UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja

El derecho al olvido. Especial referencia al Reglamento Europeo de Protección de Datos.

Trabajo fin de máster presentado por: Laura Villuendas Martínez.

Titulación: Máster en Propiedad Intelectual y Derecho de las Nuevas Tecnologías.

Línea de investigación: Cuestiones jurídicas relativas al reconocimiento tanto a nivel normativo jurisprudencial del derecho al olvido.

Director/a: Doña Susana Checa Prieto.

Zaragoza

28 de septiembre de 2017.

Firmado por: Laura Villuendas Martínez.

CATEGORÍA TESAURO: 3.15. Derecho privado.

ÍNDICE:

AGRADECIMIENTOS

A mi familia por su apoyo incondicional.

A todos los profesores de la UNIR del Máster de Propiedad Intelectual y Derecho de las Nuevas Tecnologías.

I. RESUMEN.

El debate sobre la existencia del derecho al olvido es una de las cuestiones que, en el marco de las nuevas tecnologías, más polémica ha suscitado. El objeto del presente trabajo se centra en analizar el derecho al olvido y sus características más importantes. No debe obviarse que tradicionalmente el derecho al olvido ha sido una figura jurisprudencial, ya que hasta la aprobación del Reglamento de Protección de Datos Europeos, no se había contemplado el derecho al olvido específicamente en la normativa.

A tal efecto, en el presente trabajo haremos un análisis de las distintas Sentencias dictadas en esta materia, así como la evolución que en esta materia ha sufrido la jurisprudencia española tras la Sentencia del Tribunal de Justicia de la Unión Europea de fecha 13 de mayo de 2014, en la que se sientan las bases del derecho al olvido.

Finalmente, no podemos obviar la importancia del Reglamento de Protección de Datos, por lo que se hará en el presente trabajo una sucinta referencia a los cambios más importante que a nuestro juicio incorpora.

Palabras Clave: “Protección de Datos”, “Privacidad”, “Derecho al Olvido”, “Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016”, “libertad de información”, “motor de búsqueda”.

ABSTRACT.

The discussion of the right to oblivion existence is one of the most controversial matters within the new technology settings. The present work aims to analyze the right to oblivion and its most important characteristics. It is important to notice that this right has traditionally been a jurisprudence figure which had not been contemplated in the normative until the approval of the European Information Protection Policy.

Therefore, the present work will analyze the different sentences dictated in this subject. As well as the evolution that the Spanish jurisprudence has suffered since the sentence of the European Union Court of Law, placed on the 13th of May of 2014 where the bases of the right to oblivion were established.

Finally, the importance of the Information Protection Policy has not to be omitted. Thus, the present work will cite the most important changes of the previously mentioned right according to our opinion.

Key words: “Data Protection”, “Privacy”, “Right to be forgotten”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016”, “Freedom of information”, “Search engine”.

II. INTRODUCCIÓN.

La sociedad ha sufrido una gran revolución como consecuencia de la rápida y profunda evolución que se ha producido en el marco de las nuevas tecnologías. Evidentemente, dicha evolución ha supuesto un grave reto para los distintos ordenamientos jurídicos nacionales e internacionales que han tenido que adaptar su legislación a las nuevas necesidades que han surgido.

La principal novedad que se deriva de ello es que los datos personales de los individuos, que antes eran de difícil acceso para el resto de la sociedad, pasan a tener una accesibilidad universal y en principio ilimitada. El derecho al olvido nace como la solución a esa vulneración del derecho a la privacidad.

Inicialmente, la aparición de Internet supuso paralelamente el nacimiento de un nuevo derecho, que era el derecho a la privacidad. Evidentemente en el momento en el que surge Internet, el ordenamiento jurídico español no contemplaba tales situaciones, por lo que surgió la necesidad de dictar nuevas normas, así como de adaptar las ya existentes. En este punto, es necesario recalcar la importancia que ha tenido tanto la Agencia Española de Protección de Datos de Carácter Personal como la jurisprudencia puesto que son las que a través de sus resoluciones han ido

configurando el que ahora se conoce como derecho al olvido, contribuyendo de manera notable e incuestionable a la protección de los derechos de los ciudadanos.

En este punto hay que recalcar la Sentencia de fecha 13 de mayo de 2014 dictada por el Tribunal Superior de Justicia de la Unión Europea en el asunto C-131/12 que enfrentó a Google Spain, S.L., y Google Inc., con la Agencia Española de Protección de Datos y con Don Maro Costeja González, y en la que se produce un reconocimiento expreso del derecho al olvido.

Sin duda alguna, también contribuirá notablemente a la protección de los derechos de los ciudadanos, la implantación en todos los Estados miembros de la Unión Europea del Reglamento Europeo de Protección de Datos, lo cual además dotará de uniformidad a la aplicación del derecho al olvido en la Unión Europa, lo cual a su vez conllevará una mayor seguridad jurídica.

Si bien, el mismo está orientado principalmente a legislar el derecho al olvido respecto de los motores de búsqueda. Entendemos que por su relevancia sería muy interesante que se implantara una normativa similar en el ámbito de las redes sociales, y ello por cuanto tal y como se analizará en el apartado correspondiente, ha habido también una gran proliferación en el desarrollo de las mismas.

III. PROTECCIÓN DE DATOS: CONSIDERACIONES PREVIAS.

III.1 Marco legal de la protección de datos.

Con carácter previo a analizar el concepto y el alcance del derecho al olvido, es necesario en primer lugar analizar la regulación propia de la protección de datos que existe en nuestro ordenamiento jurídico.

Así las principales fuentes del ordenamiento jurídico español que regulan la protección de datos son la Constitución Española, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo, Ley Orgánica de Protección de Datos), el Real Decreto 1720/2007, de 21 de diciembre, por el que

se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en lo sucesivo, Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos), sin obviar el Reglamento 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 (en lo sucesivo, Reglamento general de protección de datos) que entrará en vigor en mayo del año 2018.

Pues bien, una vez que hemos visto las fuentes que regulan el derecho fundamental a la protección de datos, vamos a analizar la consideración que existe del derecho fundamental de protección de datos en la normativa española, concretamente cuál es la definición de dicho derecho que se desprende de dicho texto legal.

