EL "DERECHO AL OLVIDO" CONTRA LA MUERTE DE LA PRIVACIDAD[1]

The "right to be forgotten" against the privacy's death

POR: DR. RAMÓN M. ORZA LINARES
Profesor Contratado Doctor de Derecho Constitucional
Universidad de Granada (España)
rorza@ugr.es

RESUMEN: El nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, cuya entrada en vigor está prevista para el próximo 25 de mayo de 2018, reconoce, por primera vez, un "derecho de supresión –el derecho al olvido" por el que los ciudadanos tendrán derecho a obtener de los responsables de las páginas web la supresión de sus datos personales cuando ya no sean necesarios en relación a los fines para los que fueron recogidos o tratado, cuando revoque el consentimiento otorgado previamente, su tratamiento sea ilícito, o simplemente se oponga a su tratamiento si no prevalecen otros motivos legítimos para su mantenimiento. Aunque aún se discute su efectividad, en la actualidad disponemos de la experiencia obtenida de la aplicación de la Sentencia de 13 de mayo de 2014 del Tribunal de Justicia de la Unión Europea, *caso Google vs. AEPD y Mario Costeja*, en el que se establecía la obligación para los buscadores de internet de no mostrar los resultados que supusieran mostrar datos privados de los interesados que lo hubieran solicitado previamente. Aunque es pronto para obtener conclusiones relevantes, es indudable que el "derecho al olvido" puede ser una importante herramienta para garantizar la vida privada, en un contexto de crecientes amenazas para la misma, desde instancias tanto públicas como privadas.

PALABRAS CLAVE: Constitución, Unión Europea, Protección de Datos, Derecho al Olvido, Google.

ABSTRACT: The new Regulation (EU) 2016/679 of The European Parliament and of The Council, whose entry into force is scheduled for 25 May 2018, recognizes, for the first time, a "right of suppression - the right to be forgotten". The fact that the citizens will have the right to obtain from the web pages' responsibles the suppression of their personal data when they are no longer necessary in relation to the purposes for which they were collected or treated, when it revokes the consent previously granted, when the

[1] Este trabajo forma parte del número 12 de la REJP. Dicho número ha sido coordinado por el Prof. Dr. Francisco Bombillar Sáenz. El Consejo de redacción de la Revista aceptó la coordinación del numero indicado así como el contenido del mismo en la sesión que celebró el 21 de diciembre de 2015. El contenido de la versión final de los trabajos incluidos en este número se recibió el 24 de abril de 2017. Tras analizar el contenido de cada una de las contribuciones que lo conforman, los miembros del Consejo de redacción de la Revista dieron el visto bueno al contenido de este número en una sesión extraordinaria celebrada el 16 de mayo de 2017.

treatment is unlawful, or when it simply opposes its treatment if other legitimate grounds for its maintenance do not prevail it before. Although its effectiveness is still discussed, we now have the experience gained from the application of the European Court of Justice's Judgment of May 13, 2014, in the *case of Google vs. AEPD and Mario Costeja*, which established the obligation for Internet search engines not to show the results that supposed to expose private data of the interested parties who had previously requested it. Although it is too early to consider relevant conclusions, there is no doubt that the "right to be forgotten" can be an important tool to guarantee privacy, in a context of increasing threats, from public and private institutions.
KEYWORDS: Constitution, European Union, Data Protection, the Right to be forgotten, Google.

I.- INTRODUCCIÓN. INTERNET Y LA PRIVACIDAD

Recientemente, Tim Bernes-Lee, el creador de la World Wide Web, publicó una carta en The Guardian -con motivo del veintiocho aniversario de su creación- en la que, entre otras cuestiones, manifestaba que "hemos perdido el control de nuestros datos personales"[2], cediendo su control a corporaciones privadas y a los gobiernos. Ello lleva, en opinión de este investigador, a no poder acceder a nuestros datos personales, ni podemos decidir qué hacer con ellos, a quien cedérselos, cuáles de esos datos queremos compartir o, en fin, para qué se utilizan. Por otro lado, los gobiernos pueden perseguir a opositores, espiar las opiniones y restringir la libertad de expresión.

En esta línea, la Cámara de Representantes de los Estados Unidos ratificó el pasado 28 de marzo una ley impulsada por el Senado que permite a los proveedores de internet comercializar los historiales de búsqueda de los usuarios[3], lo que posiblemente abra una

[2] BERNERS-LEE, T.; "Here are three things we need to change to save it", The Guardian, 12-03-2017, https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet (08/04/2017). Entre otras distinciones Sir Timothy ("Tim") John Bernes-Lee, recibió en 2002 el Premio Príncipe de Asturias de Investigación Científica y Técnica, junto a Lawrence Roberts, Robert Kahn y Vinton Cerf, "por haber diseñado y realizado un sistema [Internet] que está cambiando el mundo al ofrecer posibilidades antes impensables para el progreso científico y social", según el acta del jurado.

[3] S.J.Res.34 - A joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services" , esta modificación ha entrado en vigor, tras ser firmada por el Presidente Trump, el 3 de abril de 2017, https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34 (08/04/2017)

puerta para la futura comercialización legal de todos nuestros datos de navegación o personales que obren en poder de las empresas.

Estas recientes decisiones van a continuar facilitando el paulatino control de la actividad de internet (páginas web, y sobre todo, redes sociales) que comenzó tras el grave atentado del 11 de septiembre de 2001 contra las Torres Gemelas y el Pentágono. Y ello sin aludir necesariamente a prácticas ilegales.

Así, la conmoción que produjeron esos atentados llevó a la inmediata aprobación de la USA Patriot Act, el 21 de octubre de 2001[4], aunque su validez se limitaba, en principio, hasta el 31 de diciembre de 2005. Este plazo de caducidad fue ampliado finalmente, introduciendo ligeras variaciones en su regulación, hasta que el 1 de Junio de 2015 fue sustituida por la actual USA Freedon Act, firmada por el Presidente Obama.

Entre las medidas más polémicas que contemplaba la Patriot Act se encontraban las de ampliar las facilidades para la interceptación y rastreo de las comunicaciones electrónicas, pudiendo las distintas agencias gubernamentales relacionadas con la seguridad a los datos de las comunicaciones, que debían ser almacenados durante 180 días, y retrasando las notificaciones a los afectados por las investigaciones. Además, cuando se estuvieren investigando intrusiones informáticas no era necesario contar con autorización judicial para interceptar las comunicaciones del presunto "hacker".

También permitía la existencia de mandatos para entrada y registros secretos, ya fuera física o virtualmente, sin dejar rastro evidente, aunque con obligación de informar al Tribunal que lo autorizó.

En fin, entre otros aspectos, también permitía emitir órdenes judiciales que omitieran describir los instrumentos, instalaciones o lugares vigilados, cuando se pensara que tal información pudiere frustrar la investigación en curso, entre otras facilidades.

Aunque parecía que la nueva administración del Presidente Barak Obama quería derogar el Patriot Act o, al menos, sus artículos más polémicos, lo cierto es que en febrero de 2010 el Congreso norteamericano amplío su cobertura un año más y que el 26 de mayo de 2011 firmó una extensión por cuatro años de tres artículos de esta ley: la que permitía las escuchas telefónicas itinerantes, la búsqueda de registros de negocios y la vigilancia de los individuos sospechosos de actividades terroristas no vinculados a grupos ("lobos solitarios").

Finalmente, el 2 de junio de 2015, esta normativa fue sustituida por la USA Freedom Act, actualmente en vigor, que limita algunos de los poderes que la anterior regulación otorgaba a la administración norteamericana, en especial a la Agencia de Seguridad Nacional (NSA).

[4] El USA Patrio Act fue aprobado por una abrumadora mayoría de los congresistas norteamericanos. Concretamente en el Senado, sólo hubo un voto en contra y un senador que no votó, mientras que en la Cámara de Representantes la mayoría fue de 357 votos a favor, 66 en contra y 9 no votaron. El texto de esta norma puede consultarse en https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (02/04/2017)

Concretamente, se estableció que los datos de las llamadas telefónicas no fueran recolectados por la NSA, sino por las propias compañías telefónicas, aunque a esos datos podría acceder la NSA a través de una orden judicial con características especiales.

Así, la orden tendrá que ser firmada por un «Tribunal de Supervisión de Inteligencia Extranjera», formado por once jueces, que desde 2001 son nombrados por el Presidente del Tribunal Supremo, que deberá decidir si la petición se ajusta a Derecho. La labor de este Tribunal ha sido fuertemente criticada[5], especialmente cuando se conoció que el 25 de abril de 2013 había emitido una orden, firmada por el juez Roger Vinson, que obligaba a la operadora de telefonía Verizon a que facilitara información de manera continua, y a diario, a la NSA, de todas las llamadas de teléfono efectuadas por sus clientes, y de sus metadatos, tanto dentro de los EEUU como a otros países, incluyendo llamadas telefónicas locales[6].

Además, la nueva regulación contemplada en la USA Freedom Act no afecta a la capacidad de los Estados Unidos para interceptar comunicaciones fuera de sus fronteras, que no necesita de ninguna clase de autorización adicional.

