DERECHO DE AUTODETERMINACIÓN INFORMATIVA Y EL DERECHO AL OLVIDO: LA GENERACIÓN "GOOGLE" DEL DERECHO A LA VIDA PRIVADA

Ana Azurmendi
Profesora de Derecho de la comunicación de la Universidad de Navarra

RESUMEN La comunicación que se presenta aborda el derecho de autodeterminación informativa y el derecho al olvido, en el contexto de la discusión del borrador del Reglamento europeo de Protección de Datos Personales, cuya aprobación está prevista para los próximos meses de 2014. El derecho al olvido ha cobrado fuerza argumentativa sobre todo a partir de algunos casos europeos que se consideran en el estudio.
Los precedentes de este derecho así como la batalla frente a Google por parte de las agencias de protección de datos europeas ponen de manifiesto la diferente perspectiva adoptada sobre este problema, en Europa y en Estados Unidos. Si aquí se priorizaría el potencial del almacenamiento de datos personales para el desarrollo del marketing, del comercio electrónico y de la comunicación política –entre otros sectores-, Europa parece priorizar la libertad individual como clave del sistema democrático y los beneficios de los derechos a la vida privada y a la reputación.
Pero lejos de tratarse de un problema doctrinal o jurisprudencial que pueda resolverse mediante fórmulas legales o definiciones, es una realidad que afecta a millones de personas de todo el mundo, para quienes la tecnología ha ofrecido ya algunas soluciones, con aplicaciones que harían fácil tanto el control del usuario sobre sus datos como su borrado.
Las conclusiones se centran en la necesidad de una regulación europea del derecho al olvido, tal y como plantea el borrador del nuevo Reglamento europeo, y en el horizonte tecnológico de una solución efectiva al problema de la difusión universal de datos personales.

PALABRAS CLAVE: Derecho al olvido, Autodeterminación informativa, Google, *Digital Ephemerality*

1. LAS INICIATIVAS EUROPEAS Y ESTADOUNIDENSE PARA LA PROTECCIÓN DE DATOS PERSONALES: DIFERENTES PERSPECTIVAS Y EXTENSIÓN DE LA PROTECCIÓN

En enero de 2012, la Comisión Europea hizo público el borrador de un Reglamento de "Protección de Datos personales"[1] que vendría a sustituir a la Directiva 95/46/EC sobre la misma materia. Una de las principales novedades que presenta el borrador es el reconocimiento del derecho al olvido, definido como "el derecho de obtener del controlador[2] de un determinado dato personal su cancelación o eliminación y la abstención por parte del

[1] En la actualidad su versión consolidada es de octubre de 2013, que es la que se maneja en la comunicación, accesible en http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf, con acceso 5 de febrero 2014. Borrador de enero de 2012 en *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation),* COM (2012) 11 final (Jan. 25, 2012), *accesible en* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf con acceso 5 de febrero de 2014. En la actualidad, el texto

[2] El "Controlador" en definición recogida en el art. 4 (5) del borrador del Reglamento europeo de Protección de Datos es: "(…) the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, *conditions* and means of the processing of personal data; where the purposes, *conditions* and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law";

mismo controlador de diseminarlo". Esta iniciativa europea no es un acto aislado. En Francia se ha reconocido hace años un "*droit à l'oubli*" –es cierto que con referencia no sólo a datos personales, sino también a información sobre la vida privada que manejan los medios de comunicación- (Jeffrey Rosen, 2012: p. 88). En Alemania, a partir de la sentencia del Tribunal Constitucional de 1984, sobre el Censo de 1983, existe el "derecho de autodeterminación informativa" ("*Recht auf Informationelle Selbstbestimmung"*)[3]. Y en España se reconocen ambos derechos: un derecho equivalente al derecho al olvido con la Ley Orgánica 15/1999, de "Protección de Datos Personales"(Artemi Rallo Lombarte, 2010: p.2), con el derecho de rectificación y cancelación de datos personales (art. 16); y, un derecho de autodeterminación informativa a partir de la Sentencia Constitucional de STC 292/2000, de 30 de noviembre[4].

Estados Unidos, ese mismo año 2012, publicó la "*Consumer Privacy Bill of Rights*" cuyo objeto era el mayor acceso y control de los consumidores sobre sus datos personales procesados por segundas y terceras partes. Pero, como el mismo nombre de la ley revela, las iniciativas europea y estadounidense no son del todo equiparables (Steven C. Bennet, 2012: p.168-171). En el caso de Estados Unidos la ley protegería sólo algunos datos personales –los referidos a la privacidad- y obtenidos-procesados de sólo una parte de los usuarios: los consumidores. Mientras que las iniciativas europeas abordan el problema de todas las informaciones referidas a una identidad personal –sean o no relativas a la vida privada-, obtenidos-procesados de cualquier usuario (Steven C. Bennett 2012: pp. 164 y 165).

Se trata en ambos casos de reaccionar ante la necesidad puesta de manifiesto por diez Agencias de Protección de Datos -Alemania, Canadá, España, Francia, Holanda, Irlanda, Israel, Italia, Nueva Zelanda y Reino Unido- en 2010, que señalaban al motor de búsqueda *Google*, mediante acusaciones judiciales y extrajudiciales, por vulnerar de forma sistemática los derechos de protección de datos de ciudadanos.

2. *GOOGLE:* EL FRENTE DE BATALLA POR LA PRIVACIDAD

Han sido sobre todo los servicios *Buzz* y *Streetview* de *Google* los que han propiciado la reacción de las Agencias de Protección de Datos. En 2010, *Buzz*, una red social, había hecho públicamente visibles, por defecto, todas las direcciones de contacto de sus usuarios. Mientras que *Streetview*, un servicio de fotografías en tiempo real de las calles de las ciudades- había recopilado miles de datos personales de usuarios de *wifi* en el paso de los automóviles de *Google* por innumerables localidades europeas, canadienses y neozelandesas.