La Constitución Española debe ser el punto de partida a esta cuestión, y ello por cuanto es la norma suprema de nuestro ordenamiento jurídico. Así, el artículo 18.4 de la Constitución Española dispone que:

> *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

Dicho precepto ha sido objeto de un exhaustivo análisis por parte del Tribunal Constitucional, que ha venido definiendo el derecho fundamental de la protección de datos a través de una serie de Sentencias, siendo la primera de ellas la Sentencia número 254/1993[1], a partir de la cual se dictaron nuevas Sentencias cuyos fallos vinieron a confirmar esa la línea jurisprudencial iniciada por el Tribunal Constitucional en torno al derecho fundamental a la protección de datos de carácter personal.

A tal efecto es necesario precisar que nuestra Constitución es del año 1978 de tal manera que el legislador en ese momento no podía prever el papel que las nuevas tecnologías iban a tener en la sociedad española ni el alcance y efectos de las mismas,

[1] Sentencia Número 254/1993 del Tribunal Constitucional de fecha 20 de julio de 1993. (RTC 1993\254).

lo cual, como veremos a continuación, ha motivado que se haya desarrollado una jurisprudencia atendiendo al contexto social.

Respecto de la Sentencia anteriormente referenciada, vemos por lo tanto como se realiza una primera aproximación al concepto de protección de datos e igualmente una primera interpretación del artículo 18.4 de la Constitución Española. Concretamente, nuestro más alto Tribunal se pronunció en los siguientes términos:

> *Dispone el art. 18.4 CE que «la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática».*

En la Sentencia anteriormente transcrita, el Tribunal Constitucional introduce el concepto de libertad informática como un derecho fundamental independiente de otros derechos fundamentales como son el derecho a la intimidada personal y familiar. Se produce por lo tanto una bifurcación y se configura el derecho a la libertad informática como un derecho autónomo.

Especialmente ilustrativa resulta la reflexión que sobre dicho artículo realiza Miguel Ángel Davara Rodríguez [2] y que entiende que: "*Al analizar este texto cabe pensar que nuestros constitucionalistas tenían amplios conocimientos de las*

[2] Davara Rodríguez, Miguel Ángel. (1998). La relación entre los artículos 28.1 CE y 18.4 CE desde la óptica de la llamada "protección de datos personales". *Editorial Aranzadi, S.A.U., Cizur Menor.*

posibilidades de la informática, y el peligro que conlleva, en una época en la que todavía no se había producido el impacto social que trajo la entrada, casi indiscriminada, alocada e impetuosa, de los ordenadores personales, la conexión a redes mediante la moderna telemática, la «multitudinaria navegación por Internet» y las conexiones vía satélite digitalizadas; sin embargo esto no era así; no se trataba de que nuestros constitucionalistas fueran expertos informáticos, no había más que asomarse al exterior y comprobar que en todos los países de nuestro entorno socio cultural se estaba desarrollando un amplio movimiento de protección de la intimidad ante el tratamiento de datos en forma automatizada."

Vemos como el mencionado autor es consciente de que en el momento en el que se promulgó la Constitución Española el legislador no preveía el surgimiento de Internet, sino que entiende que tuvo en cuenta el contexto europeo en el que estaba surgiendo la necesidad instaurar un derecho a la intimidad en el tratamiento de datos.

Si bien como hemos puesto de manifiesto la Sentencia Número 254/1993 del Tribunal Constitucional es importante por cuanto supone una primera aproximación al derecho de protección de datos, sin duda alguna la Sentencia más relevante a nuestros efectos es la Sentencia Número 292/2000[3] ya que es en ella en la que se define el alcance del derecho fundamental a la protección de datos. Con carácter previo a analizar dicha Sentencia, es necesario poner de manifiesto que entre la primera de las Sentencias que hemos citado y la que ahora nos ocupa, se produjo un cambio sustancial y que fue nada más y nada menos que la entrada en vigor de la Ley Orgánica de Protección de Datos. Es en esta Sentencia donde se produce propiamente la configuración del derecho fundamental a la protección de datos como un derecho independiente del derecho a la intimidad, tal y como se transcribe a continuación:

> *Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar,*

[3] Sentencia Número 292/2000 del Tribunal Constitucional de fecha 20 de noviembre de 2000. (RTC 2000\292).

atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.

La Sentencia anteriormente transcrita no es solo relevante a nuestros efectos porque supone el nacimiento jurisprudencial del derecho a la protección de datos como un derecho independiente, sino que va más allá y delimita cuál es el alcance del mismo:

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y, el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que rectifique o los cancele.

Igualmente, en este punto es necesario hacer referencia a las posiciones que han mantenido a tal efecto la doctrina científica. Así, Faustino Gudín Rodríguez-Magariños[4], sobre el derecho a la intimidad se pronuncia en los siguientes términos:

> *El derecho a la intimidad es la base sobre la que podemos desplegar otros derechos más palpables como la libertad, pues sólo si elegimos, salvaguardados en el ámbito de lo arcano, podemos con propiedad desplegar nuestro querer sin tener que sopesar condicionantes de terceros ni vislumbrar una posterior represión. Se trata de un derecho fundamental esencial o primario, superlativo, por ser el primero que el individuo necesita y el último que cabe suprimir, so pena de llegar a su consideración cosificar a una persona dando por predeterminada su capacidad para elegir, negándosele, por tanto, su dignidad radical, su consideración de un ser que puede individualizar su destino.*

Finalmente, debemos hacer referencia a las circunstancias en las que se dictaron las Sentencias del Tribunal Constitucional, y que resume muy acertadamente Pablo Lucas Murillo de la Cueva[5]:

> *Ahora bien, no deja de ser significativo que tanto cuando el Tribunal Constitucional se pronuncia por vez primera sobre el derecho a la protección de datos personales, cuanto cuando, siete años más tarde, lo erige en derecho fundamental, mediaban circunstancias externas relevantes que apuntaban en la misma dirección en que acabó fallando. Así, la sentencia 254/1993 se dicta unos meses después de la entrada en vigor de la LORTAD y observa una parecida ambigüedad en lo que se refiere a la ubicación de la materia de la protección de datos en el panorama de los derechos fundamentales. Y la sentencia 292/2000 se dicta unos días antes de que se apruebe la Carta de los Derechos*

[4] Gudín Rodríguez-Magariños, Faustino. (2015). Réquiem por el derecho a la intimidad en los smartphone: análisis de la última Jurisprudencia del TC contrastada con la del TDEH. Barcelona (España). *Revista Aranzadi Doctrinal num. 9/2014.*

[5] Murillo de la Cueva, Pablo Lucas. (2010). Comentario a la ley Orgánica de Protección de Datos de Carácter Personal. *Editorial Aranzadi, S.A.U.*

Fundamentales de la Unión Europea que reconoció como derecho autónomo y distinto del derecho a la vida privada el derecho a la protección de datos y poco después de que el Tribunal Europeo de Derechos Humanos en sentencias de ese mismo año 2000, tratase ya de forma específica la protección de datos personales dentro de sus interpretaciones del artículo 8 del Convenio de Roma. Es verdad, por otro lado, que a esas alturas ya había más contribuciones doctrinales que defendían esa solución e, igualmente, es cierto que desde 1995 estaba en vigor la Directiva 95/46/CE y que la Unión Europea venía manifestando una creciente atención a los problemas de la protección de datos personales

A la vista de lo anteriormente expuesto debemos concluir que el derecho a la intimidad se configura como un derecho básico que permite el surgimiento de otros derechos íntimamente relacionados, siendo muy relevante en este escenario la Sentencia del Tribunal Constitucional Número 292/2000 fundamental ya que con la misma se produce el nacimiento formal del derecho fundamental a la protección de datos.

