea”. Op. cit., pg. 8.

35 El texto de todas las contribuciones remitidas a la Comisión en relación a la consulta, incluidas las citadas en las páginas que siguen, pueden encontrarse en http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm [Consulta: 10 de mayo de 2011].

36 El artículo 6.1. c) dispone que los Estados miembros “dispondrán” que los datos personales sean: “c) Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente”.

37 Por su parte, el artículo 12. b) de la Directiva citada establece que los Estados miembros “garantizarán” a todos los interesados el derecho de obtener del responsable del tratamiento: “b) En su caso, la rectificación, la supresión o el bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado”.

38 Según el artículo 14 de la Directiva, los Estados miembros “reconocerán al interesado el derecho” a: a) “oponerse”, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, “a que los datos que le conciernan sean

combinados”, deberían “permitir un ejercicio efectivo” del llamado “derecho al olvido”. No obstante, entiende que el marco jurídico comunitario “debe clarificar las posibilidades del ejercicio de dicho derecho a través de medidas de obligado cumplimiento para los responsables del tratamiento” que ofrezcan garantías sobre la sencillez en su ejercicio, la adopción de tecnologías “que impidan la indexación” de datos de carácter personal por motores de búsqueda y “su aplicación efectiva” en plazos perentorios³⁹.

Un criterio que contrasta con el expresado por el Consejo de Inspección de Datos de Suecia⁴⁰ que, sin hacer referencia en concreto al “derecho al olvido”, subraya la necesidad de que el ordenamiento comunitario proceda a una adaptación de la regulación del tratamiento de datos personales de los ciudadanos particulares que tome en consideración lo dispuesto en el artículo 3.2 de la Directiva 95/46/CE que, como es conocido, establece una excepción a la aplicación de la misma respecto del tratamiento de datos personales “efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas”⁴¹, dado que esta excepción ha sido interpretada por el Tribunal de Justicia de la Unión Europea en el sentido de que “contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares” y, por lo tanto, no alcanza al “tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas”⁴².

objeto de tratamiento”, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

b) “oponerse”, previa petición y sin gastos, “*al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección*”; o “*ser informado*” antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente, el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Además, los Estados miembros “*adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b)*”.

39 Vid. http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/aepd_dpa_es.pdf [Consulta: 10 de mayo de 2011].

40 Vid. http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/data_inspection_board_en.pdf [Consulta: 10 de mayo de 2011].

41 El artículo 3.2 de la Directiva 95/46/CE establece: “*Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:*

- *efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;*

- *efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas*”.

42 Sentencia de 6 de noviembre de 2003. Asunto C-101/01, Lindqvist, apartado 47. Vid. <http://curia.europa.eu/juris/cgi-bin/form.pl?lang=es> [Consulta: 10 de mayo de 2011].

Por su parte, el Comisionado Informativo de Gran Bretaña (ICUK), responsable de la promoción y aplicación de la Ley de Protección de Datos de 1998 y de la Ley de Libertad de Información de 2000, considera de “especial relevancia” el “derecho al olvido” en relación a los conceptos de consentimiento y transparencia respecto a los datos personales. En opinión de dicho Comisionado, resulta importante que la Comisión clarifique la extensión del “derecho al olvido” en la práctica, en tanto que, según afirma, existen situaciones en las que éste puede estar sujeto a limitaciones, como es el caso de los datos personales utilizados por los poderes públicos. Unas circunstancias limitadoras que, en su opinión, no concurren en relación con el tratamiento de datos con fines de marketing. A su juicio, es conveniente que la futura reforma no imponga la “cancelación” en aquellos ámbitos en los que la “ocultación” actualmente ya permite garantizar la protección de la privacidad de los derechos individuales.

En efecto, el ICUK estima que en ciertas situaciones el “derecho al olvido” podría aplicarse correctamente en la práctica, como aquellas en la que un individuo desea borrar sus registros de una red social en internet, pero estas situaciones, estima, “son limitadas”. Lo esencial, afirma, es que los individuos “conozcan la naturaleza y la extensión de sus derechos” y que esos derechos sean “recopilados de un modo no engañoso” para el individuo. En este sentido, el “derecho al olvido” admite posibilidades que quizás no son fácilmente accesibles para el individuo, o que, en determinados casos, “pueden ir contra sus derechos y libertades fundamentales”. No obstante, reconoce que podrían existir, en la práctica, “dificultades tecnológicas” para ejercer este derecho en ciertas circunstancias, como cuando la información es accesible públicamente a través de internet⁴³.