Todo ello ha llevado a que la labor en todos estos años de la NSA haya sido fuertemente criticada, especialmente a partir de la divulgación de los datos recolectados por Edward Snowden[7], siendo muy cuestionada la eficacia de la labor de esta Agencia[8].

También en Gran Bretaña entro en vigor el 30 de diciembre de 2016 la Investigatory

[5] Sin embargo la actuación de este Tribunal también está sujeta a polémica, ya que de las 24.082 solicitudes de autorización solicitadas por la NSA (entre los años 2001 y 2015), sólo 720 fueron modificadas y únicamente 12 fueron rechazadas. Los datos están obtenidos del Electronic Privacy Information Center (Cfr. https://epic.org/privacy/surveillance/fisa/stats/default.html [Consulta: 20 de septiembre de 2016]). La página web de la Foreign Intelligence Surveillance Court es: http://www.fisc.uscourts.gov/ (02/04/2017)

[6] Véase la información emitida por el diario The Guardian en su página web: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (02/04/2017)

[7] Se trataría de la filtración de una serie de documentos entre 2013 y 2015, extraídos por E. Snowden, que en conjunto superarían los 1,7 millones, además de miles de documentos secretos de las agencias de inteligencia de Estados Unidos, también contendrían miles de archivos secretos de países como Australia, Canadá o Reino Unido, gracias a su acceso a la exclusiva red Five Eyes, y los que tuvo acceso por su trabajo para Booz Allen Hamilton, uno de los mayores contratistas militares y de inteligencia del gobierno de Estados Unidos. Las primeras filtraciones fueron publicadas el cinco y el seis de junio de 2013 por los diarios The Guardian y The Washington Post y en España, por el diario El País Cfr. http://internacional.elpais.com/internacional/2013/06/07/actualidad/1370564066_752776.html (02/04/2017).

[8] Incluso el Parlamento Europeo se ha manifestado en varias ocasiones en contra del espionaje masivo a ciudadanos europeos realizados por las agencias de seguridad norteamericanas. Así, el 12 de marzo de 2014 el Pleno aprobó con 544 votos a favor, el informe realizado por la Comisión de Libertades Públicas denominado "US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs". Véase: http://www.europarl.europa.eu/news/es/news-room/20140307IPR38203/ee.uu.-debe-poner-fin-al-espionaje-masivo-o-afrontar-las-consecuencias y para el texto completo: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230 (02/04/2017).

Powers Act 2016[9]. Esta ley obliga a las empresas a almacenar los datos (incluidas todas las páginas que se visitan por los ciudadanos) durante un plazo de 12 meses. El gobierno podrá hackear dispositivos, redes y servidores y acceder a los datos de las personas incluso si sobre ellas no pesa ninguna sospecha de delito. Además, también podrá obligar a las empresas tecnológicas a hackear los dispositivos de sus usuarios para ayudar a los servicios de seguridad a acceder a sus datos. Se permite también acceder a los metadatos (fechas, duración, números de teléfono) de las conversaciones mantenidas por los ciudadanos con periodistas, abogados o médicos, protegidas actualmente por el secreto profesional.

En la Unión Europea, la desconfianza de las autoridades por el uso que los ciudadanos pudieran estar haciendo de internet llevó a la aprobación de la Directiva 2006/24/CE, que modificaba la anterior Directiva 2002/58/CE, en la que se establecía la obligación de los proveedores de acceso a internet de conservar los datos generados en las trasmisiones electrónicas.

Así, el artículo 1 de esta Directiva establecía, en su apartado 1, la obligación de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones de conservar determinados datos generados o tratados por los mismos, «para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro», y en su apartado 2, que los citados datos son concretamente «los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado», pero no «se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas»[10].

El periodo de conservación de tales datos era en una horquilla que iba desde los seis meses, como mínimo, a los dos años como máximo (Artículo 6).

Esta Directiva, sin embargo, fue anulada, en sus aspectos más polémicos, por el Tribunal de Justicia de la Unión Europea en su Sentencia de 8 de abril de 2014[11].

No obstante, las consecuencias de esta anulación todavía no se han trasladado a la legislación española, a pesar del tiempo transcurrido desde su publicación. De hecho, en España, la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones[12], todavía vigente, fue aprobada con posterioridad a la fecha de la Sentencia del TJUE, y sobre las obligaciones de conservación de los datos, mantiene, en su artículo 42, la regulación que

[9] http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf (08/04/2017)
[10] Artículo 1 de la Directiva 2006/24/CE. Concretamente, en el artículo 5 se pormenorizan los datos que necesitan ser conservados. Además, en el apartado 2 de este artículo 5 se enfatiza de nuevo que «De conformidad con la presente Directiva, no podrá conservarse ningún dato que revele el contenido de la comunicación».
[11] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 8 de abril de 2014. Asunto "*Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y KärntnerLandesregierung y otros", dictada por Petición de Decisión Prejudicial de High Court - Irlanda, Verfassungsgerichtshof – Austria*.
[12] El texto de la Ley se puede consultar en https://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-4950

sobre esta materia contenía la Ley 25/2007, de 18 de octubre[13]. De hecho, la única modificación que ha tenido desde su aprobación, ha sido la obligada por la STC 20/2016, de 4 de febrero, que anuló parte de su artículo 34. Concretamente, la Ley 25/2007, establecía que la duración de la conservación de los datos fuera de doce meses[14]. A ello debemos sumar que el rango de datos que se debe conservar por las compañías de telecomunicaciones es muy amplio.

Tras los atentados de Francia en noviembre de 2015, la preocupación por garantizar la seguridad de los ciudadanos europeos fue manifestada por los miembros del Consejo Europeo en Bruselas en su reunión de 17 y 18 de diciembre de 2015, y que se plasmaron en la acelerada aprobación de una propuesta de Directiva para poner en marcha un Registro de Nombre de Pasajeros (PNR) de compañías aéreas, justificada por la necesidad de prevenir delitos graves y, especialmente, de naturaleza terrorista.

Este Registro fue finalmente creado por la Directiva (UE) 2016/681, de 27 de abril de 2016[15]. Esta Directiva fue aprobada por el Parlamento Europeo por 461 votos a favor, 179 en contra y 9 abstenciones. La disposición prevé un plazo de dos años para que los distintos países incorporen esta normativa a su ordenamiento interno. En la actualidad, y mientras transcurre este plazo de dos años, se mantiene la obligación de las compañías aéreas de comunicar a las autoridades competentes de la Unión Europea los datos de información anticipada sobre pasajeros (API), que incluyen el número y tipo de documento de viaje que se ha utilizado, la nacionalidad, el nombre y apellidos completos, la fecha de nacimiento, el puesto fronterizo de entrada, el código del transporte, los horarios de salida llegada, el número de pasajeros y el lugar de embarque inicial.

Con la aprobación de esta nueva Directiva, los datos recopilados por las compañías aéreas y que deben ser comunicados a las autoridades, van a ser más completos –en el sentido apuntado más arriba- y además deben ser entregadas entre 24 y 48 horas antes de la hora programada para el vuelo e inmediatamente después del cierre del vuelo, nada más terminar el embarque, cuando todos los pasajeros están a bordo, el avión se dispone a despegar y es imposible subir o bajar de avión (artículo 8.3 de la Directiva)[16]. Todos los países deberán, asimismo, crear una Unidad de Información de Pasajeros (art. 4 de la Directiva), que recopilará todos estos datos y que deberá conservarlo durante cinco años, aunque deben despersonalizarse pasados seis meses, de forma que el interesado de ser identificado inmediatamente (artículo 12 de la Directiva), siendo la encargada de compartir los datos con los otros países y con las autoridades competentes

[13] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, modificada por la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. Su texto se puede consultar en https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243 (02/04/2017).

[14] Artículo 5 de la Ley 25/2007

[15] Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. El texto se puede consultar en: http://www.boe.es/doue/2016/119/L00132-00149.pdf (02/04/2017).

[16] La relación de datos que deben suministrar las compañías aéreas están indicados en el Anexo I de la Directiva.

en caso de que sea necesario para prevenir o investigar acciones terroristas o los delitos graves recogidos en el Anexo II de la Directiva (pertenencia a organización delictiva, trata de seres humanos, explotación sexual de niños y pornografía infantil, tráfico ilícito de estupefaciente y sustancias psicotrópicas, tráfico ilícito de armas, corrupción, blanqueo del producto del delito y falsificación de monedas, delitos informáticos/ciberdelincuencia, fraude, espionaje industrial, homicidio, violación y secuestro, detención ilegal, toma de rehenes, tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte, etc.)[17].