III.2 Principios de la protección de datos.

Los principios de la protección de datos están recogidos en los artículos 4 a 12 de la Ley Orgánica de Protección de Datos de Carácter personal, y son los siguientes:

- Calidad de los datos.
- Derecho de información en la recogida de datos.
- Consentimiento del afectado.
- Datos especialmente protegidos
- Datos relativos a la salud
- Seguridad de los datos
- Deber de secreto
- Comunicación de datos
- Acceso a los datos por cuenta de terceros

De los principios anteriormente mencionados, el principio de calidad de datos y, dentro de este, el principio de finalidad se configura como dos pilares básicos del sistema de protección de datos, por lo tanto, y dado que dichos principios son especialmente relevantes a nuestros efectos, únicamente ellos van a ser objeto de análisis al estar directamente vinculados con el derecho al olvido, que es el objeto de este trabajo.

Principio de calidad de datos: el principio de calidad de datos se encuentra contemplado en el artículo 4.1 de la Ley Orgánica de Protección de Datos que dispone que:

> *Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.*

Dicho principio, exige que los datos personales sean exactos y se encuentren actualizados, tal y como así se plasma en el apartado tercero del artículo 4 del mismo texto legal:

> *Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.*

Como no podía ser de otra manera, la jurisprudencia se ha pronunciado sobre dicho extremo. Así, la Audiencia Nacional[6] ha dispuesto que:

> *La existencia de culpabilidad resulta clara en el caso de autos por falta de diligencia de la entidad recurrente, pues lo que impone el artículo 4.3 de la LOPD, de calidad del dato, es que los datos personales recogidos en*

[6] Sentencia Número 251/2016 de la Audiencia Nacional de fecha 4 de mayo de 2016 (JUR 2016\134261).

> *cualquier fichero, sean exactos y respondan en todo momento a la situación actual de los afectados, responsabilidad que incumben a los responsables de los ficheros*

El principio de finalidad, no se encuentra como un principio expresamente contemplado en el título II de la Ley Orgánica de Protección de Datos, sino que el mismo se encuentra incluido dentro del principio de calidad de datos. Concretamente, dicho principio está plasmado en el artículo 4.2 de la Ley Orgánica de Protección de Datos que dispone que:

> *Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.*

El Tribunal Constitucional en su Sentencia Número 17/2013[7], entre otras, se ha pronunciado sobre tal principio:

> *En conclusión, tal como establece nuestra doctrina, es claro que la Ley Orgánica de protección de datos no permite la comunicación indiscriminada de datos personales entre Administraciones públicas dado que, además, estos datos están, en principio, afectos a finalidades concretas y predeterminadas que son las que motivaron su recogida y tratamiento.*

A la vista de los dos principios desarrollados podemos concluir con que los datos personales deben responder siempre a la realidad de la situación de su titular e igualmente su tratamiento debe realizarse para la finalidad para la que fueron recabados dichos datos, salvo las propias excepciones que se contemplan en la Ley Orgánica de Protección de Datos.

[7] Sentencia Número 17/2013 del Tribunal Constitucional de fecha 13 de enero de 2013 (RTC 2013\17).

Finalmente, no podemos dejar de hacer referencia en este punto al deber del obtener el consentimiento de los afectados. Salvo las excepciones contempladas en el artículo 6.2 de la Ley Orgánica de Protección de Datos existe un deber de obtener el consentimiento previo de los afectados, tal y como se así se establece en el apartado primero del artículo sexto del a Ley Orgánica de Protección de Datos:

> *El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.*

El consentimiento se configura como el elemento esencial del derecho fundamental a la protección de datos de carácter personal, tal y como así se ha pronunciado el Tribunal Constitucional[8]:

> *El consentimiento del afectado es, por tanto, el elemento definidor del sistema de protección de datos de carácter personal.*

En cuanto al consentimiento, el mismo debe ser previo, libre, inequívoco, específico e informado, tal y como así queda plasmado en la Ley Orgánica de protección de datos de carácter personal, y tal y como así queda reflejado en la jurisprudencia[9]:

> *La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal pone de manifiesto el carácter consustancial que el elemento de la información tiene con la prestación de consentimiento en relación con la disposición de los datos personales, pues el artículo 3 .h) define el consentimiento del interesado como «toda manifestación de voluntad, libre , inequívoca , específica e informada, mediante la que el*

[8] Sentencia Número 39/2016 del Tribunal Constitucional de fecha 3 marzo de 2016. RTC 2016\39).

[9] Sentencia número 186/2008 de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid de fecha 31 de enero de 2008 (JUR 2009\164175).

interesado consienta el tratamiento de datos personales que le conciernen»

Ha sido la propia Agencia Española de Protección de Datos[10] la que ha venido a definir, uno por uno, los distintos requisitos que debe reunir la manifestación del consentimiento:

a) Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil (LEG 1889, 27).

b) Específico, es decir referido a un determinado tratamiento o serie de tratamientos concretos y en el ámbito de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.

d) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la Ley Orgánica impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

El principio del consentimiento expresado conllevará, por tanto, la necesidad del consentimiento inequívoco del afectado para que puedan tratarse sus datos de carácter personal, permitiéndose así a aquel ejercer efectivo control sobre dichos datos y garantizando su poder de disposición

[10] Resolución de la Agencia Española de Protección de Datos número R/02767/2016 de fecha 4 de noviembre de 2016 (JUR 2017\419).

sobre los mismos. Dicho consentimiento podrá prestarse de forma expresa, oral o escrita, o de manera tácita, mediante actos reiterados y concluyentes que revelen su existencia.