Ante las acusaciones judiciales y extrajudiciales de aquel momento, *Google* argumentó que el problema se había resuelto al implementar una mayor transparencia, tal y como anunció en su web corporativa, en la que hizo públicos sus nuevos principios de privacidad[5].

Pero la tormenta sobre *Google* viene de lejos. La actitud de sus directivos, sus respuestas slogan del tipo "somos responsables, todo lo hacemos para mejorar nuestros servicios a

---

[3] Gerrit Hornung y Christoph Schnabel, "Data protection in Germany I: The population census decision and the right to informational self-determination", Computer Law & Security Report, Vol.25, n 1, 2009, pp 84-88,

[4] Sentencia del Tribunal Constitucional 222/2000, de 30 de noviembre:
"La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. (Fundamento jurídico 6)

[5] Accesibles en http://www.google.com/policies/technologies/ con acceso 5 de febrero de 2014.

nuestros usuarios" repetidas a coro por cada representante de la compañía contrasta –al menos en el tono- con su defensa frente a las demandas judiciales de "soy global ergo alegal". Todo esto más las declaraciones del CEO de *Google*, Eric Smith, al Wall Street Journal en agosto de 2010[6], ha motivado que, aunque la corporación no sea la única empresa que con carácter internacional opera con los datos personales de sus usuarios, al final, el debate sobre las nuevas dimensiones del derecho a la vida privada y de protección de datos personales en la era Internet se haya centrado en *Google*. Eric Smith, en la entrevista del periódico económico titulada "*Google and the Search for the Future. The Web icon's CEO on the mobile computing revolution, the future of newspapers, and privacy in the digital age"* afirmaba:

> "I actually think most people don't want *Google* to answer their questions (….) They want *Google* to tell them what they should be doing next. (…) Because of the info *Google* has collected about you, we know roughly who you are, roughly what you care about, roughly who your friends are. (…)
> "The power of individual targeting—the technology will be so good it will be very hard for people to watch or consume something that has not in some sense been tailored for them."(…)
>
> "I don't believe society understands what happens when everything is available, knowable and recorded by everyone all the time"
>
> Añade el periodista: "He predicts, apparently seriously, that every young person one day will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends' social media sites".

Erick Smith fue relevado de su cargo en abril de 2011. Pero posiblemente puso sobre la mesa uno de los temas más preocupantes en el entorno redes sociales-Internet: el riesgo que supone para la libertad de los individuos el enorme poder de información acumulado por las empresas de Internet. Un poder que básicamente consiste, por un lado, en su capacidad de predecir los comportamientos de millones de personas –previo conocimiento, durante años, de sus intereses, de sus comunicaciones personales, de sus intercambios de opiniones, sus *sites* favoritos, sus acciones profesionales, sus compras online, sus fotografías, las que de otros han publicado de ellas, y miles de cuestiones más-. Y, por otro lado, en la generación de unas identidades digitales que acompañen de por vida a los ciudadanos, determinando en muchos casos decisiones de su entorno profesional, personal, etc. Éste es el horizonte protegible de las nuevas versiones del derecho a la privacidad (Omer Tene 2011: p. 21).

3. LOS PRIMEROS CASOS SOBRE EL DERECHO AL OLVIDO

Tal y como señala Alessandro Mantelero (2013: p. 229), el derecho al olvido podría considerarse incluido en el derecho estadounidense, entre las intromisiones ilegítimas en la vida privada, dentro de la acción "*public disclosure of private fact*"; los casos *Melvin v.Reid* (1931) y *Sidis v. F-R Publishing Co*. (1940) serían los representativos de este *tort*[7]. Pero, como es evidente por las fechas, no se trata del "derecho al olvido" en los términos que ahora se plantean, sino de un tipo clásico de intromisión ilegítima en la vida privada: la difusión de hechos ciertos con alguna –pero no determinante- relevancia pública que dañan la reputación u otros intereses de una persona.

---

[6] Accesible la entrevista completa en http://online.wsj.com/news/articles/SB10001424052748704901104575423294099527212, con acceso 5 de febrero de 2014.

[7] Ver un resumen de los dos casos en Alessandro Mantelero, "The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'", Computer Law & Secrutiy Review, 29, 2013, pp.230 y 231.

Sí se refieren al "derecho al olvido" los primeros casos resueltos en Italia y en Francia por sus respectivas autoridades de protección de datos, *Autorità garante per la protezione dei dati personali y la Commission Nationale Informatique et Libertés* (CNIL), sobre la publicación de datos por la *Autorità garante della concorrenza e del mercato*, en 2004[8] y por *LEXEEK*, en 2011, y el planteado en España por el camping "*Els Alfacs*" (*Alfacs Vacances)* contra *Google España*, en 2010 (con sentencia desestimatoria de 23 de Febrero de 2012 del Juzgado de Primera Instancia de Amposta, Tarragona).