En relación a las cautelas que suscitan estas nuevas regulaciones, destaca la manifestada por el Consejo de Europa que ya ha mostrado su preocupación por esta Directiva, y apunta algunos aspectos que deberían ser contemplados para considerar a este Registro como respetuoso en relación a la protección de datos[18]. También Joe Cannataci, encargado del derecho a la privacidad de la ONU ha criticado la Investigatory Powers Act 2016 en el sentido de señalar que va contra la jurisprudencia del Tribunal Europeo de Derechos Humanos y que "menosprecia el espíritu del derecho fundamental a la privacidad"[19]

Por lo que se refiere al ámbito de las empresas, el panorama no es tampoco muy alentador. A pesar de que la regla general es la del consentimiento de los interesados para poder recabar y tratar datos personales, lo cierto es que, cada vez con mayor intensidad, son más diversos y numerosos los datos personales que se vierten a la red. Es más, en muchas ocasiones, el ciudadano ni siquiera es consciente de que está suministrando datos personales en muchas de las actividades que realiza cuando utiliza el correo electrónico, los motores de búsqueda o la simple navegación.

Aunque formalmente tales páginas piden ese consentimiento, a la hora de utilizar distintas redes sociales o de instalar apps en sus dispositivos móviles, a través de una página inicial en la que se deben aceptar distintos términos y condiciones de uso o la utilización por la aplicación de datos internos de esos dispositivos móviles (número de teléfono, de contactos, de ubicación, etc.), lo cierto es que tales términos y condiciones están escrito en un lenguaje excesivamente técnico o incluso críptico, que impide la correcta compresión de su significado o se refieren a una legislación ajena a la del país en la que se encuentra el usuario.

[17] Un análisis más exhaustivo de esta Directiva y de otras regulaciones sobre la privacidad en la Unión Europea se puede consultar en ORZA LINARES, R. M.; "La defensa de la privacidad en la era de la ciberseguridad". Actas del II Congreso Internacional de Estudios Militares, Granada, octubre 2016, en prensa.

[18] COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL (T-PD) "Avis sur les implications en matière de protection des données du traitement des dossiers passagers" Estrasburgo, 19 de agosto de 2016, http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2016)18rev%20Avis%20PNR_Fr.pdf (04/04/2017)

[19] El texto de las críticas se puede consultar en el CANNATACI, J.; "First anual report", de 8 de marzo de 2016, http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc (04/04/2017)

Por lo demás, las condiciones se ofrecen sin posibilidad de ser matizadas por sus usuarios que sólo tienen la opción de aceptarlas o rechazarlas en bloque -y ya conocemos los abundantes problemas derivados de los contratos de adhesión-. Por último, y no es un problema menor, tampoco existen controles fiables para que los menores de edad no estén aceptando -y por lo tanto, contratando- condiciones y términos legales que ni entienden ni están autorizados a suscribir. De hecho, en la mayoría de las legislaciones de los países, se establece como edad del consentimiento la de 16 años, aunque no se establecen métodos o técnicas para comprobar la exactitud de ese dato.

Por otro lado, las grandes corporaciones que explotan sitios como «Microsoft», «Apple», «Google» «Yahoo» o «Facebook», por citar las más conocidas, suelen situar sus sedes en Estados Unidos, dónde las regulaciones estatales de protección de datos de los usuarios suelen tener una menor intensidad que, por ejemplo, en la Unión Europea. Además, en relación a la protección del anonimato, se observa una tendencia creciente a buscar datos reales de las personas que utilizan las redes sociales. No es sólo que una persona ceda voluntariamente sus datos, sino que se establecen controles y cruces de información con otros usuarios para comprobar que los datos que se introducen son reales, pertenecen a personas físicas identificables a los que, además, se les incita de muy diversas maneras, a seguir incluyendo información de carácter personal (profesión, nombres de los cónyuges, edad, sexo, lugar de residencia, centros de enseñanzas, aficiones, gustos literarios y musicales, etc.). Y a todo ello se le suma la posibilidad de vincular fotografías y vídeos personales. De hecho, recientemente, «Facebook» ha adquirido a la empresa de mensajería instantánea «Whatsapp» y lo primero que hizo fue realizar un cruce entre los perfiles de los usuarios de «Facebook» y los números de teléfono y nombres de la aplicación de mensajería. Solo tras las advertencias de las autoridades de protección de datos europeas, se introdujo una opción para que fuera cada usuario el que decidiera si podían cruzarse sus datos contenidos en estas dos aplicaciones[20]. De hecho, usar las ventajas de estas aplicaciones y servicios implica –en todo caso- ceder parte de nuestra privacidad.

Como vemos, podemos encontramos con una exposición absoluta de la intimidad personal. De hecho la exposición pública a la que se someten muchos ciudadanos puede darnos la impresión de que la protección de la vida privada ya no importa tanto y que el ataque combinado contra la misma tanto desde instancias públicas como empresariales pueda suponer la "muerte" del derecho a la privacidad[21]. Es más, se ha llegado a apuntar

[20] Sin embargo, ello no impide que esa información pueda seguir siendo usada para otros propósitos. Así en las condiciones de servicio de aceptación obligada para utilizar esta aplicación de mensajería se señala que "Facebook y la familia de empresas de Facebook recibirán y usarán esta información para otros propósitos. Esto incluye ayudar a mejorar los sistemas de infraestructura y entrega; entender cómo se usan nuestros Servicios o los de ellos; proteger los sistemas; y combatir las actividades infractoras, el abuso o los mensajes no solicitados". Y en la "familia Facebook" se encuentran también Instagram, Oculus u Onavo, aplicaciones que, incluso, puede que no estemos utilizando.

[21] Tim O'Reilly ha manifestado que la privacidad "técnicamente" ha muerto (http://www.abc.es/20111123/sociedad/abcp-privacidad-muerto-20111123.html) y Mark Zuckerberg ha manifestado también en diversas entrevistas que "la privacidad está muerta" (http://www.abc.es/20100111/medios-redes-web/facebook-zuckerberg-privacidad-201001111438.html y también http://es.digitaltrends.com/internet/la-privacidad-esta-muerta-dice-mark-zuckerberg-incluso-

que si alguien desea proteger al máximo su vida privada, debe salir de internet, renunciar al correo electrónico y no utilizar ni smartphones ni tablets[22].

Además las amenazas a nuevas formas de invasión de la privacidad son cada vez más crecientes, y no provienen sólo de internet o de las redes sociales, sino de ataques perpetrados a la intimidad por la proliferación de cámaras de video vigilancia tanto en manos privadas como públicas o de tecnologías como las de reconocimiento facial que han avanzado mucho en los últimos años.

II.- EL DERECHO AL OLVIDO

En toda esta descripción que hemos realizado en las páginas anteriores, que parecen construir un mundo donde los ciudadanos cada vez están más controlados y más expuestos, la aparición de nuevos derechos como el "derecho al olvido" va a ir en una dirección totalmente contraria.

En efecto se trata de crear instrumentos jurídicos a disposición de los particulares para que éstos puedan recuperar el control de sus vidas, de sus datos privados, muchas veces recabados y tratados sin su conocimiento y en contra de su voluntad. El derecho al olvido surge, pues, como una derivación, de los viejos de derechos de acceso, rectificación, cancelación y oposición que venían siendo reconocidos por las legislaciones de protección de datos de los diversos países en relación con los bancos de datos informatizados. No obstante, su conceptualización posee unas características propias que lo distinguen de los anteriores y que le permiten adaptarse a las nuevas exigencias y tecnologías de la sociedad de la información.

1.- ANTECEDENTES

De hecho, la intención y la posibilidad de borrar nuestro pasado ha estado presente en las preocupaciones de las personas, de modo persistente, a lo largo de la historia. Así se suelen describir tanto en la literatura como en la vida real los esfuerzos realizados para alejarse o borrar el pasado, sobre todo si éste le era perjudicial[23].

En cualquier caso, desde un punto de vista jurisdiccional, se suele citar como antecedente más remoto del "derecho al olvido", en 1931, el caso *Melvin v. Reid* que se resolvió en la Corte de California. Se trataba de un asunto en el que la víctima, tras un

---

para-su-hija-que-es-esta-por-nacer/) o que la norma social ha evolucionado a lo largo del tiempo y "la gente se siente realmente cómoda no sólo compartiendo información de diferente tipo sino de forma más abierta y con más gente" (http://www.periodistadigital.com/tecnologia/internet/2010/01/11/fundador-facebook-gente-no-quiere-privacidad.shtml) (11-04-2017).

[22] PASCUAL, A.; ¿Privacidad? ¡No existe la privacidad!, El Confidencial, 12 de noviembre de 2013, http://blogs.elconfidencial.com/tecnologia/loading/2013-11-12/privacidad-no-existe-la-privacidad_53255/ (17-04-2017).

[23] Uno de los destinos tradicionales era alistarse en la Legión Extranjera Francesa o cuerpos similares (La Legión, en España, ahora exige certificado de antecedentes penales). Cfr. http://www.cambiandoelrumbo.com/index.php/alistarse-en-la-legion-extranjera-como-se-alistan-los-legionarios-cambiando-su-propia-vida-incluso-la-identidad/ (04/04/2017)

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 olvidados[24].

Más recientemente, con la aparición de los primeros ordenadores y las bases de datos, y tras los primeros estudios llevados a cabo por el Consejo de Europa[25], una primera respuesta legal a esta persistencia de los datos, fue la creación de los derechos de acceso, rectificación, cancelación y oposición en relación con la recolección y tratamiento de los datos personales que pudieran constar en las bases de datos públicas o privadas[26].