III.3. Derechos de los ciudadanos: haciendo referencia a las novedades que incluye el Reglamento de Protección de datos, ya que se amplían los conocidos derechos ARCO.

III.3.1. Derechos tradicionalmente reconocidos.

Tradicionalmente, cuatro han sido los derechos que en materia de protección de datos se han contemplado para los ciudadanos. Dichos derechos son los derechos de acceso, cancelación, oposición y rectificación. Son los denominados derechos ARCO.

Tal y como apunta Eva María Blázquez Aguado[11], estas prerrogativas pueden ejercitarse por sí mismos (ya que son derechos personalísimos, de acuerdo con lo señalado por el Reglamento 1729/2007) o, en su caso, por su representante legal (cuando tenga restringida su capacidad legal por incapacidad o por ser menor de edad).

El derecho de acceso está descrito en el párrafo primero del artículo 15 de la Ley Orgánica de Protección de Datos que dispone que:

El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

Los derechos de rectificación y cancelación están reconocidos en el artículo 16.2 de la Ley Orgánica de Protección de Datos que establece que:

[11] Blázquez Aguado, Eva María (2017). La implantación de un protocolo de videovigilancia en el centro de trabajo. *Revista Aranzadi de Derecho y Nuevas Tecnologías num. 43/2017.*

Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

Finalmente, el derecho de oposición al que se refiere el artículo 17 de la Ley Orgánica de Protección de Datos, está previsto en sus artículos 6.4 y 30.4. Así, el primero de los preceptos dispone que:

En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

En tanto que el segundo añade que:

Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Pues bien, como hemos indicado con anterioridad tales han sido los Derechos que inicialmente se han reconocido a los ciudadanos, sin que el ejercicio de los mismos pueda suponer ingresos adicionales al titular del fichero, tal y como así se recoge en el artículo 24.3 del Reglamento que desarrolla la Ley Orgánica de Protección de Datos, y tal y como así reconoce la jurisprudencia. Sírvase a modo de ejemplo la Sentencia del Tribunal Supremo que sobre dicho extremo determina que:

Con el empleo de la palabra "gratuitamente" en el artículo 15 , relativo al derecho de acceso por el propio interesado a sus datos de carácter personal sometidos a tratamiento y con los de "contraprestación alguna" en el artículo 17.2 , relativo al procedimiento de oposición , acceso ,

rectificación o cancelación , de manera explícita el legislador excluye la posibilidad de que en el ejercicio de los derechos que en esos preceptos se contemplan puede el responsable del fichero obtener un lucro a cuenta del interesado, y esa exclusión se corrobora en el artículo 24.3 del Reglamento cuando en el inciso final del párrafo primero se expresa que "en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan" .

Una vez analizados cuales son los principales derechos que tienen reconocidos los ciudadanos en materia de protección de datos, en el apartado siguiente entraremos a analizar las principales novedades que sobre dicha materia introduce el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

III.3.2. El Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas y los nuevos derechos en él reconocidos.

III.3.2.1 El Reglamento Europeo relativo a la protección de las personas físicas.

El 27 de abril de 2016 se aprobó el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). El mismo entró en vigor a nivel europeo el día 25 de mayo de 2016 (a los veinte días de su aprobación). Ahora bien, no será aplicable en los Estados miembros hasta dos años después de su entrada en vigor, es decir, hasta el día 25 de mayo del año 2018.

La modificación de la actual Ley Orgánica de Protección de Datos, para adecuarla a lo dispuesto en el mencionado Reglamento, ya ha iniciado su camino, pero todavía está en ciernes. Ahora bien, independientemente de que el legislativo

español adecue o no la normativa a lo dispuesto en el Reglamento, éste comenzará a aplicarse en mayo de 2018.

El Reglamento General de Protección de Datos se aplica a los tratamientos de datos personales realizados en el entorno de una persona jurídica o física establecida en la Unión, con independencia de que el tratamiento tenga lugar dentro o fuera de la Unión.

Igualmente se aplica al tratamiento de datos personales de residentes en la Unión efectuado por un "responsable o encargado no establecido en la Unión", cuando las actividades de tratamiento estén vinculadas con:

- La oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago.

- El control de su comportamiento, en la medida en que tenga lugar en la Unión.

En definitiva, el ámbito de aplicación territorial enunciado por el Reglamento General de Protección de Datos es tan amplio que abarca un gran abanico de situaciones relacionadas con la Unión Europea.

El Reglamento no se limita a incluir modificaciones en la legislación actual, sino que constituye un nuevo sistema de protección de datos inspirado por principios diferentes y, valorando la importancia que tienen las modificaciones tecnológicas a las que se enfrentan las empresas europeas.

III.3.2.2 Nuevos derechos reconocidos en el Reglamento Europeo de Protección de Datos.

Pues bien, una de las múltiples novedades que introduce el Reglamento es la relativa a los derechos de los ciudadanos, ya que se amplían los mismos, de tal manera que a los ya reconocidos derechos ARCO se añaden los siguientes:

Se amplían los derechos de los ciudadanos. Hasta ahora existían los denominados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). Pues bien, el Reglamento además de los anteriores, incluye los siguientes:

Principio de transparencia: se concreta en la obligación de adoptar todas las medidas que sean necesarias para facilitar al interesado toda información indicada en los artículos 13 y 14 (derecho de información).

Por lo tanto, podemos decir que este principio exige que la información dirigida al interesado sea fácil de entender y accesible, de manera que ello permita a los ciudadanos conocer qué ocurre cuándo facilitan sus datos para un determinado tratamiento.

Principio de información: obligación de facilitar al interesado la información exigida en el artículo 13 del Reglamento cuando se obtengan sus datos personales. Igualmente, debe facilitarse determinada información en aquellos casos en los que los datos no se han obtenido directamente del interesado, que es la que queda recogida en el artículo 14.

Supresión o derecho al olvido: supresión de los datos personales que le conciernan cuando concurra alguna de las circunstancias del artículo 17 del Reglamento. Especialmente relevante resulta este derecho, por cuanto aparece expresamente contemplado el derecho al olvido, ya que debemos de tener en cuenta, que hasta ahora ha sido una figura creada por la doctrina y la jurisprudencia.

Igualmente, era previsible que el Reglamento recogiera expresamente este derecho y ello por cuanto el objeto del mismo fue expresamente reconocido por el Tribunal de Justicia de la Unión Europea en su Sentencia 13 de mayo de 2014, tal y como analizaremos posteriormente,

No nos detenemos en este derecho, por cuanto el derecho al olvido es el objeto del presente trabajo, de tal manera que a lo largo del trabajo analizaremos todas las vicisitudes relativas al mismo.