La *Autorità garante per la protezione dei dati personali* resolvió la demanda planteada por un anunciante sancionado por publicidad engañosa por la agencia italiana de la competencia, *Autorità garante della concorrenza e del mercato*. Aquél había visto cómo su nombre aparecía en el boletín de la agencia de la competencia asociado al ilícito de publicidad engañosa. Como consecuencia de su difusión permanente en Internet, favorecida por los motores de búsqueda, se le estaba causando un grave perjuicio. El demandante no impugnaba la publicación en el boletín de la autoridad de la competencia, sino su "difusión en Internet sin adoptar las oportunas cautelas" (tales como el oscurecimiento de los nombres, o la posibilidad de permitir el acceso a las medidas sólo mediante una investigación dentro del sitio, donde los motores de búsqueda no pudieran acceder). Por el contrario, la autoridad de la competencia italiana estimaba que era necesario publicar la identidad del anunciante, puesto que "su omisión frustraría el propósito mismo de la legislación de la publicidad engañosa, especialmente cuando, como en este caso, de no tener esos datos, no sería posible identificar el anuncio". La *Autorità garante per la protezione dei dati personali* argumentó que la autoridad de la competencia podría seguir publicando sus medidas en su sitio web, pero "modulando el tiempo en el cual las decisiones relativas a las denuncias serán directamente detectables en Internet a través de los motores de búsqueda externos". Obligó a la autoridad de la competencia a incluir una sección dentro de su sitio web donde se puedan consultar por vía telemática aquellas decisiones con determinada antigüedad, y donde no sea posible la "directa detectabilidad de las decisiones contenidas en ella a través de motores de búsqueda externos". Al mismo tiempo, solicitó a la autoridad de la competencia que definiera el periodo de tiempo considerado proporcional para las finalidades perseguidas por la publicación de datos en su web.

En el caso francés, la CNIL publicó una resolución sancionadora en 2011 contra la asociación *LEXEEK*[9], que elabora bases de datos de sentencias judiciales publicadas en Francia, por no eliminar en ellas los nombres y direcciones de las partes y testigos de los juicios, a pesar de los requerimiento de la CNIL, desde 2008, para que lo hiciera. El fundamento para la sanción condenatoria (de 10.000€) fue la "practique attentatoire au respect de la vie privée des personnes et au droit à l'oubli numérique".

En cuanto al caso del camping *Les Alfacs* la empresa denunció en 2010 a *Google España* por no atender a sus solicitudes de no situar entre los primeros resultados de búsqueda la tragedia sucedida en el camping en 1978; cuando la explosión de un camión cisterna cargado con propileno costó la vida de 243 personas. Se reclamaba el derecho al olvido y el derecho al honor de la empresa. Se pedía a *Google* que distinguiera las búsquedas sobre la tragedia de aquellas otras dirigidas a obtener información sobre el camping, puesto que la situación actual de presentación de resultados de búsqueda en *Google* perjudicaba de forma grave al negocio. El recurso fue desestimado porque la demanda debería haberse dirigido contra *Google.inc*, responsable de los contenidos y no contra *Google España*, responsable de la publicidad.

---

[8] Caso comentado por Pere Simon Castellano en Pere Simon Castellano, "El derecho al olvido en el universo 2.0", Bid 28 (2012) DOI: 10.1344/105.000001808
http://bid.ub.edu/28/simon2.htm con acceso 4 de marzo de 2014.

[9] Decisión accesible en http://www.cnil.fr/fileadmin/documents/La_CNIL/decisions/D2011-238_LEXEEK.pdf, con acceso 6 de febrero de 2014.

Sin duda *Autorità garante della concorrenza e del mercato, LEXEEK* y *Les Alfacs* ponen de manifiesto la necesidad de una protección específica más allá de la ofrecida por la tradicional "privacidad" o "derecho al honor". En los tres casos, una de las formas de resolver esa protección sería respetar una adecuada dosificación de los tiempos de publicación de la información. De manera que si bien es lógico, e incluso exigible, que un contenido informativo, perjudicial para los intereses de personas o empresas, sea accesible al conjunto de ciudadanos por circunstancias de su actualidad y relevancia, también es razonable que, una vez desaparecidas estas circunstancias, el perjuicio provocado por la publicidad pueda atenuarse. Bien mediante la inserción de los datos en una sección donde esos datos se hacen indetectables para los motores de búsqueda externos, bien mediante el anonimato de los protagonistas de los hechos ya juzgados o sancionados–utilizando iniciales en las decisiones o sentencias publicadas en Internet- o bien mediante la desvinculación en las búsquedas de las actividades actuales de personas físicas o jurídicas de los hechos noticiosos de hace décadas como ocurre en *Les Alfacs.* Un cuestión en la que profundiza Pere Simon Castellano (2, 2012: pp. 64-98).

4. LA RESPUESTA DEL ABOGADO GENERAL DEL TRIBUNAL DE JUSTICIA EUROPEO SOBRE UNA CONSULTA PREJUDICIAL SOBRE EL DERECHO AL OLVIDO

Existe un cuarto caso sobre derecho al olvido planteado por la AEPD frente a Google que ha originado una consulta de la Audiencia Nacional española al Tribunal de Justicia Europeo (Caso C-131/12) *Petición de decisión prejudicial presentada por la Audiencia Nacional (España) el 9 de marzo de 2012- Google Spain, S.L., Google, Inc. / Agencia de Protección de Datos (AEPD), Mario Costeja González*[10]. En esta ocasión un ciudadano se ha visto perjudicado durante años por un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, publicado en el periódico La Vanguardia en 1998. Desde el momento en el que este medio de comunicación digitalizó todos sus números en papel, el nombre de Mario Costeja aparece vinculado, en las búsquedas de Google, a datos de su situación civil y patrimonial que son incorrectos en la actualidad. De esta situación se ha derivado un daño en su vida profesional. Solicitó primeramente a la Agencia Española de Protección de Datos que se exigiera al periódico la eliminación de esos datos pero la petición no prosperó. La Agencia estimó que la publicidad de la subasta realizada en La Vanguardia era legal. Su eliminación significaría atentar contra la libertad de expresión. Sin embargo, la AEPD solicitó a *Google España* y *Google Inc.* que dejara de indexar este contenido. *Google* recurrió la acción de la Agencia –junto con otras más semejantes- ante la Audiencia Nacional.