Desde esta regulación, el derecho al olvido podía hacerse coincidir simplemente con el derecho de cancelación de los datos[27], 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 van a ser excluidas de la regulación general y suelen presentar numerosas dificultades a la hora de cancelar o, simplemente, de rectificar los datos recogidos[28].

[24] Cfr. https://casetext.com/case/melvin-v-reid (04-04-2017)

[25]El Consejo de Europa ya en 1967 crea una comisión con la finalidad de estudiar el conflicto entre la privacidad y el uso de informática. De sus trabajos surge en 1968 su Resolución 509 de la Asamblea del Consejo sobre "los derechos humanos y los nuevos logros científicos y técnicos". También en 1973 y 1974 se aprueban otras dos Resoluciones sobre protección de la vida privada frente a los bancos de datos. Un resumen de la actividad del Consejo de Europa en estas materias se puede consultar en http://www.dhnet.org.br/dados/cursos/edh/interdisciplinario/ddhh549.htm (10/04/2017). Ya en 1981 se aprueba el Convenio núm. 108 del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respeto al tratamiento automatizado de los datos de carácter personal (fue ratificado por España el 27 de enero de 1984). Entró en vigor el 1 de octubre de 1985, tras cinco ratificaciones, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (11/04/2017).

[26]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, Mª L.; *La información de las Entidades de Crédito. Estudio especial de los informes comerciales bancarios* Valencia ,Ed. Tirant lo Blanch, 2000; Dubié, P. "Protección de datos y derecho al olvido", Derecho de los negocios, 2003, nº 14, Nº 154-155, págs. 1-16

[27]Garriga Domínguez, Ana (2004) *Tratamiento de datos personales y derechos fundamentales.* Madrid, Dykinson, , pág. 40

[28] 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 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"*, lo cierto es que esta cuestión es difícil de controlar por cuanto en 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"*.

Con internet esta pervivencia del pasado se ha reforzado hasta extremos inimaginables años antes. 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 original[29]. Y todo ello en un tiempo extremadamente corto, incluso simultáneamente.

Y este problema no sólo afecta a las personas individuales implicadas, sino también a las empresas (por ejemplos, 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 cuándo se publicaron[30]. Pero, sin embargo, al ser recuperados por los buscadores, aparecen registrados de manera inmediata, poniéndolos de nuevo de actualidad.

En la vida real, como contrapuesta a la vida virtual, este problema ya había 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 penales[31].

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".*

[29] 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 (18/04/2017)

[30]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.

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

Por ello, podemos concluir que este derecho debería entenderse como el derecho de las personas a impedir que datos personales propios circulen por internet sin su consentimiento. Las razones pueden ser muy variadas, pero en lo que se refiere a datos cuyo conocimiento pueda perjudicar a las personas, de lo que se trata, como ha señalado Pere Simón recientemente, es de tener la posibilidad de «equivocarse y volver a empezar»[32]. Es más, ya el propio Tribunal Constitucional en una sentencia de 1999 señalaba que "el art. 18.1 [Constitución Española] garantiza... un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos"[33].

2.- LAS PRIMERAS RESOLUCIONES QUE AFECTAN AL "DERECHO AL OLVIDO" EN ESPAÑA

En este estado de cosas, la Agencia de Protección de Datos española comenzó a analizar los problemas derivados de la persistencia de las informaciones en internet ya hace diez años a partir de la primera denuncia presentada por un ciudadano el 19 de marzo 2007.

En aquel asunto, la Agencia Española de Protección de Datos, en su Resolución de fecha 9 de julio de 2007 -reafirmada tras el recurso de reposición del recurrente, el día 10 de septiembre de 2007[34]- analizó la incidencia que las noticias antiguas publicadas en las páginas web de los diarios, pudieran tener en los derechos de los recurrentes. Así:

- Por un lado, la Agencia de Protección de Datos consideraba que la publicación de informaciones relevantes y veraces entra dentro del ejercicio legítimo del derecho a la información y, por lo tanto, su publicación fue 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.
- Por otro, en lo que se refiere a la publicación en internet de las noticias a través de la puesta a disposición de los internautas del archivo o hemeroteca del periódico, la Agencia también consideró 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.
- Pero, finalmente, por lo que respecta a la responsabilidad concreta del buscador

[32] SIMÓN CASTELLANO, P.; "El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos", Ponencia presentada en el Congreso *Libertad, transparencia y política en Internet: ejercicio, amenazas y garantías*. Madrid, Centro de Estudios Políticos y Constitucionales, 2012. Su monografía *El Régimen Constitucional del Derecho al Olvido Digital* (Ed. Tirant Lo Blanc, Valencia, 2012) es también de obligada consulta.

[33] STC 144/1999, de 22 de julio, fundamento jurídico 8. http://hj.tribunalconstitucional.es/es/Resolucion/Show/3886 (10-04-2017). Lo que también nos remite a un posible "derecho al anonimato" para cuyo análisis podemos citar a ORZA LINARES, R.; "El derecho al anonimato en la red", Telos, núm. 89, oct-dic, 2011, págs. 24-33. STC 144/1999, de 22 de julio, fundamento jurídico 8. http://hj.tribunalconstitucional.es/es/Resolucion/Show/3886 (10-04-2017).

[34]El texto de estas Resoluciones, se pueden consultar en las siguientes direcciones electrónicas: http://www.agpd.es/portalwebAGPD/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: http://www.agpd.es/portalwebAGPD/resoluciones/recursos_reposicion/rr_sobre_tutela_de_derechos/common/pdfs/REPOSICION-TD-00299-2007_Resolucion-de-fecha-10-09-2007_Art-ii-culo-16-LOPD.pdf (17-04-2017).

> Google (directamente denunciado también), como servicio de intermediación, la Agencia, en ésa y otras Resoluciones del año 2007, consideraba que tampoco tenían 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, en base a 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 servicios[35].

Un par de años más tarde, sin embargo, el criterio de la Agencia, en relación con los buscadores, cambió radicalmente, considerándolos a éstos a partir de entonces como responsables de los datos que tratan.

De hecho, en una Resolución de 26 de enero de 2009, consideró 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, era responsable y, por lo tanto debía evitar que los datos personales del recurrente pudieran recuperarse cuando se utilizara el mencionado buscador[36].

En esta última resolución, la Agencia realizó una serie de reflexiones sobre el hecho de que los periódicos volcaran en la red su hemeroteca. Considera así 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

[35] 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: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2009/common/pdfs/TD-01164-2008_Resolucion-de-fecha-26-01-2009_Art-ii-culo-17-LOPD_Recurrida.pdf (17-04-2017). Este cambio de criterio venía anunciado desde antes. Así, ya en diciembre de 2007, la Agencia publicó una "Declaración sobre buscadores de Internet" donde recogía ampliamente su razonamiento sobre la responsabilidad de los buscadores en el tratamiento de los datos personales de las personas físicas, en tanto que también eran responsable de su tratamiento. Su texto completo se puede consultar en https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/declaracion_aepd_buscadores.pdf (17-04-2017).

[36] 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 la información (la del periódico), éste buscador no refleje ese resultado en sus búsquedas, pero sí lo pudieran seguir haciendo otros como Yahoo, Bing, Ask o cualquier otro que no hubiera sido afectado por la decisión de la Agencia.

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"[37].

Esta línea de actuación, que pasa por obligar a los buscadores, o al menos a los buscadores que son denunciados, a que impidan la presentación de datos personales de los ciudadanos en sus resultados de búsquedas, fue confirmada en numerosas Resoluciones de la Agencia[38], incluso cuando esos datos vinieran de fuentes oficiales[39].

[37] 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.

[38] 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 http://www.agpd.es/portalwebAGPD/resultados-ides-idphp.php , aunque el buscador que utilizan es sumamente confuso (17-04-2017).
Un análisis exhaustivo de las resoluciones de la Agencia Española de Protección de Datos puede encontrarse también en ORZA LINARES, R. y RUÍZ TARRÍAS, S.; "El derecho al olvido en Internet", Neutralidad de la red y otros retos para el futuro de Internet, Universitat Oberta de Cataluny y Ed. Huygens, Barcelona, 2011. Págs. 371-389 (el texto, disponible en pdf, se puede obtener en http://goo.gl/bs4kO) (10-04-2017)

[39] Curiosamente, sin embargo, la Resolución de 20 de octubre de 2011, que se refería a datos que aparecían publicados en la página web del Boletín Oficial del Estado, también establecía la obligación para la propia página web oficial de atender la solicitud de cancelación presentada por el ciudadano: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-00689-2011_Resolucion-de-fecha-20-10-2011_Art-ii-culo-16-LOPD.pdf (17-04-2017). Sin embargo, la Resolución de 30 de julio de 2010, procedimiento TD/00299/2010, sólo obligaba a Google a ignorar la información contenida en el Boletín Oficial de la Comunidad de Madrid. http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00299-2010_Resolucion-de-fecha-30-07-2010_Art-ii-culo-34-RD-1720-b-2007_Recurrida.pdf En el mismo sentido, la Resolución de 30 de julio de 2010, procedimiento TD/00336/2010, en relación con el otorgamiento de indulto al reclamante y su publicación en el Boletín Oficial del Estado. http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00299-2010_Resolucion-de-fecha-30-07-2010_Art-ii-culo-34-RD-1720-b-2007_Recurrida.pdf (10-04-2017).