Más concretamente, el representante de la Comisión para la Protección de la Privacidad de Bélgica pone de manifiesto la necesidad de realizar una “ponderación” entre el “derecho al olvido” y la necesidad de almacenar información de carácter esencialmente histórico y cultural. En este sentido, afirma que la recopilación de datos en archivos dedicados a la investigación histórica debe ser fomentada y tratada como instrumento válido de conservación de los datos dada la utilidad operativa de los mismos, de ahí que no se encuentre “justificada”, en su opinión, la divergencia a la hora de aplicar “cancelaciones” entre las operaciones de tratamiento de datos realizadas con fines periodísticos y con fines históricos, dado que ambos objetivos protegen el mismo valor jurídico: “la libertad de información”⁴⁴.

En opinión del Gobierno Federal alemán se debe proceder a una clara distinción entre los términos “derecho al olvido” y “derecho de cancelación”. En relación con el primero, los requisitos relevantes deberían ser claramente definidos, del mismo modo que debería especificarse “contra quién” puede alegarse este derecho. Del mismo modo, afirma, también deberían ser especificadas las excepciones al mismo, al tiempo que debería examinarse la procedencia de consagrar este derecho en una norma jurídica que —como la Directiva de

43 Vid. http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/ico_infocommoffice_en.pdf [Consulta: 10 de mayo de 2011]

44 Vid. http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/cvpv_en.pdf [Consulta: 10 de mayo de 2011]

Protección de Datos- podría excluir las actividades personales y familiares de los ciudadanos. En última instancia, estima que debe ser tomada en consideración la aplicación técnica de tales medidas. En definitiva, el Gobierno Federal alemán manifiesta un gran interés en la idea de una “fecha de expiración de los datos” (“expiry date for data”), aunque considera que la aplicación técnica de la misma constituye un gran cambio⁴⁵.

En última instancia, en opinión del Supervisor Europeo de Protección de Datos (EDPS), el concepto del “derecho al olvido” está conectado con el “derecho a la portabilidad” de los datos, según se desprende de la Comunicación de la Comisión -“Un enfoque global de la protección de los datos personales en la Unión Europea”-, dirigida a reforzar los derechos sobre la protección de datos. En su opinión, resultan conceptos “complementarios” a los principios ya mencionados por la Directiva 95/46/CE, que protegen el derecho a la protección de datos en relación con el tratamiento de datos personales y establecen la obligación del responsable de los datos de “cancelar información” tan pronto como y no más allá del tiempo necesario en relación con el propósito del tratamiento de los datos personales⁴⁶.

Estas dos “nuevos conceptos”, estima, tienen un “valor añadido” en el contexto de la sociedad de la información, donde cada vez se recopila una mayor cantidad de datos y se retienen por periodos indefinidos de tiempo. La práctica muestra que, aunque los datos sean proporcionados por el propio titular, el “grado de control” efectivo de éste sobre sus datos personales es “muy limitado”. Esta es la realidad en lo que respecta, actualmente, a Internet. Además, “desde una perspectiva económica”, resulta más costoso para el responsable de los datos su cancelación que su almacenaje, de tal modo que los derechos de los individuos a este respecto chocan contra la tendencia natural de la economía⁴⁷.

En cualquier caso, ambos derechos (el “derecho al olvido” y el “derecho a la portabilidad”) podrían contribuir a “decantar la balanza” a favor del titular de los datos. El objetivo del “derecho a la portabilidad” de los datos podría ser el de proporcionar un mayor control a los individuos acerca de su información, mientras que el “derecho al olvido” podría garantizar que la información desaparezca automáticamente transcurrido un periodo de tiempo, aun cuando el titular de los datos no haya actuado o no sea todavía consciente de que los datos han sido almacenados⁴⁸.

Desde esta perspectiva, una “nueva codificación” del “derecho al olvido” podría asegurar la “cancelación” de los datos personales o la “prohibición de utilizarlos”, sin necesidad de una actuación del titular de los datos, pero con la condición de que los datos hayan sido

45 Vid. http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/bundesregierung_en.pdf [Consulta: 10 de mayo de 2011].

46 Vid. Apartado 83, en http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/edps_en.pdf

47 Vid. Apartado 84, en http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/edps_en.pdf [Consulta: 10 de mayo de 2011].

48 Vid. Apartado 85, en http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/edps_en.pdf [Consulta: 10 de mayo de 2011].

objeto de almacenamiento durante un cierto periodo de tiempo. En otras palabras, podría atribuirse a los datos una especie de “fecha de expiración”.