Este órgano jurisdiccional elevó consulta prejudicial ante el Tribunal de Justicia Europeo en 2012, con el objeto de obtener aclaración sobre aspectos concretos de la Directiva 95/45/EC de "Protección de Datos Personales" y, así, perfilar mejor su aplicabilidad a determinadas acciones del motor de búsqueda *Google*. Junto a esto, pretendía precisar los argumentos para poder exigir a la empresa de Internet acciones relacionadas con la garantía del derecho al olvido. Entre otras se hacía la pregunta:

> "3.1. ¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulados en el art. 14.a) de la Directiva 95/46/CE comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?"

[10] Se trata de la *Petición de decisión prejudicial presentada por la Audiencia Nacional (España) el 9 de marzo de 2012- Google Spain, S.L., Google, Inc. / Agencia de Protección de Datos (AEPD), Mario Costeja González* accesible en http://curia.europa.eu/juris/document/document.jsf?docid=123131&doclang=ES, con acceso 11 de febrero de 2014.

El preámbulo de la decisión prejudicial llegó el 25 de junio de 2013, con las Conclusiones del Abogado General del Tribunal de Justicia Europeo Niilo Jääskinen[11], que se resumirían en:

a) Los proveedores de servicios de motor de búsqueda en Internet no son responsables, sobre la base de la Directiva sobre Protección de Datos, de los datos personales incluidos en las páginas web que tratan.
b) La normativa nacional de protección de datos les es de aplicación (a los proveedores de servicios) cuando establecen en un Estado miembro una oficina que orienta su actividad hacia los habitantes de dicho Estado. Aunque el fin de esta oficina sea el de promover y vender espacios publicitarios en su motor de búsqueda y aunque el tratamiento técnico de los datos se realice en otro Estado, sea o no miembro de la Unión Europea.
c) Los derechos de cancelación y bloqueo de datos, establecidos en el artículo 12, letra b), y el derecho de oposición, establecido en el artículo 14, letra a), de la Directiva 95/46, no confieren al interesado el derecho a dirigirse a un proveedor de servicios de motor de búsqueda para impedir que se indexe información que le afecta personalmente, publicada legalmente en páginas web de terceros, invocando su deseo de que los usuarios de Internet no conozcan tal información si considera que le es perjudicial o desea que se condene al olvido.

En la exhaustiva línea argumental del Abogado General, señalaba entre otras cuestiones:

> "B. *Motores de búsqueda en Internet y protección de datos*
>
> 32. Al analizar la posición legal de un motor de búsqueda en Internet en relación con las normas de protección de datos, deben tenerse en cuenta los siguientes elementos.
>
> 34. (…), los resultados que ofrece un motor de búsqueda en Internet no se basan en una búsqueda instantánea de todo el World Wide Web, sino que se compilan a partir del contenido que el motor de búsqueda en Internet ha tratado previamente. Ello significa que el motor de búsqueda en Internet ha recopilado contenidos a partir de páginas web existentes y que ha copiado, analizado e indexado dicho contenido en sus propios dispositivos. Este contenido recuperado contiene datos personales si éstos figuran en alguna de las páginas web fuente.
>
> 35. (…) para que los resultados sean más fáciles de usar, los motores de búsqueda normalmente muestran contenidos adicionales además del enlace a las páginas web originales. Pueden ser extractos de texto, contenido audiovisual o incluso instantáneas de las páginas web fuente. Esta vista previa de la información puede, al menos en parte, recuperarse a partir de los dispositivos del proveedor de servicios de motor de búsqueda en Internet, y no instantáneamente desde la página web original. Ello quiere decir que el proveedor del servicio está realmente en posesión de la información expuesta de este modo."

Y continúa en su aclaración para la Audiencia Nacional española:

> "D. *El papel y la responsabilidad de los editores de la página web fuente*
>
> 42. (…) técnicamente, el editor tiene la posibilidad de incluir en sus páginas web códigos de exclusión que restringen el indexado y el archivo de la página y que, por tanto, incrementan la protección de datos personales. En casos extremos, el editor puede retirar la página web del servidor de alojamiento, volver a publicarla sin los datos personales controvertidos y solicitar que se actualice la página en las memorias ocultas de los motores de búsqueda.
>
> (…)
>
> 44. No obstante, la responsabilidad del editor no garantiza que los problemas de protección de datos puedan abordarse de manera definitiva recurriendo sólo a los responsables del tratamiento de las páginas web fuente. (…)

[11] Conclusiones accesibles en http://curia.europa.eu/juris/document/document.jsf?text&docid=138782&pageIndex=0&doclang=ES&mode=req&dir&occ=first&part=1&cid=362663 con acceso 11 de febrero de 2014.

> 45. De hecho, la accesibilidad universal de la información en Internet se basa en los motores de búsqueda en Internet, ya que sin ellos hallar información relevante sería demasiado complicado y difícil y produciría resultados limitados (…)

Acerca de lo que plantea *Google* para evadir la aplicación de la Directiva Europea, al señalar que es *Google.Inc* con sede en California la empresa que trata los contenidos y que *Google* España únicamente se dedica al negocio publicitario, se responde:

> "68. (…) se lleva a cabo tratamiento de datos personales en el marco de las actividades de un 'establecimiento' del responsable del tratamiento, en el sentido del artículo 4, apartado 1, letra a), de la Directiva, cuando la empresa que provee el motor de búsqueda establece en un Estado miembro, a fines de promover y vender espacios publicitarios en su motor de búsqueda, una oficina o una filial que orienta su actividad hacia los habitantes de dicho Estado".