Concretamente, en relación con los datos publicados por el Boletín Oficial del Estado (BOE), la Agencia, en una significativa Resolución, la dictada el 28 de agosto de 2012 en el que se analiza una reclamación de un ciudadano contra la publicación en el B.O.E. de sus datos a propósito de la concesión de un indulto, señaló en un muy interesante razonamiento que el BOE "al publicar en su página web los datos personales de ciudadanos, está realizando un tratamiento de datos total o parcialmente automatizado; y ello aunque exista una obligación legal de publicar determinados actos administrativos y de que sea considerado una fuente de acceso público", ello no le exime –según la legislación vigente en materia de protección de datos de carácter personal- "de adoptar las medidas necesarias, y adecuadas según el estado actual de la tecnología, para evitar la indexación de los datos personales del reclamante en sus páginas, con objeto de que en el futuro los motores de búsqueda de internet no puedan asociarlas a él y con ello se impida la divulgación de manera indiscriminada de sus datos personales".

Por ello, la Agencia considera que "si bien el ciudadano no puede oponerse al mantenimiento en el Boletín Oficial de sus datos de carácter personal, al resultar éste perfectamente legítimo por encontrarse amparado en la Ley que ordena la publicación de los Reales Decretos de indulto, sí puede sin embargo el ciudadano oponerse -en los casos en que exista un motivo legítimo y fundado en el sentido previsto en el artículo 6.4 de la LOPD- a que sus datos personales sean objeto de tratamiento previniendo su posible captación por los buscadores de Internet o dicho de otra forma, obstaculizando una cesión para el tratamiento por los mismos por los responsables de dichos motores de búsqueda"[40].

Y el estado actual de la tecnología a la que se refiere la Agencia, en la actualidad consiste en la utilización de un fichero denominado *robots.txt* que se inserta en el archivo que se sube a la página web y que recoge los datos que los buscadores no deben indexar a la hora de rastrear las páginas webs.

Pero la utilización de esos ficheros por el BOE tampoco es pacífica. De hecho, el Boletín utilizó hasta 2010, pero luego dejo de hacerlo, por lo que todo lo que aparecía en el Boletín fue indexado y clasificado por los buscadores. La Agencia se ocupó de ello y, en una Resolución de fecha 23 de noviembre de 2011 indicó que "La AEPD entiende que, en el actual estado de la tecnología -al margen de las mejoras técnicas que quepa introducir sobrevenidamente (sic.)- la adopción del protocolo de la industria denominado "robots.txt" es un método válido para atender las solicitudes de los ciudadanos que, de acuerdo con lo previsto en el Capitulo IV del Título III del Reglamento de desarrollo de la LOPD han ejercitado su derecho de cancelación o de oposición ante un boletín o diario oficial, al considerar que existen motivos que justifican la cesación del tratamiento consistente en permitir la indexación de sus datos publicados en una determinada edición". De hecho, el BOE comunicó a la Agencia que

[40] Resolución de 29 de agosto de 2012. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-01018-2012_Resolucion-de-fecha-29-08-2012_Art-ii-culo-34-RD-1720-b-2007.pdf (10-04-2017).

volvía a utilizar esos ficheros para que los buscadores no indexaran los datos que aparecían allí[41]

En cualquier caso, esto es una solución parcial, ya que en nuestro país existen numerosos Boletines Oficiales (uno por cada Comunidad Autónoma, uno por cada provincia, etc.) que están faltos de una regulación común y donde cada uno ofrece soluciones distintas y, además, en la actualidad los buscadores han empezado a ofrecer en sus resultados de búsquedas algunos de los datos que, en teoría no hubieran podido obtener, de acuerdo con el contenidos en esos ficheros *robots.txt*[42].

Esta línea de actuación de la Agencia Española de Protección de Datos le llevó a abrir más de un centenar de procedimientos contra el buscador "Google", hasta 2009, en el que le instaba a eliminar de sus resultados de búsquedas los datos correspondientes a los reclamantes, tanto de páginas web privadas como oficiales.

Finalmente, "Google Spain S.L." recurrió una de éstas resoluciones ante la Audiencia Nacional por cuanto consideraba que la responsabilidad de mantener esos datos accesibles al público era 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, dictó una Providencia de fecha 22 de febrero de 2011 en el que la Sala de lo Contencioso Administrativo (Secc. 1) de la Audiencia Nacional acordaba 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 definitiva, la cuestión prejudicial presentada por nuestra Audiencia Nacional podían resumirse en tres cuestiones: la aplicación territorial de la legislación de protección de datos, si la actividad de los buscadores como "proveedores de contenidos" de internet podría ser considerada como "tratamiento de datos personales" y el alcance de los derechos de cancelación y oposición en relación con las informaciones personales publicadas en páginas web.

3.- La Sentencia de 13 de mayo de 2014 del Tribunal de Justicia de la Unión Europea, *caso Google vs. AEPD y Mario Costeja*

[41] Resolución de fecha 23 de noviembre de 2011. Disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-00950-2011_Resolucion-de-fecha-23-11-2011_Art-ii-culo-34-RD-1720-b-2007.pdf (10-04-2017).

[42] En la siguiente página web puede consultarse su fichero *robots.txt*: http://www.boe.es/robots.txt, en que se señalar todo el contenido que no debe aparecer en los buscadores (10-04-2017).

Llevada la cuestión prejudicial al Tribunal de Justicia de la Unión Europea (TJUE), éste dictó Sentencia el 13 de mayo de 2014[43].
Tal y como se describe en la misma, en este procedimiento se trataba de dilucidar si la responsabilidad de eliminar unos datos que un ciudadano, Mario Costeja González, consideraba lesivos para su honor era responsabilidad de la página web en la constaban los mismos –propiedad de un diario- o del buscador. Concretamente se trataba de que, cuando un internauta introducía su nombre en el buscador de Google, éste mostraba como resultado de esa búsqueda dos anuncios aparecidos en el diario "La Vanguardia", de 19 de enero y de 9 de marzo de 1998, respetivamente, en los que figuraba la subasta de unos inmuebles suyos embargados por deudas a la Seguridad Social. El Sr. Costeja afirmaba en su reclamación ante la Agencia, que tales deudas y embargos con la Seguridad Social estaban totalmente solucionados y resueltos desde hacía años y era una información que, en aquellos momentos, carecía totalmente de relevancia.

Fruto de una reclamación presentada el 5 de marzo de 2010, la Agencia de Protección de Datos española, como en otros asuntos similares anteriores, ordenó a Google, en su Resolución de fecha 30 de julio de 2010[44], que no mostrara en el futuro esta información, por cuanto consideraba que no era posible eliminar la información original que constaba en la hemeroteca que el mencionado diario había volcado en la red. Google, por el contrario, sostenía que la responsabilidad de la información recaía en exclusiva sobre el propietario de la página web original y que su buscador era simplemente un mediador sin responsabilidad en el contenido de las páginas web que indexaba. Google señalaba por lo tanto que ni era responsable de los datos, ni ejercía control sobre los mismos ni era responsable de su tratamiento.

En virtud de la cuestión prejudicial presentada por la Audiencia Nacional se incoó el correspondiente procedimiento en el Tribunal de Justicia de la Unión Europea para interpretar el alcance de los artículos 2, letras b) y d), 4, apartado 1, letras a) y c), 12, letra b) y 14, párrafo primero, letra a) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.
Las partes del litigio fueron, por un lado, Google Spain, S.L. y Google Inc. y, por otro, la Agencia Española de Protección de Datos y el Sr. Costeja González.

---

[43] Sentencia del Tribunal de Justicia de la Unión Europea (gran Sala) de 13 de mayo de 2014 Asunto C-131/12 Google Spain, S.L., Google Inc. contra Agencia Española de Protección de Datos (AEPD), Mario Costeja González (Petición de decisión prejudicial planteada por la Audiencia Nacional). El texto íntegro de la Sentencia se puede consultar en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=269153
También está disponible las Conclusiones del Abogado General Sr. Niilo Jääskinen, presentadas el 25 de junio de 2013, cuyas conclusiones estaban más cercanas a las tesis defendidas por Google, http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=ES . (10-04-2017).

[44] Resolución de fecha 30 de julio de 2010, procedimiento TD/00650/2010. El texto íntegro de la resolución se puede consultar en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00650-2010_Resolucion-de-fecha-30-07-2010_Art-ii-culo-16-LOPD_Recurrida.pdf (10/04/2017).