Este “principio”, afirma el Supervisor Europeo, se encuentra ya reconocido en sentencias judiciales nacionales o aplicado a sectores específicos, como por ejemplo, expedientes policiales, antecedentes criminales o expedientes disciplinarios⁴⁹.

Es en este sentido en el que un “nuevo derecho al olvido” podría conectarse con la “portabilidad de los datos”. El “valor añadido” que ello proporcionaría consiste en que no requeriría solicitud o requerimiento por parte del titular de los datos para que éstos fueran “cancelados”, en tanto que la cancelación se produciría de un modo “automático”. Sólo en circunstancias específicas en las que estuviera establecida la necesidad de prolongar la conservación de los datos, el responsable de los datos podría tener derecho a retenerlos. El “derecho al olvido” podría entonces “invertir la carga de la prueba” desde el individuo al responsable de los datos, y construir una “privacidad por defecto” en el ámbito del tratamiento de los datos personales⁵⁰.

En definitiva, el Supervisor Europeo de Protección de Datos considera que el “derecho al olvido” podría resultar especialmente útil en el contexto de los servicios de la sociedad de la información. La existencia o no de una “obligación de cancelar” la información tras un periodo de tiempo determinado tiene sentido especialmente en relación con los medios de comunicación y con Internet, y notablemente en las redes sociales.

Del mismo modo, afirma, podría ser útil en la medida en que sean accesibles los terminales de los equipos, de manera que los datos almacenados en dispositivos u ordenadores móviles podrían ser “automáticamente cancelados” o “bloqueados” tras un periodo determinado de tiempo cuando ya no estén en posesión del individuo. En este sentido, el “derecho al olvido” puede traducirse en una “privacidad deliberadamente” obligada⁵¹.

Por su parte, el Consejo Europeo, en la reunión 3071st Justicia y Política Interior (24 y 25 de febrero de 2011), ha adoptado un conjunto de conclusiones acerca de la mencionada Comunicación de la Comisión, donde reconoce que, dada la diferente transposición de la Directiva de 1995 relativa a la protección de datos personales por los Estados miembros, una armonización de la protección de datos al más alto nivel “sería beneficiosa tanto para los titulares de los datos como para los responsables de los mismos”⁵².

49 Vid. Apartado 88, en http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/edps_en.pdf [Consulta: 10 de mayo de 2011].

50 Vid. Apartado 89, en http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/edps_en.pdf [Consulta: 10 de mayo de 2011].

51 Vid. Apartado 90, en http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/edps_en.pdf [Consulta: 10 de mayo de 2011].

52 Vid. Punto 11 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf [Consulta: 10 de mayo de 2011].

En este sentido, afirma, la revisión de la normativa sobre protección de datos, tomando como base lo establecido en el artículo 16 del Tratado de Funcionamiento de la Unión Europea ofrece, entre otros aspectos, “una oportunidad para mejorar los procedimientos de protección de los datos”⁵³, por lo que, “anima” a la Comisión a “explorar la introducción del derecho al olvido, como un instrumento legal innovador, en la medida en que las nuevas tecnologías posibiliten el ejercicio de dicho derecho”⁵⁴.

4. CONCLUSIONES

En definitiva, podemos concluir que el acelerado desarrollo de la sociedad de la información y la creciente complejidad técnica de las tecnologías asociadas a su desarrollo plantean nuevos retos en nuestras sociedades democráticas. Estos nuevos retos aparecen en dos líneas relativamente convergentes: por un lado, es necesario la redefinición de derechos tradicionalmente contruidos entre nosotros, sobre todo en lo que se refiere a los derechos relacionados con la libertad de expresión o el derecho a la información y su posibles conflictos con el derecho al honor, a la intimidad personal o a la propia imagen; y, por otro, como respuesta a nuevos peligros que amenacen la libertad de los ciudadanos, es necesario la creación de nuevos derechos que la sigan garantizando, entre ellos podemos citar el derecho al anonimato en la red o, en el caso que aquí nos ocupa, el derecho al olvido.

Concretamente, en relación a este último derecho, hemos reflejado en las páginas anteriores las repuestas que se han ofrecido desde la Agencia Española de Protección de Datos que, aunque suponen un primer intento de amparar a los ciudadano en este derecho, no dejan de ser relativamente insatisfactorias, ya que se han centrado en hacer responsable especialmente al buscador “Google”, dejando un poco al margen de sus resoluciones a los responsables originarios de volcar esa información en la red (probablemente porque en numerosas ocasiones el responsable es una institución pública). Esta respuesta aparece, como poco, parcial, ya que no afronta el principal problema –que es como hemos señalado– el de la responsabilidad de las fuentes originales de la información y, por otra parte, porque al centrar en un único buscador la responsabilidad de ocultar los resultados de sus búsquedas, deja de lado a otros buscadores que, en este mismo momento, también pueden indexar y exponer en sus resultados la información conflictiva o buscadores que puedan surgir en el futuro.