Y sobre el derecho al olvido:

> "109. Aunque el Tribunal de Justicia declarase que los proveedores de servicios de motor de búsqueda en Internet se responsabilizan, como responsables del tratamiento, *quod non,* de los datos personales contenidos en las páginas web fuente de terceros, un interesado tampoco tendría un 'derecho al olvido' absoluto que pudiera invocar frente a los proveedores de servicios. Sin embargo, el proveedor de servicios necesitaría ponerse en la posición del editor de la página web fuente y comprobar si la difusión de los datos personales en la página web podría considerarse legal y legítima a los efectos de la Directiva. Dicho de otro modo, el proveedor de servicios necesitaría abandonar su función de intermediario entre usuario y editor y asumir la responsabilidad por el contenido de la página web fuente y, cuando resultase necesario, censurar el contenido evitando o limitando el acceso a éste".

En definitiva: se asume y reconoce el "derecho al olvido" frente al proveedor de servicios, aunque con un matiz de subsidiariedad respecto al editor de la página web fuente, aspecto que no queda completamente aclarado en la respuesta ofrecida por el Abogado General.

5. TEMPORALIDAD DE LOS DATOS PERSONALES O DIGITAL EPHEMERALITY COMO UNA SOLUCIÓN VINCULADA AL DERECHO AL OLVIDO

En todos los casos mencionados, los datos personales sobre los que se solicita "derecho al olvido" habían tenido una difusión proporcionada a su relevancia en el momento de su primera publicación. Así, es lógico que una sanción a un anunciante por publicidad engañosa se publique en el boletín de la autoridad de la competencia (Caso *Autorita garante de la concorrenza*), como lo es que en una sentencia original aparezcan nombradas las partes que intervienen (caso *LEXEEK)*, que en un periódico se informe de un accidente de dimensiones catastróficas (caso *"Els Alfacs"*) o que se dé publicidad a una subasta de bienes con carácter previo a su celebración (caso *"Mario Costeja"*). Sin embargo, el hecho de que, hasta 10 y 15 años después, esos mismos datos estén accesibles con carácter ilimitado a un número indeterminado de personas no parece tan lógico si ocasiona perjuicios notables, de tipo moral y económico, a las personas físicas o jurídicas nombradas, cuando las circunstancias que fueron la causa de aquella publicación ya no perduran en la actualidad.

Una de las soluciones que se barajan para mitigar este perjuicio, a la vez que se respeta la libertad de expresión, consiste en establecer un plazo de tiempo razonable para la accesibilidad universal de este tipo de datos, a partir del cual se deberían:

a) Eliminar esos datos de la fuente original, sustituyéndolos por iniciales (parece apropiado para las publicaciones de resoluciones y sentencias judiciales, en algunos casos también para periódicos).
b) Plantear un doble paso en el acceso a la información, de manera que los contenidos publicadas por medios de comunicación a partir de una fecha con respecto a su difusión inicial pasen a un fondo de hemeroteca que no sería accesible directamente para los motores de búsqueda, sino que sería necesario entrar en la web del medios de comunicación y desde ahí iniciar otro proceso de registro y de búsqueda para el acceso a los números anteriores a esa fecha.

Temporalidad de los datos frente a su permanencia en Internet es una de las ideas de las que más se habla como medio para incorporar el derecho al olvido (Susan Corbett 2013: p. 148). Otra solución cercana sería, en palabras de Meg Leta Ambrose (2013: p.1) la *Digital Ephemerality*. Se trata de una exigencia que podría vincularse al "derecho al olvido" sobre determinados datos, pero que, al mismo tiempo, es ya un objetivo buscado por muchos usuarios de Internet con el *Snapchat* –una aplicación de móvil que permite a los usuarios enviar fotos que desaparecen en 10 segundos- o por empresas como *Reputation.com* o *Reputación en Internet*, o *Abine* que vende el servicio *DeleteMe* que elimina perfiles públicos de las principales webs de datos, información social y de contacto, fotos personales etc. *Abine*, al mismo tiempo, oferta el servicio de lanzar los contenidos positivos sobre sus clientes a los primeros resultados de búsquedas. Tal posibilidad de control sobre los contenidos relativos a la propia persona muestra la proximidad del derecho al olvido con el derecho de autodeterminación informativa.

Hoy por hoy, cualquiera de estas soluciones parece difícil de aplicar en la práctica, a pesar de que hay investigaciones en marcha que muestran un futuro de mayor control de los ciudadanos sobre sus datos personales. Como el proyecto *"Vanish"*[12] de la Universidad de Washington, mencionado por Susan Corbett (2013: nota 64, p. 149), en el que se está trabajando sobre un sistema de encriptación cuya función sería la autodestrucción de los datos después de un periodo de tiempo determinado. Así, en lugar de confiar en que será *Google*, *Facebook* o *Hotmail* quienes eliminan los datos almacenados, será *"Vanish"* quien encripte los datos y luego deshaga la clave de encriptamiento.

Pero la oposición a esta temporalidad del mantenimiento de datos personales en Internet tiene también su razón de ser. El derecho a la información (David S. Ardia 2010: p. 30) o necesidades públicas como la seguridad (Jef Ausloos 2012: p. 149) quedan o, cuando menos, pueden quedar muy neutralizados ante un derecho al olvido que podría eliminar de forma definitiva informaciones importantes. Una de las críticas más repetidas contra el derecho al olvido es que, de aplicarse, se estaría facilitando un tipo de censura sutil, en la medida en que, si se permite a todas las personas eliminar sus datos personales según su deseo, dejarían de estar accesible datos relevantes y, en consecuencia, podría darse lugar a una falsificación de la realidad. Por esta razón, en opinión de Ardia y Ausloos, al constatar que, en muchas ocasiones, no es posible discernir qué información de la accesible en la actualidad será relevante en un futuro, sería preferible no considerar un derecho al olvido generalizado. Por otro lado, María Eduarda Gonçalves e Inés Andrade (2013: pp. 255-259) y Troncoso Reigada (2012: p.16) consideran que hay otras razones añadidas a las del derecho a la información, la libertad de expresión y a la necesidad de seguridad, como son:

a) razones de interés público en el área de salud pública;
b) finalidades de carácter histórico, estadístico y de investigación científica;

12 Más sobre el proyecto en http://vanish.cs.washington.edu/ con acceso 28 febrero 2014

c) el cumplimiento de la obligación legal de conservar datos personales.