Limitación al tratamiento: finalmente se contempla este derecho en virtud en determinados supuesto, se reconoce la potestad de los interesados de obtener una limitación del tratamiento de sus datos personales. Los supuestos son los contemplados en el artículo 18.1 del Reglamento y son los siguientes:

a) El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) El interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Por lo tanto, cuando concurra alguno de los supuestos anteriormente citados, el responsable de los ficheros deberá conservar dichos datos, pero únicamente podrá utilizarlo en los casos en los que expresamente se prevé en la normativa.

Derecho a la portabilidad de datos: Se introduce el derecho a la portabilidad de los datos para solicitar a un responsable que los esté tratando de modo automatizado bien la recuperación de esos datos en un formato que permita su traslado a otro responsable o bien la transferencia de los datos directamente al nuevo responsable cuando sea técnicamente posible.

Está contemplado en el artículo 20 del Reglamento Europeo de Protección de Datos y, a la vista de dicho precepto, podemos concluir que es un derecho que tiene una doble vertiente ya que permite a los interesados la posibilidad de solicitar la transferencia de sus datos de carácter personal de un responsable a otro responsable del fichero e igualmente sirve para que en interesado pueda solicitar y obtener sus datos personales en un formato electrónico. Respecto de esta segunda vertiente, podríamos decir que viene a complementar el derecho de acceso existente ya en la Ley Orgánica de Protección de Datos.

III.3.2.3 Otras novedades que incluye el Reglamento Europeo de Protección de Datos.

Pues bien, es evidente que no es esta la única novedad que se introduce con el Reglamento Europeo de Protección de Datos. Aprovechando este apartado y por las repercusiones que el mismo va a tener en la normativa española de la protección de Datos, a continuación, vamos a enumerar de forma sucinta alguna de las novedades que, a nuestro juicio especialmente relevantes.

Nuevo concepto de consentimiento.

Hasta ahora, la Ley Orgánica de Protección de Datos requería el consentimiento de los titulares de los datos para su tratamiento, pero no se recogía ninguna otra exigencia.

El Reglamento General de Protección de Datos Europeo establece una regulación más exhaustiva sobre el consentimiento. El Reglamento exige que el consentimiento, con carácter general, sea libre, informado, específico e inequívoco,

en tanto que la Ley Orgánica de Protección de Datos únicamente exigía que el mismo fuera inequívoco. En primer lugar, en el artículo 13 del citado Reglamento, detalla la información que se les debe dar a los afectados (así como a los trabajadores, o a cualquier interesado cuya información se vaya a recabar). En concreto, se deberá informar sobre los siguientes extremos:

- Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.

- La identidad de los destinatarios o las categorías de destinatarios de los datos personales.

- La identidad del responsable de la gestión y si procede, del delegado de protección de datos.

- El plazo durante el cual se conservarán los datos personales.

- La existencia de un derecho a solicitar al responsable del tratamiento el acceso a los datos personales que haya facilitado, su rectificación o supresión, o la limitación de su tratamiento.

- La posibilidad a ejercitar el derecho a presentar una reclamación ante una autoridad de control.

- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento.

- La intención de transferir sus datos personales a un tercer país u organización internacional.

Es decir, al contrario de lo que sucede con la aplicación de la normativa actual, ya no será suficiente con una mera explicación genérica. Con la aplicación del

Reglamento General de Protección de Datos, será necesario informar de manera clara, sencilla, pero completa de todas y cada una de las cuestiones expuestas.

El consentimiento ha de ser claro y expreso y, además, en el caso de tratamientos no relacionados directamente con el servicio prestado, deberá ser específico.

Para poder considerar que el consentimiento es inequívoco el Reglamento requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado. El consentimiento no puede deducirse del silencio o de la inacción de los ciudadanos.

Igualmente, se prevé que el consentimiento tiene que ser explicito, por lo tanto, ya no podrá entenderse como concedido implícitamente mediante algún tipo de acción positiva. Así, será preciso que la declaración u acción se refieran explícitamente al consentimiento y al tratamiento en cuestión.

Hay que tener en cuenta que el consentimiento tiene que ser verificable y que quienes recopilen datos personales deben ser capaces de demostrar que el afectado les otorgó su consentimiento, por lo tanto, recae sobre el responsable del tratamiento de datos la carga de probar que ese consentimiento efectivamente se prestó.

Privacidad desde el diseño y privacidad por defecto.

La privacidad desde el diseño se enuncia en el artículo 25 del Reglamento como una obligación. Atendiendo a lo dispuesto en el considerando 78, lo podemos adoptar como la clave a seguir por el responsable del tratamiento para demostrar el cumplimiento legislativo, ya que, como se indica en dicho considerando *“el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto”.*

El mencionado artículo 25 establece unos criterios a considerar en la aplicación del principio de privacidad desde el diseño y que son relativos a lo siguiente:

- El estado de la técnica;
- El coste de la aplicación;
- La naturaleza, ámbito, contexto y fines del tratamiento, así como
- Los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas.

Es decir, se puede afirmar que el principio de protección de datos desde el diseño debe ser uno de los ejes sobre los que desarrollar un programa de compliance en materia de protección de datos, de manera que la gestión del riesgo que implica todo tratamiento de datos personales sea considerada en el momento mismo de la concepción de una idea que dé lugar al diseño o desarrollo de aplicaciones, servicios y productos.

En definitiva, la protección de datos desde el diseño es una cuestión estratégica que, tanto el responsable como el encargado del tratamiento (aunque especialmente el primero), deben valorar para asegurar el derecho fundamental a la protección de datos mediante la adopción e implementación de medidas técnicas y organizativas que consideren en la persona, titular de los datos, desde el principio o, incluso, desde el momento mismo en el que se genera una idea que pueda dar lugar a una aplicación, servicio o producto.

Evaluación del impacto de privacidad.

Relacionado íntimamente con lo anterior, el Reglamento General de Protección de Datos establece la obligación de redactar y preparar un registro de tratamientos, en el que se incluyan todos los tratamientos de datos personales que se vayan a

realizar por el encargado del tratamiento. Además, en el registro, se debe valorar el riesgo que entraña cada uno de ellos.

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos para la protección de datos similares.

El objetivo que se persigue mediante la evaluación de impacto de privacidad es analizar e identificar los riesgos que un determinado sistema de información, producto o servicio puede entrañar para la protección de datos.