En resumen, se trataba de dilucidar si la resolución administrativa de la Agencia Española de Protección de Datos por la que, estimando parcialmente la reclamación presentada por el Sr. Costeja González, se requería a Google para que no mostrara las informaciones referidas anteriormente que afectaban al reclamante en relación al anuncio que aparecía en la página web del diario "La Vanguardia", era respetuosa con lo regulado tanto en la Directiva de protección de datos, como en la Carta de los Derechos Fundamentales de la UE. Por otro lado, la Agencia rechazó la pretensión del Sr. Costeja de obligar al mencionado diario para que modificara la información que aparecía en su hemeroteca.

Tras un exhaustivo análisis de las características de los motores de búsqueda el Tribunal de Justicia de la Unión Europea concluyó que:

- El artículo 2, letras b) y d), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que la actividad de un motor de búsqueda, que consiste en hallar información publicada o subida en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de "tratamiento de datos personales", en el sentido del mencionado artículo 2 letra d).
- Por lo tanto, el gestor de un motor de búsqueda es "responsable" de dicho tratamiento a los efectos del artículo 2, letra d) de la mencionada Directiva.
- Como quiera que el gestor del motor de búsqueda mantiene en algún Estado miembro una sucursal o filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro, la legislación aplicable a la protección de datos es la vigente en la Unión Europea, tal como dispone el artículo 4, apartado 1, letra a) de la Directiva.
- En virtud de ello, el gestor del motor de búsqueda está obligado a eliminar de la lista de resultados obtenidas, a partir de la búsqueda efectuada de un nombre de una persona, los vínculos a páginas web publicadas por terceros y que contengan información relativa a esa persona, incluso aunque esa información no se borre previa o simultáneamente de esas páginas web. E, incluso, si la publicación de tales datos personales sea en sí misma lícita o venga obligada por la legislación del Estado miembro o no cause perjuicio al interesado.
- Los derechos a la intimidad y protección de datos prevalecen, en principio, sobre los intereses económicos del gestor del motor de búsqueda y sobre el derecho de los ciudadanos a acceder a la información disponible y lícita, salvo en casos de existencia de un interés público.
- Este interés público puede venir dado por que el interesado haya desempeñado un papel relevante en la vida pública o el acceso a la información esté justificado por el interés público, lo que justificaría un interés preponderante del público en tener, a raíz de ello, acceso a la información de que se trate.
- Corresponde por lo tanto, a los gestores de los motores de búsqueda la responsabilidad de examinar si los interesados tienen derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual,

vinculada a su nombre en la lista de resultados obtenida en la búsqueda (según disponen los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46), una vez que hayan ejercido sus derechos de cancelación u oposición.

- De hecho, el derecho al olvido no es un mecanismo de "borrado automático". Solo procederá cuando se justifique la necesidad de dicho borrado conforme a los criterios de la normativa sobre protección de datos. No se trata, por tanto, de imponer al prestador de servicios una obligación general de supervisar los datos que trasmitan o almacenen.

Aunque la Sentencia en general fue recibida como un decidido avance en la protección de los datos personales en relación a las informaciones publicadas en internet, hubo también algunas voces críticas con tal decisión. Tales razones aludían a la nueva obligación que se establecía para los gestores de búsquedas de internet, mientras se mantenía la información original en las páginas web. Para estos autores, se trataría sólo de incidir sobre las herramientas de acceso a la información, pero no al hecho de la existencia de la información misma.

Con tal decisión, si bien se podía dificultar el acceso a determinadas informaciones, no por ello se imposibilitaba totalmente. Bastaría con acudir a las páginas web originales dónde esa información seguiría estando presente. Esto es especialmente fácil en las páginas web oficiales cuyo sentido es, por lo demás, hacer públicas determinadas informaciones. Es más, lo único que ordenaba la Sentencia es que no se mostraran enlaces concretos entre los resultados cuando se hiciera una búsqueda específicamente por el nombre del interesado, pero ello no afectaría a la persistencia de los datos ni a los resultados de la búsqueda si se utilizaban otras palabras distintas a las del propio nombre y apellidos de la persona en cuestión. De hecho, Yahoo advierte sobre la posibilidad de que distintas personas puedan tener el mismo nombre y apellidos, por lo que señala que los "los resultados de Yahoo Search con contenido sobre otra persona que comparta tu mismo nombre, no estarán sujetos a cambios o eliminaciones"[45]

También se ha apuntado la posibilidad de que este tipo de resoluciones pudieran reforzar a los gobiernos represivos que buscaran restringir la libertad de expresión en internet.

Finalmente, la Audiencia Nacional (Sala de lo Contencioso Administrativo) en su Sentencia de 29 de diciembre de 2014[46], puso fin al procedimiento inicial, aplicando la Sentencia del Tribunal de Justicia, acordando la desestimación de los recursos contencioso-administrativos interpuestos por Google, y declarando por lo tanto las Resoluciones de la Agencia Española de Protección de Datos como conformes a derecho.

---

[45] YAHOO; Ayuda: Eliminación de resultados de búsqueda de Yahoo Search, en https://es.ayuda.yahoo.com/kb/search-for-desktop/Eliminaci%C3%B3n-de-resultados-de-b%C3%BAsqueda-de-Yahoo-Search-sln4530.html?impressions=true (17-04-2017)

[46] Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional 5129/2014, de 29 de diciembre de 2014. El texto íntegro de esta sentencia se puede consultar en http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=7260043&links=%22725%2F2010%22&optimize=20150126&publicinterface=true (17/04/2017)

A partir de estas resoluciones jurisdiccionales Google –y también Yahoo y Bing- pusieron en marcha páginas web en la que los ciudadanos europeos podían solicitar a los buscadores que no se mostraran en los resultados de búsqueda datos personales vinculados a su nombre.

Por ello, para que Google, por ejemplo, atienda nuestra petición de no encontrar informaciones que nos resulten perjudiciales, debemos solicitarlo a través de un formulario web en el que se nos pide que ofrezcamos a esa empresa un elenco de datos y elementos de verificación de los mismos[47]. A partir de ahí y tras un examen de nuestra solicitud, un "comité de expertos"[48] nombrados por Google valoraría si la solicitud se refería a datos irrelevantes, obsoletos o inaceptables, y, en consecuencia, la aceptaría. En tal caso, para el futuro, en los resultados de búsqueda no se mostrarían tales datos personales o informaciones, siempre que en la misma se utilizaran específicamente el nombre y los apellidos del solicitante.

III.- LA REGULACIÓN DEL DERECHO AL OLVIDO EN LA UNIÓN EUROPEA

Las tesis establecidas en la Sentencia del TJUE, han sido recogidas en el actual Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), publicado en el Diario Oficial de la Unión Europea de fecha 4 de mayo de 2016[49]. No obstante no comenzará a aplicarse hasta el 25 de mayo de 2018, mientras tanto seguirán vigentes las disposiciones actuales en relación a la protección de datos que haya en cada país miembro de la Unión Europea.

Junto a esta norma se ha publicado también la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de

[47] El formulario que debe rellenarse se encuentra en la dirección https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=es. Para el buscador BING: https://www.bing.com/webmaster/tools/eu-privacy-request y para Yahoo, https://io.help.yahoo.com/contact/index?y=PROD_SRCH&token=w5FCchB1dWGbc2RE0kcjij0u65u86GoeqUkmqtTbcuO%2BLU%2FUQgc3BzwNZtXp6XEXn5YwJ6Wu6A9MCYnw7SzQy5BySKiGUpoj0xug9Sr7JfZdSQjOyA5v2Of2mZTMotlsehDS1xQqu1g%3D&locale=es_ES&page=contactform&selectedChannel=email-icon&isVip=false (02/04/2017)

[48] El Comité de Expertos de Google en relación con el derecho al olvido está compuesto por Luciano Floridi, Sylvie Kauffmann, Lidia Kolucka-Zuk, Frank La Rue, José Luís Piñar, Sabine Leutheusser-Schnarrenberger, Peggy Valcke, Jimmy Wales, Eric Schmidt y David C. Drummond. Más información en https://www.google.com/intl/es/advisorycouncil/ (17-04-2017).

[49] El texto completo del Reglamento se puede obtener en: https://www.boe.es/doue/2016/119/L00001-00088.pdf (17-04-2017).

dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[50].

Centrándonos en el Reglamento, el tema que nos ocupa viene tratado en su artículo 17 bajo el nombre de "Derecho de supresión ("el derecho al olvido")" (sic), señalándose lo siguiente:

> "1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:
>
> a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
> b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
> c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
> d) los datos personales hayan sido tratados ilícitamente;
> e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
> f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.
>
> 2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
>
> 3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:
>
> a) para ejercer el derecho a la libertad de expresión e información;
> b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;
> c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;
> d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado

[50] Su texto se puede obtener en: https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80808 (17-04-2017). El análisis de esta Directiva, aún siendo especialmente interesante, no será objeto de estas páginas.

1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones"

La justificación de esta regulación la ofrece el Reglamento en su Considerando 65, cuando afirma que: "Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento".

Así, continúa, "los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento".

Además, "este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se [era] plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet". No obstante, "el interesado debe poder ejercer este derecho aunque ya no sea un niño".

Sin embargo, "la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones".

En relación con la posibilidad de utilizar medidas técnicas que impidan la indexación de los datos, se señala en el Considerando 66 que "a fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos". De este modo, "al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales".