Unos límites que, desde su punto de vista, son muy difíciles de equilibrar con el derecho al olvido, hasta el punto de que la "metáfora de la proporcionalidad" en la ponderación de derechos en conflicto no funciona de forma correcta en el caso de los datos personales[13].

6. EL DERECHO DE AUTODETERMINACIÓN INFORMATIVA

Las empresas *Reputation.com* o *Reputación en Internet*, o *Abine* no sólo son un negocio de eliminar datos personales, sino que, al mismo tiempo, ofrecen servicios de posicionamiento en los resultados de búsquedas acerca de sus clientes. Tal posibilidad de control sobre los datos relativos a la propia persona muestra la proximidad existente entre el derecho al olvido y el de autodeterminación informativa, un derecho de construcción jurisprudencial reconocido por primera vez en Alemania en la influyente sentencia del Tribunal Constitucional de 1983, recurso de amparo contra la Ley del "Censo de Población, Profesiones, Viviendas y Centros de Trabajo" de 1982[14]. Se definió entonces como:

> "facultad del individuo para determinar fundamentalmente por sí mismo la divulgación y utilización de los datos referentes a su persona"; un derecho al "libre desarrollo de la personalidad en las actuales condiciones de procesamiento de datos personales que implica la protección del individuo frente a una ilimitada recolección, archivo, uso y transmisión de sus datos personales"[15]

El derecho de autodeterminación informativa se comprende aquí como la prerrogativa individual sobre la publicación y uso de datos personales propios, que genera una obligación de protección frente a una recolección y tratamiento indiscriminado de los mismos. Este derecho no se fundamenta en el derecho a la vida privada, sino, principalmente,

> "en los valores de libertad y dignidad humana en relación con el desarrollo de la personalidad".

Según esta sentencia, el tratamiento automatizado de datos de carácter personal podía

> "repercutir en (la) libertad de decidir en la medida en que el individuo no sabe lo que los terceros conocen de él y en tanto en cuanto, siendo conocedores de información acerca de su persona, ellos sí pueden prever su decisión".

Es decir: el alto grado de predicción de las conductas y decisiones de los ciudadanos, que hoy es posible conseguir gracias al cruce de una cantidad inmensa de datos personales recabados en Internet, limitaría de forma considerable la libertad real existente en una sociedad. De este modo, se erosionaría el núcleo del sistema democrático, fundado sobre el reconocimiento de la libertad de los ciudadanos (cfr. Martínez Martínez, Ricardo, 2004: p. 242). El caso del técnico informático Edward Snowden, ha puesto sobre la mesa –entre otras cuestiones- la capacidad de la *NSA* (Agencia Americana de Seguridad) de recolectar datos personales de millones de

---

13 Lorenzo Cotino Hueso (2011: pp. 396-399) hace una aportación sobre las posibles soluciones a estos conflictos entre derechos.

14 Han estudiado esta sentencia, entre otros, Gerrit Hornung y Christoph Schnabel, "Data protection in Germany I: The population census decision and the right to informational self-determination", Computer Law & Security Report, Vol.25, n 1, 2009; Antonio Enrique Pérez Luño, "La defensa del ciudadano y la protección de datos", Revista Vasca de Administración Pública 14(1986) pp.43-55; David H., Flaherty, *Protection pirvacy in surveillance societies. The Federal Republic of Germany, Sweden, France, Canada and The United States* (2 ed., North Carolina Press, Chappel Hill 1992) pp. 46 y ss.; y Ricardo Martínez Martínez, *Una aproximación crítica a la autodeterminación informativa* (Thompson-Civitas, Madrid 2004) p. 241.

15 Traducción a partir de la que hace del original alemán Flaherty, op.cit.

usuarios de Internet a través del programa *PRISM*, mediante la entrada directa a los grandes proveedores de servicios de telecomunicaciones y de la red: *Yahoo, Google, Facebook, Youtube, Skype, AOL y Apple*[16].

En España, el Tribunal Constitucional reconoció por primera vez el derecho de autodeterminación informativa en la Sentencia 292/2000, en la que declaró inconstitucionales varios incisos de los artículos 21.1 y 24.1 y 2, de la Ley Orgánica 15/1999 de "Protección de Datos Personales", considerando que vulneraban el derecho a la intimidad, ya que permitían las cesiones de datos entre Administraciones públicas para fines distintos a los que motivaron su recogida; y, además, en el momento de recabar los datos, no era necesario para la Administración informar al ciudadano de que esa cesión podía darse. Tal como señala la sentencia se trataría de un nuevo derecho fundamental de "autodeterminación informativa", de "libertad informática" (en atención a sentencias anteriores del mismo tribunal, como las STC 245/1993, de 20 de julio; 143/1994, de 4 de mayo; 11/1998, de 13 de enero; 94/1998 de 4 de mayo; y 202/1999, de 8 de noviembre) o simplemente "de protección de datos personales". Los casos que se habían presentado con anterioridad a éste –un recurso de inconstitucionalidad del Defensor del Pueblo por algunos incisos de artículos de la ley de 1999- habían ido desde la denegación de un Gobierno Civil –el de Guipúzcoa- a dar información a un ciudadano sobre los datos que poseía sobre su persona (STC 254/1993) a la negativa de una entidad de crédito a que un empleado cancelara sus datos médicos de un fichero informatizado de la empresa (STC 202/1999)[17].
Como señala el Tribunal Constitucional, la protección de datos personales es:

> "una forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los 'derechos de la persona'" (STC 292/2000, Fundamento jurídico 4), pero es "también, 'en sí mismo, un derecho o libertad fundamental'" (STC 292/2000, Fundamento jurídico, n. 4).