La evaluación de impacto relativa a la protección de los datos se requerirá en particular en caso de:

a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) Observación sistemática a gran escala de una zona de acceso público.

La evaluación deberá incluir como mínimo:

a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) Una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

¿Cómo debe hacerse?

- Debe llevarse con anterioridad a la implantación del nuevo producto, servicio o sistema.
- Debe ser sistemático y debe estar orientado a llevar a cabo una efectiva revisión de los procesos.
- Debe permitir una identificación clara de los responsables de las distintas tareas.
- Debe identificar y clasificar la información para determinar los datos personales que se tratan y sus características.
- Debe identificar quién y cómo tendrá acceso y tratará los datos personales.
- Deben participar todos los afectados por el proyecto en cuestión.
- Se deben describir los controles que se van a implantar para asegurar 1) que sólo se tratarán los datos personales necesarios 2) que solo se tratarán para las finalidades legítimas previstas y definidas.

Se incluye también una novedad respecto a las comunicaciones con las autoridades y con los titulares de los datos personales. Las brechas de seguridad que se produzcan, según lo establecido en el nuevo Reglamento, se deben comunicar a las autoridades en el plazo de 72 horas. Asimismo, se deberán comunicar igualmente a los afectados, a los que deberá informar de la naturaleza de la violación de la seguridad y de las recomendaciones para que se puedan mitigar los potenciales efectos adversos.

Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

En caso de incumplimiento de la obligación de comunicar podrán llegar a imponerse multas por importe de 10 millones de euros o de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior.

Delegado de protección de datos.

Se crea una nueva figura, regulada en el artículo 37, que se deberá instaurar en las empresas que se encuentren en alguno de los supuestos del párrafo primero y que el Reglamento denomina Delegado de Protección de Datos. Quien se designe Delegado de Protección de Datos debe ser una persona con conocimientos especializados en Derecho y, en concreto, en materia de protección de datos. Estos Delegados pueden ser o no empleados, pero, de cualquier forma, deben desempeñar sus funciones con total independencia.

Las funciones del Delegado de Protección de Datos, que se regulan en el artículo 39 del Reglamento, son las siguientes:

- Informar y asesorar al responsable del tratamiento de datos de las obligaciones que debe efectuar para cumplir con el Reglamento General de Protección de Datos.

- Supervisar la aplicación de las normas por el encargado del tratamiento en materia de protección de datos personales (asignación de responsabilidades, formación del personal, auditorías, etc.).

- Supervisar la aplicación del Reglamento General de Protección de Datos y, en particular, los requisitos relativos a la protección de datos.

- Velar por la conservación de la documentación.

- Supervisar la documentación, notificación y comunicación de las violaciones de datos personales.

- Supervisar la respuesta a las solicitudes de la autoridad de control y cooperar con ella, por solicitud de las mismas o por iniciativa propia.

- Ejercer de punto de contacto con la autoridad de control sobre cuestiones relacionadas con el tratamiento.

En definitiva, el Delegado de Protección de Datos velará porque se cumpla la normativa de protección de datos en las empresas. Es decir, es un instrumento más que contribuye a la prevención del incumplimiento de la normativa sobre protección de datos.

Igualmente, se establece en la normativa que el delegado de protección de datos no será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones.

Régimen sancionador.

Una de las modificaciones más notables es la introducción de un régimen sancionador agravado con respecto a la Ley Orgánica de Protección de Datos, que

comenzará a ser aplicable a todos aquellos que no hayan adecuado su actividad a lo dispuesto en el Reglamento de Protección de Datos antes de mayo de 2018.

Las sanciones previstas en el Reglamento General de Protección de Datos van hasta los 20 millones de euros, o el 4% de la facturación global anual del ejercicio anterior (la que resulte más elevada de las dos).

Vemos como las modificaciones introducidas en el Reglamento General de Protección de Datos suponen una concepción diferente de la protección de datos en el ámbito europeo. El Reglamento del Parlamento Europeo introduce conceptos novedosos, que implican novedosas obligaciones para las empresas. Sobre todo, se debe recordar que el Reglamento persigue un control previo y eficaz de la protección de datos, y por ello, ya no se persigue tan sólo la resolución de los peligros creados, sino que dichos peligros no se originen, y que las empresas, mediante un sistema eficaz de compliance, puedan evitar las posibles amenazas a la seguridad. Es decir, la nueva regulación requiere que las empresas realicen un verdadero esfuerzo para asegurar su cumplimiento. En este sentido, ya no es suficiente con una mera observación de lo dispuesto en la Ley Orgánica de Protección de Datos, sino que los operadores que traten datos de carácter personal deben contar con un sistema de prevención eficaz.

Para concluir, únicamente nos queda informar de que con fecha 23 de junio de 2017 ha sido impulsado por el Consejo de Ministros el Anteproyecto de la nueva Ley Orgánica de Protección de Datos de Carácter Personal.

IV. EL DERECHO AL OLVIDO: CONSIDERACIONES GENERALES.

IV.1 El nacimiento del derecho al olvido. Contexto.

El derecho al olvido nace en respuesta al fenómeno de Internet. Debemos tener en cuenta que la red no olvida. En el momento en el que una información es publicada en Internet la misma puede ser vista por cualquier persona y en cualquier momento, y, además, dicha información perdura en el tiempo.

No debemos obviar la importancia que la publicidad de dicha información puede tener en nuestro día a día. Por ejemplo, cada vez es más frecuente que las empresas acudan a Internet para buscar información sobre las personas que optan a un determinado puesto de trabajo, examinando por ejemplo sus redes sociales. En estos supuestos existe sin duda alguna un grave riesgo de descontextualización, ya que puede ser que se realicen interpretaciones de la información visualizada que no se ajusten a la realidad de los acontecimientos.

Miguel Ángel Davara Rodríguez[12] hace una aproximación muy acertada sobre la problemática existente con Internet:

> *A todo esto, hay que añadir la utilización de la red en Internet en dos aspectos básicos por su incidencia en la protección de datos:*
>
> - *De una parte, las denominadas redes sociales que alcanzan a millones de usuarios en el mundo, siendo de múltiples y distantes países incluso realidades, tecnológica y jurídicamente hablando y,*
>
> - *De otra parte, el cloud computing que, desde sus tres aspectos básicos centrados en el software como servicio, la plataforma como servicio y la infraestructura como servicio, basa su desarrollo, imparable e irreversible en programas y servicios y, consecuentemente, se tratan los datos de carácter personal de personas identificadas o identificables por su nombre y apellidos o no identificadas o identificables sino relacionadas y localizadas, de acuerdo con perfiles en red sin necesidad de conocer su identificación personal.*

La principal problemática del derecho al olvido es que no está expresamente regulado en nuestro ordenamiento jurídico, y ello a pesar de que tanto la doctrina como las distintas autoridades administrativas reconocen la necesidad de limitar la perdurabilidad de las informaciones que se publican en internet. La realidad es que hoy en día el derecho al olvido es una figura de creación jurisprudencial, si bien tal y

[12] Rodríguez Davara, Miguel Ángel (2013). "El derecho al olvido en Internet", Madrid, *La Ley.*

como analizaremos posteriormente el Reglamento Europeo de Protección de Datos ha introducido expresamente el derecho al olvido.