La insatisfacción que conlleva esta solución ha obligado a la Unión Europea a afrontar iniciativas para lograr un nuevo avance en esta materia. Aunque hemos recogido las posibles líneas de evolución de estas nuevas regulaciones, no podemos dejar de poner de manifiesto

53 Vid. Punto 3 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf [Consulta: 10 de mayo de 2011].

54 Vid. Punto 22 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf [Consulta: 10 de mayo de 2011].

la multiplicidad de soluciones aportadas y las dificultades técnicas indudables que presentan algunas de las aportadas.

5. BIBLIOGRAFÍA

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2009) *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line*. Madrid, Instituto Nacional de Tecnologías de la Comunicación y la AEPD.
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Memoria, diversos años*. Accesibles en: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/index-ides-idphp.php> [Consulta: 10 de mayo, 2011]
- ALONSO BLAS, D. (1996): “El futuro de la protección de datos a nivel europeo”, en DAVARA RODRIGUEZ, M.A. (Coord.) *“Encuentros sobre Informática y Derecho (1995-1996)”*. Pamplona: Aranzadi.
- BELLO JANEIRO, D. (2001): “La protección de datos de carácter personal en el Derecho comunitario”, *Anuario de la Facultad de Derecho de la Universidad de la Coruña*, nº 5.
- BRU CUADRADA, E. (2007): “La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad”, *Revista de Internet, Derecho y Política*, nº 5.
- CORRAL TALCIANI, H. (2000) «Configuración jurídica del derecho a la privacidad II: Concepto y delimitación». *Revista Chilena de Derecho*, vol. 27 núm. 2, págs. 331-355
- DUBIÉ, P. (2003) «Protección de datos y derecho al olvido», *Derecho de los negocios*, Año nº 14, Nº 154-155, págs. 1-16
- FERRANDO VILLALBA, M^a L. (2.000), *La información de las Entidades de Crédito. Estudio especial de los informes comerciales bancarios* Valencia ,Ed. Tirant lo Blanch.
- GARRIGA DOMÍNGUEZ, A. (2004) *Tratamiento de datos personales y derechos fundamentales*. Madrid, Dykinson
- GUERRERO PICÓ, M^a C. (2006): “*El impacto de internet en el derecho fundamental a la protección de datos de carácter personal*”. Thomson-Civitas.
- HEREDERO HIGUERAS, M. (1997): “*La Directiva comunitaria de protección de los datos de carácter personal (Comentario a la Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos)*”. Pamplona: Aranzadi.
- HERRÁN ORTIZ, A.I. (2001): “La protección de datos de carácter personal en el marco de la Unión Europea”, en *REDI*, nº 39.
- MAYER-SCHÖNBERGER, V. (2010): *Delete. Il diritto all'oblio nell'era digitale*. Milan: Egea.
- ORWELL, G. (1949) 1984. 1ª edición 1952, Barcelona: Ed. Planeta
- ORZA LINARES, R. M. (2009) “¿Es posible la creación de nuevos derechos fundamentales asociados a las nuevas tecnologías de la información y de la comunicación?”. Ponencia

presentada al *IV Congreso de la Cibersociedad: Crisis analógica, futuro digital*. Accesible en: <http://www.cibersociedad.net/congres2009/es/coms/es-posible-la-creacion-de-nuevos-derechos-fundamentales-asociados-a-las-nuevas-tecnologias-de-la-informacion-y-de-la-comunicacion/991/>. [Consulta: 10 de mayo, 2011].

PACE, A. (1998) «El derecho a la propia imagen en la sociedad de los *mass media*» *Revista Española de Derecho Constitucional*, núm. 52, pags. 33-52

PRIETO GUTIÉRREZ, J.M^a. (1997): “La Directiva 95/46/CE como criterio unificador”, *Poder Judicial*, nº 48.

SÁNCHEZ BRAVO, A. (1998): “*La protección del derecho a la libertad informática en la Unión Europea*”. Sevilla: Universidad de Sevilla.

VIGURI PEREA, A. (1999): “*Intimidad versus informática (La protección de datos de carácter personal: perspectiva desde el derecho comparado)*”, *La Ley*, Tomo de Jurisprudencia 2.