Es un derecho:

> que se diferencia del "derecho a la intimidad del artículo 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar" (STC 292/2000, Fundamento jurídico 6).

La peculiaridad del derecho a la protección de datos consiste en su distinta función, que es garantizar a los individuos un poder de disposición sobre esos datos (cfr. STC 291/2000, Fundamento jurídico 6) y no tanto lo que caracteriza al derecho fundamental a la intimidad: "proteger frente a cualquier invasión que pueda realizarse en aquél ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad" (STC 292/2000, Fundamento jurídico 6).

Sin embargo, como apuntan Rapahel Gellert y Serge Gutwirth (2013: p. 522), no siempre funciona la distinción entre el derecho a la protección de datos y el derecho a la vida privada, puesto que, aunque la regulación europea –sobre todo la Directiva 94/46/EC de Protección de Datos y el borrador actual de 2013 del Reglamento de Protección de Datos- así lo considere, el hecho de que el Convenio Europeo de Derechos Humanos sólo contenga en su artículo 8 la referencia al derecho a la vida privada, ha significado que el Tribunal Europeo de Derechos

---

[16] Ver "The Guadian"6 junio 2013 en http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data con acceso 25 febrero 2014.
[17] Estudia esta sentencia Concepción Conde Ortíz La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad, Dykinson, Madrid, 2005 accesible en http://app.vlex.com/#/vid/291636 con acceso 5 marzo de 2014

Humanos haya resuelto casos relativos a protección de datos bajo el paraguas del derecho a la vida privada.

7. DERECHO AL OLVIDO Y A LA AUTODETERMINACIÓN INFORMATIVA EN LA NUEVA PROPUESTA DE REGLAMENTO SOBRE DATOS PERSONALES

El derecho al olvido está incluído en el borrador del nuevo Reglamento de la Unión Europea de Protección de Datos Personales, norma que actualizará la Directiva europea de 1995. Su objetivo es lograr una mayor uniformidad en la protección de datos entre los Estados Miembros, algo que no se ha conseguido hasta el momento. Al contrario, se tiene la experiencia de la dificultad de aplicación armonizada de la Directiva 95/46/EC (Paul De Hert y Vagelis Papakonstantinou, 2012: p. 131). Otras de las finalidades del Reglamento propuesto son: una mejor protección frente a amenazas que no existían en los años 90 y el incremento de la vigilancia sobre los controladores de datos no europeos (Meg Leta Ambrosse, 2013: p. 9).

Entre la versión del borrador, aprobada por la Comisión Europea en enero de 2012, y la versión consolidada de octubre de 2013, el derecho al olvido ha sufrido un rebajamiento considerable de su intensidad garantista, hasta el punto de desaparecer incluso del título del artículo 17. El escepticismo que había suscitado la formulación inicial, así como las críticas acerca del reconocimiento del derecho de obtener el borrado sobre datos transferidos a terceras partes o que se habían autorizado transferir a terceras partes han tenido su efecto. En apariencia, con la nueva redacción de octubre de 2013, se equilibraría mejor el derecho al olvido con otros derechos humanos. Yendo al análisis del texto:
El artículo 17, *"Right to erasure",* contempla, en primer lugar, el derecho de cada persona a obtener del controlador de datos el borrado de sus datos personales, de forma inmediata, cuando,
- no sean ya necesarios para el propósito para el que fueron recogidos y tratados;
- el sujeto de los datos retire el consentimiento
-un tribunal o autoridad reguladora establecidos en Europa determine de forma definitiva que el dato debe ser borrado; o
-que el dato ha sido procesado ilícitamente.

Sólo en casos excepcionales se permitirá al controlador retener y no borrar los datos:

a. Para la defensa del derecho a la libertad de expresión de acuerdo con el art. 80
b. Por razones de interés público en el área de salud pública, de acuerdo con el art. 81;
c. Para finalidades de investigación histórica, estadística y científica, de acuerdo con el art. 83(el cual, en cualquier caso, requiere que cualquier dato personal se conserve de forma separa del resto de información bajo los más altos estándares técnicos);
d. Por cumplimiento de obligación legal de conservación;
e. Cuando la retención de datos personales es necesaria para el cumplimiento de un contrato
f. Los datos deben mantenerse con finalidades de prueba; o
g. El tipo particular de tecnología de almacenamiento no permite la eliminación y haya sido instalado con anterioridad a que el Reglamento entre en vigor

   En el caso de f y g, el controlador de datos debe restringir el procesamiento de los datos personales, de manera que los datos retenidos no están sujetos al acceso y a las operaciones de procesamiento normales, sino sólo retenidos para finalidades específicas.

Constituirían facultades del derecho al olvido, aunque no se menciona en el texto como tal, la obligación de borrado inmediato de datos personales de los servidores en internet del controlador, foros, comunidades, plataformas, etc. Sin embargo, se ha eliminado la obligación general de dar los pasos razonables para informar a terceras partes que procesen datos publicados (sería el caso de motores de búsqueda a quienes se permite rastrear redes sociales) acerca de su obligación de eliminar links, copias o replicaciones de datos personales. Sólo cuando no hay justificación legal para la publicación de datos permanece la obligación de informar (por ejemplo si no hay consentimiento para la publicación de los datos). Con todo, esta fórmula contenida en la versión consolidada del borrador del Reglamento es un reconocimiento del derecho al olvido. El hecho de que se evite darle este nombre es más una cesión a las acciones de lobby de las grandes empresas estadounidense de Internet que un cambio sustancial en la política de la Comisión Europea al respecto.