En este punto nos planteamos cómo nace el derecho al olvido. Pues bien, el derecho al olvido nace porque los ciudadanos quieren eliminar ciertos datos que les son concernientes y que se encuentran en la red.

Podemos decir, que la evolución de las tecnologías ha llevado aparejado el nacimiento de nuevos derechos, siendo uno de ellos el derecho al olvido. Evidentemente si nos retrotraemos cien años atrás, cuando no existía Internet, la publicación de datos personales en determinados medios, no era una cuestión que preocupara a la población, ya que el acceso a tales datos no era tan sencillo como es ahora. Evidentemente, la aparición de Internet junto con el desarrollo de otras tecnologías ha conllevado la aparición de nuevos problemas. Basta con introducir un nombre en un motor de búsqueda para que podamos obtener determinados datos personales de diversas personas. Pero además dicha obtención, puede llevarse a cabo en cualquier momento y en cualquier lugar.

Tal y como pone de manifiesto Juan María Martínez Otero[13]: *"las tecnologías digitales permiten traer al presente casi cualquier información, con sorprendente rapidez y sin ningún coste, produciendo lo que se ha dado en llamar el efecto eterno de la información, fruto de la memoria total de Internet".*

Ello conlleva el nacimiento de una nueva preocupación para los ciudadanos que consideran que ello implica una gran exposición y una vulneración de su privacidad y que, en determinadas ocasiones, les lleva a solicitar la eliminación de tales datos personales. Por ello, aquellos ciudadanos que desean que sus datos sean eliminados, se ven obligados a presentar solicitudes ante los distintos responsables de los tratamientos de los datos de carácter personal para que procedan a dicha eliminación.

[13] Martínez Otero, Juan María (agosto de 2015). El derecho al olvido en internet. *Revista de Derecho Político de la UNED Número 93.*

Todo ello ha conllevado el surgimiento de un gran número de solicitudes de personas que exigen que sus datos sean eliminados de páginas web, redes sociales, motores de búsqueda… lo cual, como no podía ser de otra manera, ha generado dificultades ya que debemos tener en cuenta que en el momento en el que se aprobó la Ley Orgánica de Protección de Datos de carácter personal, el uso de Internet era muy reducido. Ello ha obligado a las distintas autoridades administrativas y judiciales a aplicar una normativa desfasada, que se ha visto superada por la realidad de los acontecimientos, realizando así, tanto el legislador como los propios tribunales un gran esfuerzo para dar solución a las nuevas problemáticas surgidas, siendo una de tales problemáticas la configuración del derecho al olvido.

IV.2. El derecho al olvido, la dignidad humana y el libre desarrollo de la personalidad.

Como hemos visto anteriormente, el derecho fundamental a la protección de datos se constituye como uno de los pilares fundamentales en nuestro ordenamiento jurídico, siendo el punto de partida para el nacimiento del derecho al olvido.

No debemos obviar la conexión que existe entre el derecho a la protección de datos y el derecho a la dignidad del ser humano. Nuestro Ordenamiento jurídico pretende que se produzca el olvido de determinados hechos o informaciones de algunos sujetos, ya que, en caso de no ser así, ello podría afectar a su futuro. Es por ello que, para encuadrar el derecho al olvido en el marco constitucional, debemos partir del artículo 10.1 de la Constitución Española que determina que:

> *La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.*

La importancia de la dignidad humana como derecho de los individuos ha sido consagrada por el Tribunal Constitucional[14] quien la ha configurado como un valor supremo del Ordenamiento Jurídico español, tal y como se transcribe a continuación:

[14] Sentencia del Tribunal Constitucional 53/1985 de fecha 11 de abril de 1985 (RTC 1985\53).

> *Indisolublemente relacionado con el derecho a la vida en su dimensión humana se encuentra el valor jurídico fundamental de la dignidad de la persona, reconocido en el artículo 10 como germen o núcleo de unos derechos «que le son inherentes». La relevancia y la significación superior de uno y otro valor y de los derechos que los encarnan se manifiesta en su colocación del título destinado a tratar de los derechos y deberes fundamentales, y el artículo 15 a la cabeza del capítulo donde se concretan estos derechos, lo que muestra que dentro del sistema constitucional son considerados como el punto de arranque, como el prius lógico y ontológico para la existencia y especificación de los demás derechos.*

En este contexto debemos tener en cuenta que hay determinados datos del pasado de los individuos que pueden afectar a su dignidad humana. Por lo tanto, es manifiesta la conexión que existe entre el derecho al olvido y el derecho a la dignidad, ya que el primero se configura como un medio para la defensa del segundo, en el sentido de eliminar o anonimizar determinados datos que pueden afectar a los derechos de la personalidad de los afectados. En este sentido la Audiencia Nacional[15] determina que:

> *Más adelante, se alude a que, tanto desde la perspectiva del Derecho Comparado como desde el punto de vista del ordenamiento español, parece claro, que el Tribunal Constitucional ha imbricado los derechos y bienes constitucionales reconocidos por el artículo 18 de la Constitución (RCL 1978, 2836) en la categoría de los derechos de la personalidad inextricablemente unidos con la dignidad humana, y ello incluye al derecho fundamental a la protección de datos.*

[15] Sentencia de la Audiencia Nacional de fecha 29 de diciembre de 2014 (RJCA 2015\183).