En definitiva, los ciudadanos europeos van a tener en sus manos –de hecho ya la tienen, desde mayo de 2014, a través del cumplimiento de la STJUE- la posibilidad de impedir que gran parte de sus datos personales persistan en el entorno virtual. Así, si una persona está interesada en borrar sus datos personales, en primer lugar, debería acudir a los sitios que tratan sus datos con su consentimiento o su actividad positiva, por

ejemplo, en páginas web o en redes sociales a las que haya subido contenido (Twitter, Facebook, Instagram, Snapchat, Flickr o similar), manifestando la revocación del mencionado consentimiento y la consiguiente eliminación de todo el contenido que le afecte y que esté justificado por el consentimiento original.

Seguidamente debería ponerse en contacto con los gestores o administradores de las páginas web en las que existieran datos personales o informaciones que no hubiera suministrado voluntariamente. Aquí puede encontrarse con que esos datos aparecen allí de modo ilícito o lícito. En el primer caso los datos personales deberían ser eliminados de inmediato. En el segundo caso, tendríamos la posibilidad de ejercer el derecho de supresión (olvido).

Este derecho se puede ejercer solicitando a los buscadores[51] que no vinculen el nombre y los apellidos del interesado a los datos personales que aparecen en unas concretas páginas web de modo lícito y que debemos identificar correctamente. A través de esa vía, como ya se ha apuntado en reiteradas ocasiones, no se elimina la información original, pero se dificulta su obtención. Ya no estará tan accesible al no mostrarse en los resultados la información que le afecta en caso de que alguien utilice los buscadores con el nombre y apellidos del solicitante.

En cualquier caso, es de destacar que esta decisión queda en manos de los gestores o responsables de los buscadores, aún cuando debería prosperar esa solicitud cuando la utilización de tales datos personales o información fuese obsoleta o ya no tuviera relevancia ni interés público. De todos modos debemos resaltar en este punto que la información no será suprimida ni de los índices del buscador, ni de la fuente original. Las fuentes permanecerán inalterada y el resultado se mostrará cuando la búsqueda se realice por cualquier otra palabra o término distinta al nombre del afectado.

Si, a pesar de cumplir con tales exigencias, los responsables o gestores de los buscadores no respondieran a la petición realizada o el ciudadano considerara que la respuesta que recibe no es la adecuada, puede elevar una queja a las Autoridades de protección de datos de cada país, en España, la Agencia Española de Protección de Datos, frente al responsable del tratamiento. La autoridad determinará si estima esa queja o no. Esta decisión de las Autoridades de protección de datos puede ser recurrible ante los Tribunales, en España, ante los tribunales de la jurisdicción contecioso-administrativo.

Por lo que respecta a la práctica de eliminación de contenidos por parte de los buscadores, Google ofrece algunas razones por las que decide aceptar las reclamaciones. Concretamente acepta todas aquellas solicitudes en la que se den algunas de las siguientes situaciones:

a) Ausencia clara de interés público. Así, señala, “sitios web de agregadores con páginas que contienen datos personales de contacto o direcciones, instancias en las que el nombre del solicitante ya no aparece en la página o páginas que ya no

[51] Los formularios para ejercer este derecho al olvido están disponibles sólo para los buscadores Google, Yahoo y Bing (vid. Nota 44)

están online (error 404)"

b) Información confidencial: "páginas con contenido relacionado únicamente con la salud, la orientación sexual, la raza, la etnia, la religión, la afiliación política o la pertenencia a un sindicato de una persona"
c) Contenido relacionado con menores de edad: "contenido relacionado con menores de edad o con delitos menores cometidos cuando el solicitante era menor de edad".
d) Condenas o antecedentes prescritos, exoneraciones y fallos absolutorios: en estos casos se señala que "de acuerdo con la legislación local que rige la rehabilitación de personas que han cometido un delito, tendemos a retirar el contenido relacionado con condenas que han prescrito, acusaciones que se ha demostrado que son falsas ante un tribunal, o infracciones penales de las que el solicitante fue absuelto. También tenemos en cuenta para nuestro análisis el tiempo que hace que este contenido se publicó y la naturaleza del delito"[52].

Y, por el contrario, se suelen rechazar las peticiones cuando:

a) En opinión de Google, "existe otra fórmula [Soluciones alternativas] que permite al solicitante retirar la página de nuestros resultados de búsqueda". Así, el solicitante "podría haber publicado el contenido en un sitio web que ofrezca a los usuarios la posibilidad de evitar que su contenido aparezca en los resultados de búsqueda". En estos casos, "indicamos al solicitante la información necesaria sobre las herramientas correspondientes"
b) Cuando por motivos técnicos, como "una URL rota o incompleta", que impiden la localización exacta de la página. O cuando los solicitantes "piden también que retiremos las páginas resultantes de una consulta que no coincide con su nombre ni con el nombre de la persona a la que el solicitante dice representar".
c) URL duplicada por la misma persona: un solicitante envía varias solicitudes de eliminación de la misma página para el mismo nombre.
d) Y, por último "es posible que rechacemos una eliminación si consideramos que la página contiene información de interés público". Aunque Google reconoce que "determinar si un contenido es de interés público suele ser complicado, e implica tener en cuenta diversos factores". Los factores a los que se aluden son "que el contenido esté relacionado con la vida profesional del solicitante, con un delito pasado, con un cargo político, que trate de un personaje público, o que el contenido en sí mismo sea de autoría propia, documentos gubernamentales o material periodístico".

No obstante, debemos señalar que Google fue requerida, en septiembre de 2014, por el Tribunal de Gran Instancia de París por cuanto "las medidas adoptadas por Google cuando accede a retirar un enlace de sus resultados de búsqueda tras una reclamación basada en la normativa europea de protección de datos de carácter personal son completamente insuficientes", ya que la exclusión de los resultados solo era efectiva cuando se realizaba la búsqueda desde la versión del buscador que correspondía con el

[52] GOOGLE, "Informe de Transparencia: Privacidad de las búsquedas en Europa". En https://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=es#how_evaluate (17-04-2017).

país desde el que se había realizado la solicitud de supresión (google.es, google.fr, google.pt, etc)[53]. En el mismo sentido, la Agencia Española de Protección de Datos señalaba que la aceptación de las solicitudes de supresión debería hacerse efectiva en todas las versiones del buscador accesibles desde España[54]. Con respecto a esta cuestión, en la actualidad, según información de Google, las solicitudes de supresión de resultados aceptadas cubre la retirada de los resultados de nuestras propiedades de búsqueda, como Búsqueda de Google, Google Imágenes, Google Vídeos y Google Noticias y desde cualquier dominio del buscador, incluido Google.com[55].

Actualmente, según el propio buscador, las solicitudes recibidas desde el 29 de mayo de 2014 ascienden, en la fecha de redacción de este artículo, a 713.255 solicitudes en las que se pedía la retirada u ocultación de 2.000.321 páginas web. De este total de solicitudes ha aceptado el 43,1 por ciento y ha rechazado el 56,9 por ciento. Por lo que se refiere concretamente a España, ha recibido 57.418 solicitudes que ha llevado a analizar a 170.809 páginas. De ellas ha admitido sólo el 38 por ciento, mientras que ha rechazado el 62 por ciento.

El país europeo que ha presentado un mayor número de solicitudes es Francia, con un total de 227.318 solicitudes y 411.918 páginas analizadas. Hasta este momento, ha aceptado el 48,7 por ciento de las solicitudes y ha rechazado al restante 51,3 por ciento.

Un ejemplo de solicitud recibida desde Francia se refiere a "un cura condenado por posesión de pornografía infantil [que] nos pidió que retirásemos los artículos en los que se informa de su sentencia y expulsión de la iglesia". Google rechazó su solicitud. Desde Bélgica "una persona nos solicitó que retirásemos un enlace que llevaba a un artículo sobre un concurso en el que participó cuando era menor de edad". Esta solicitud si fue aceptada[56].

IV.- ALGUNAS CONSIDERACIONES FINALES SOBRE EL "DERECHO AL OLVIDO"

De todo lo anterior, podemos extraer algunas consideraciones finales sobre este "derecho al olvido". La primera que debemos resaltar es, si bien la STJUE suscitó críticas y existía una suspicacia generalizada sobre la posibilidad de que pudiera llevarse a cabo tal decisión, lo cierto es que con la colaboración de Google y de otros buscadores

[53] Ordonnance de référé du 16 septembre 2014, https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-du-16-septembre-2014/ (17-04-2017)
[54] Resolución de 2 de diciembre de 2015, Procedimiento E/02887/2015, Fundamento de Derecho III, in fine (http://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2015/common/pdfs/E-02887-2015_Resolucion-de-fecha-02-12-2015_Art-ii-culo-34-RD-1720-b-2007.pdf) (17-04-2017)
[55] GOOGLE; Informe de transparencia: Preguntas frecuentes, en https://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=es#does_this_ruling_also_apply (17-04-2017).
[56] Datos obtenidos de https://www.google.com/transparencyreport/removals/europeprivacy/ (17-04-2017). En esta página se puede encontrar interesante información adicional sobre las solicitudes.

no directamente afectados por esa decisión, pero que también se sumaron a este propósito, la implementación de las páginas web de solicitud y la aceptación de un destacado número de solicitudes ha permitido comprobar que se ha reforzado la eficacia del derecho a la intimidad y la protección de los datos personales de los interesados.