8. CONCLUSIONES

El derecho al olvido europeo se plantea como un conjunto de posibilidades de acción de los ciudadanos para eliminar sus datos personales en Internet siempre que se cumplan una serie de condiciones establecidas por ley. Tales facultades quedarían aún por delimitar pero estarían centradas en la facultad de borrar los datos, aunque contemplarían otras como la facultad de obtener del controlador de datos la abstención de continuar con su diseminación, así como de obtener de terceras partes el borrado de cualquier enlace a los mismos, o copia o replicación de tales datos, tal y como contempla el art. 17 del borrador del nuevo Reglamento de protección de datos. Su objeto es garantizar un marco de libertad para el individuo en la vida social en unas circunstancias, como las de la Sociedad de la Información, en la que existe, por una parte, un alto grado de predicción de conductas y decisiones de los ciudadanos y, por otra, una accesibilidad universal a datos personales, precisamente por la inmensa capacidad existente de recolección, tratamiento y difusión de datos. La temporalidad sería una de las claves para preservar el derecho, de forma que la accesibilidad de datos en función de plazos determinara una cierta proporcionalidad con respecto a la limitación de otros derechos en juego, como el derecho a la información. Pero junto al establecimiento de unos tiempos y la articulación de unas posibilidades de acción, el horizonte del derecho al olvido debe de tener en cuenta también soluciones tecnológicas. En la actualidad, las iniciativas englobadas en la *Digital Ephemerality* facilitan tanto la desaparición de perfiles personales de Internet como el diseño de la propia identidad digital.

9. BIBLIOGRAFÍA

Ardia, D. (2010), Reputation in a Networked World: Revisiting the Social foundations of Defamation Law. *Havard Law Review*, 45.

Ausloos, J. (2012),The Right to be Forgotten, a Worth remembering? *Computer Law & Security Review*, 28.

Bennett, S. (2012) The 'Right to Be Forgotten': Reconciling EU and US Perspectives. *Berkeley Journal of International Law*, 30, (1).

Conde Ortíz, C. (2005) *La protección de datos personales: un derecho autónomo con base en los conceptos de intimidad y privacidad*, Madrid: Dykinson. Recuperado el 5 de marzo de 2014 en http://app.vlex.com/#/vid/291636

Corbett, S. (2013), The retention of personal information online: A call for international regulation of privacy law. *Computer Law & Security review* , 29.

Cotino Hueso,L. (2011) La colisión del derecho a la protección de datos personales y las libertades informativas en la red: pautas generales y particulares de solución en Cotino Hueso, L. (ed) *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenzas y garantías*, Valencia: Publicacions de la Universitat de València, pp.. 386-401.

De Hert, P., y Vagelis Papakonstantinou, V. (2012), The proposed data protection Regulation replacing Directive 95/46/EC, A sound system for the protection of individuals. *Computer law & Security review*, 28.

Flaherty, D.(1992) *Protection privacy in surveillance societies. The Federal Republic of Germany, Sweden, France, Canada and The United States* (2 ed.), Chappel Hill: North Carolina Press.

Gellert, R. y Gutwirht, S. (2013) The legal construction of privacy and data protection computer. *Computer Law & Security Review*, 29.

Gonçalves, M.E. y Andrade, I. (2013) Security policies and the weakining of personal data protection in the European Union. *Computer&Security review*, 29, pp. 255-263.

Hornung, G. y Christoph Schnabel, Ch. (2009) Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Report*, 25, (1).

Leta Ambrose, M. (2013) A digital Dark Age and the Right to be forgotten. *Journal of Intenet Law*, 17, (3).

Mantelero, A. (2013), The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Securty Review*, 29.

Martínez Martínez, R. (2004) *Una aproximación crítica a la autodeterminación informativa*, Madrid: Thomposon-Civitas.

Pérez Luño,A.E. (1986), La defensa del ciudadano y la protección de datos. *Revista Vasca de Administración Pública*, 14.

Artemi Rallo Lombarte, A. (2010) El derecho al olvido y su protección. A partir de la protección de datos. *Telos: Cuadernos de comunicación e innovación*, 85. Recuperado el 7 de marzo 2014 en http://telos.fundaciontelefonica.com/seccion=1268&idioma=es_ES&id=2010110416500001&activo=6.do

Jeffrey Rosen, J. (2012), The Right to be Forgotten. *Stanford Law Review online*, 64. Recuperado el 3 de marzo 2014 http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten

Simon Castellano, P. (2012), *El régimen constitucional del derecho al olvido digital*. Valencia: Agencia Española de Protección de Datos y Tirant lo Blanch.

Simon Castellano, P. (2012), El derecho al olvido en el universo 2.0., *Bid* 28. DOI: 10.1344/105.000001808 Recuerpado el 4 de marzo 2014 en http://bid.ub.edu/28/simon2.htm

Tene, O. (2011), Privacy: the new generations. *International Data Privacy Law*, 1, (1).

Troncoso Reigada, A. (2012), El derecho al olvido en Internet a la luz de la propuesta de reglamento general de protección de datos personales de la Unión Europea. *Revista de Derecho, comunicaciones y Nuevas Tecnologías*, 8.

Troncoso Reigada, A. (2013) Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. *Revista de Internet, Derecho y Política*, 16.

FORMA DE CITAR:
Azurmendi, A, Derecho de autodeterminación informativa y el Derecho al Olvido: la Generación "Google" del derecho a la vida privada, en AA.VV. (2014). *Internet, Derecho y Política. Una década de transformaciones*. Actas del X Congreso Internacional, Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona 3-4 Julio, 2014. Barcelona: UOC-Huygens Editorial