Ello, no obstante, no debe hacernos pasar por alto que, aunque Google sea el principal buscador en idioma español[57], existen otros muchos buscadores que no se sienten afectados ni por esa decisión del TJUE ni por la regulación de la Unión Europea. Entre ellos podemos citar a Baidu, motor de búsqueda líder en idioma chino, pero que permite realizar búsquedas en otros idiomas, o Yandex que es el primer buscador en ruso. También podemos citar a Ask, Aol, Altavista, Duckduckgo, entre otros. Además existen serias dudas que la regulación que pueda estar vigente en la Unión Europea pueda imponerse a empresas o buscadores de otros países. Aceptar sencillamente esta tesis puede llevar a que tuvieran que ser directamente aplicables en la Unión Europea regulaciones o resoluciones judiciales de otros países (Corea del Norte, China, etc.) o que ello pudiera obligar a empresas europeas que quisieran operar en ellos.

También puede resultar preocupante que, a través de la recepción de las solicitudes, los buscadores pueden –a la vez- ir construyendo una interesante base de datos, con datos privados y, en muchas ocasiones, sensibles, de cuyo control nada se sabe. Si bien no hay datos de su utilización por estas compañías hasta ahora, nada hace pensar que más adelantes puedan comercializar de algún modo con esa información de tanta calidad y acreditada por los propios interesados, como la que están recibiendo. De hecho, estas compañías son de capital privado, poseen ánimo de lucro, y su domicilio social se sitúa en los Estados Unidos, dónde estas regulaciones son, y pueden serlo aún más en el futuro, mucho más flexibles que en la Unión Europea.

En cualquier caso, a la hora de utilizar el derecho al olvido, habría que tener en cuenta que éste se puede ejercer:

1. Frente a los titulares de la página web dónde aparecen los datos personales. Los responsables del tratamiento de la información en origen, los responsables de su publicación, tienen la posibilidad retirar una información de su página o modificarla, o de incluir códigos de exclusión que restringen el indexado de la misma. Así mismo, pueden discutir frente al afectado, que pretende ejercer su derecho de cancelación u oposición, la licitud del dato, la existencia de consentimiento, la actualidad y proporcionalidad de la información y finalmente la invocación de otros derechos que puedan entrar en colisión con los del afectado que pretende su cancelación, pues inevitablemente se produce una confrontación entre los derechos del afectado a ejercer un control sobre el tratamiento y difusión de sus datos personales y el interés perseguido en su difusión y los derechos que asisten al que los ha introducido, en donde adquieren especial relevancia, los derechos de libertad de expresión e información.

[57] Con una penetración del 96 %, seguido de Bing (datos de septiembre de 2013), http://www.rivassanti.net/posicionamiento-web/listado-de-buscadores-mas-usados-en-espanol/ (14-04-2017)

Pero la responsabilidad del editor no garantiza la solución a todos los problemas, pues no evita que los datos personales hayan sido replicados en otras páginas, lo que convertiría el rastreo y el contacto con todos los editores en una misión imposible. Además, el editor puede residir en un Estado tercero, y las páginas web de que se trata pueden estar excluidas del ámbito de aplicación de las normas de la Unión Europea sobre protección de datos.

2. Frente a los buscadores. En este caso, hay que solicitar la exclusión de la información vinculada al nombre y a los apellidos. Para ello debemos rellenar cuidadosamente los correspondientes formularios para cada uno de los buscadores que dan esta posibilidad –hasta la actualidad sólo Google, Bing y Yahoo-. Además debemos tener en cuenta que una de las causas para rechazar la solicitud, según indican los responsables de Google, es que el interesado no suministre la información solicitada o que esta sea inexacta, sobre todo en lo que respecta a la identificación de las páginas de las que se desea la exclusión. Asimismo debemos resaltar que la causa principal para fundamentar nuestra solicitud vendría dada –de acuerdo con lo establecido en el Reglamento de protección de datos- por el hecho de que los datos recabados ya no fueran útiles en relación con los fines para los que fueron recogidos o tratados. En todo caso, esta solicitud se puede hacer de manera simultánea a la realizada frente al titular de la página web que contiene nuestros datos.

Precisamente en relación con la obsolescencia de los datos, señala Córdova Catroverde, que "será necesario ponderar la permanencia de ese interés en el tiempo, problema que guarda una especial importancia cuando del ejercicio del "derecho olvido" se trata, pues, aun cuando la utilización de los datos pudiera estar justificada en un principio, el paso del tiempo ha podido hacerlo desaparecer". Así, para este autor, "la actualidad de la información y de los datos que incorpora puede dejar de ser relevante, desapareciendo el interés público que justificaba su inicial publicación". Y es esa pérdida de actualidad "la que resulta especialmente trascendente para acceder al derecho al olvido, dado que precisamente es el paso del tiempo y la voluntad del afectado de que determinados datos o informaciones no sigan siendo accesibles al conocimiento público, unido al hecho de la intemporalidad de los datos en internet, la que justifica el ejercicio del derecho al olvido"[58].

De hecho, como apunta Ana Azurmendi, "una vez transcurridos 10-15 años, el interés por acceder con carácter universal a los datos que se habían publicado no es idéntico al del momento de su primera publicación en origen". En esta línea, "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 en el caso objeto de la Sentencia del Tribunal de Justicia (caso «Mario Costeja») que se dé publicidad a una subasta de bienes con carácter previo a su

[58] CÓRDOVA CASTROVERDE, D. "El "derecho al olvido" tras la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014". El Derecho Revista de Jurisprudencia, núm. 1, 01-10-2014. También en http://www.elderecho.com/tribuna/administrativo/derecho_al_olvido-proteccion_de_datos_11_765430009.html (17-04-2017).

celebración", pero tal interés no se mantiene "una vez transcurridos años desde la publicación inicial". Especialmente "cuando esa accesibilidad universal ocasiona perjuicios notables, de tipo moral y económico, a las personas físicas o jurídicas nombradas"[59].

En contra de considerar el mero transcurso del tiempo como criterio para determinar la caducidad de los datos, se apuntan razones de interés público como la investigación científica, la historia, estadística, salud pública y otras que, junto con el derecho a la información, la libertad de expresión y la seguridad, abogarían por el mantenimiento de los datos originales publicados en internet[60].

En cualquier caso y para concluir, deberíamos remarcar que el derecho al olvido no es un derecho absoluto. Como otros derechos y bienes constitucionalmente protegidos, puede ceder ante otros bienes o intereses constitucionalmente relevantes, siempre que tal límite sea necesario, proporcional y respetuoso con el contenido esencial del derecho fundamental restringido[61].

Esta cuestión fue debidamente señalada en la Sentencia de la Audiencia Nacional española que aplicó la STJUE sobre el derecho al olvido, al señalar que «de la Sentencia (del TJUE) se deduce la prevalencia del derecho a la protección de datos... Ahora bien, esa prevalencia del derecho de oposición al tratamiento de los datos personales por su titular, sobre el interés legítimo del gestor del motor de búsqueda en la actividad que desarrolla, no es absoluta ni ajena a la situación personal concreta del reclamante, con la única salvedad de que la ley establezca otra cosa". Así, "al igual que la protección del derecho fundamental al respeto de la vida privada, del que la protección de datos personales constituye una manifestación autónoma, las injerencias, o límites, en este derecho pueden venir justificados cuando, previstas por la ley, constituyan una medida que en una sociedad democrática, sea necesaria para la salvaguarda de otros intereses, entre otros, la protección de los derechos y libertades de los demás, como reza el artículo 8 del Convenio Europeo de Derechos Humanos [y] como viene a reconocer, también, el artículo 52.1 y 3 de la Carta"[62].

[59] AZURMENDI, A. "Por un "derecho al olvido" para los europeos: aportaciones jurisprudenciales de la Sentencia del Tribunal de Justicia Europeo del caso *Google Spain* y su recepción por la Sentencia de la Audiencia Nacional española de 29 de diciembre de 2014", Revista de Derecho Político de la UNED, núm. 92, enero-abril de 2015, págs.297. También, en el mismo sentido RALLO LOMBARTE, A. "El derecho al olvido y su protección. A partir de la protección de datos" Telos, vol. 85 (2010).

[60] Ibídem, pág. 298. Esta autora menciona, entro otros autores, a Luís Javier Mieres: "el derecho al olvido no puede consistir en reescribir la historia, borrando algunas partes de ella"

[61] Existe una importante jurisprudencia española e internacional sobre los límites de los derechos fundamentales, cuyo análisis excede la finalidad del presente trabajo.

[62] SAN (Sala de lo Contencioso) 5129/2014, de 29 de diciembre de 2014, Fundamento de Derecho Décimo Tercero- Criterios de ponderación, ya citada