Tal y como prescribe Pere Simón Castellano[16] "*El derecho al olvido se configuraría, en este contexto, como un derecho de libertad del ciudadano, a poder escoger cuándo y dentro de qué límites procede relevar datos e informaciones que forma parte de su identidad. Hacemos referencia a un derecho al olvido vinculado necesariamente al derecho a la autodeterminación informativa, que se concreta en el control efectivo sobre los datos personales –habeas data-, a decidir cuáles pueden ser tratados y consultados por terceros."*

Anteriormente hemos analizado la relación entre el derecho al olvido y el derecho a la intimidad. Pues bien, debe tenerse en cuenta que, si bien tanto el derecho a la intimidad como el derecho a la dignidad están íntimamente relacionados con el derecho al olvido, los bienes jurídicos que protegen son distintos. A tal efecto resulta especialmente ilustrativa la famosa Sentencia del Tribunal Constitucional Número 292/2000 en la que se establece claramente esta distinción:

> *La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio [RTC 1999, 144]). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio [RTC 1999, 134] ; 98/2000, de 10 de abril [RTC 2000, 98] ; 115/2000, de 5 de mayo [RTC 2000, 115]), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre estos datos".*

[16] Simón Castellano, Pere. (2015). *El reconocimiento del derecho al olvido digital en España y en la Unión Europea.* Barcelona (España). Bosch

A la vista de lo anteriormente expuesto, podemos concluir que desde esta perspectiva constitucional el derecho al olvido pretende impedir el uso ilícito y lesivo de los datos personales que atenten contra la dignidad humana.

IV.3. Concepto y caracteres del derecho al olvido.

IV.3.1. Concepto del derecho al olvido.

Una vez que hemos introducido tanto el contexto en el que surgió el derecho al olvido, como el encuadre constitucional del mismo, la siguiente pregunta qué debemos efectuarnos es ¿Qué debe entenderse por derecho al olvido?

Pues bien, aunque en nuestro ordenamiento jurídico el derecho al olvido es un concepto de reciente creación, sí que hay que poner de manifiesto que el derecho al olvido tiene un antecedente bastante antiguo ya que parte de la definición del jurista americano Louis Brandeis, que en 1890 lo definió como "the right to be let alone", el derecho a que te dejen estar solo o en paz.

Pues bien, para Beatriz Villaverde[17] el derecho al olvido *es "el derecho que tiene el titular de un dato personal a borrar, bloquear o suprimir información personal que se considera obsoleta por el transcurso del tiempo o que de alguna manera afecta el libre desarrollo de alguno de sus derechos fundamentales. Como cabe apreciar, este derecho puede en ocasiones colisionar con la libertad de expresión y/o de información e incluso del derecho de libertad de empresa".*

Para Luis Javier Mieres es[18] *"la última manifestación de la necesidad de preservar la privacidad de las personas frente a las amenazas que entraña el progreso tecnológico".*

[17] Villaverde, Beatriz (10 de febrero de 2015). Madrid. Creativa legal. Recuperado de: http://www.creativalegal.com/2015/02/10/la-historia-del-derecho-al-olvido/

[18] Mieres Mieres, Luis Javier (2014). *El Derecho al olvido digital.*

Para Marina Sancho López[19] "*el derecho a olvido aspira a ser la respuesta jurídica al problema obligando, por ley, a borrar o hacer anónimos los datos personales una vez se ha logrado el objetivo de su tratamiento, concediendo al titular el derecho a oponerse justificadamente al mismo. Se pretende impedir así el perpetuo mantenimiento de algunos datos en Internet altamente sensibles para la dignidad e intimidad de las personas, lo que en la práctica supone, por ejemplo, la eliminación o bloqueo de datos de ficheros de morosos o de listados comerciales, o la cancelación de antecedentes.*"

No podemos obviar en este punto la definición de un experto en la materia como es Miguel Ángel Davara Rodríguez[20] que define el derecho al olvido como *"aquel derecho que tiene el titular de un dato a que éste sea borrado, o bloqueado, cuando se produzcan determinadas circunstancias y, en particular, que no sea accesible a través de la red de Internet".*

La Agencia Española de Protección de Datos define el derecho al olvido como "*el [21]la manifestación de los tradicionales derechos de y cancelación y oposición aplicados a los buscadores de internet. El 'derecho al olvido' hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información).*"

[19] Sancho López, Marina (2016). Consideraciones procesales del ejercicio del derecho al olvido: examen de jurisprudencia reciente y nuevo marco legal. *Revista Aranzadi de Derecho y Nuevas Tecnologías num. 41/2016.*

[20] Rodríguez Davara, Miguel Ángel (2013). "El derecho al olvido en Internet", Madrid, *La Ley.*

[21] Agencia Española de Protección de Datos. 2015. Recuperado de: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php

A la vista de lo anteriormente expuesto vemos como el derecho al olvido se configura como una herramienta a través de la cual los ciudadanos pueden controlar la información personal que sobre ellos se publica en internet y en instrumentos similares, de manera que les permite limitar su difusión cuando la misma es inexacta, obsoleta o carece de relevancia.

IV.3.2. Caracteres del derecho al olvido.

En el presente apartado vamos a analizar cuáles son los requisitos para que se produzca el nacimiento a ejercer el derecho de protección de datos. Debemos de tener en cuenta que el derecho al olvido no puede ser ejercido por cualquiera ni tampoco respecto a cualquier tipología de datos, sino que es necesaria la concurrencia de una serie de elementos, para que así sea.

En primer lugar, es necesaria la concurrencia de un elemento subjetivo, y ello por cuanto, el derecho al olvido únicamente puede ser ejercido por una persona física. La base para ello la encontramos tanto en el en el artículo 2.1 como en el artículo 3.a) de la Ley Orgánica de Protección de Datos de Carácter Personal. Así el primero de los artículos, relativo al ámbito de aplicación de la Ley dispone que:

> *La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.*

Por su parte, el artículo 3.a) define datos de carácter personal como:

> *Cualquier información concerniente a personas físicas identificadas o identificables.*

Por lo tanto y dado que únicamente las personas físicas son titulares del derecho a la protección de datos, el derecho al olvido únicamente se predica respecto estas, en ningún caso respecto de las personas jurídicas.

Ahora bien, respecto de las personas físicas esta cuestión ha sido matizada por los Tribunales, ya que cuando una persona física actúa en el tráfico como empresario, se le deniega el derecho al olvido. Concretamente, ha sido el Tribunal de Justicia de la Unión Europea quien en su sentencia de 9 de marzo de 2017 sobre el asunto C-398/15, ha señalado que la publicidad de los registros de sociedades tiene por objeto garantizar la seguridad jurídica en las relaciones entre las sociedades y los terceros, buscando proteger los intereses de los terceros en relación con las empresas, considerando que estas sólo ofrecen su patrimonio social como garantía respecto a ellos. Por tanto, no existe vulneración si los datos personales de las personas físicas inscritas en un registro de sociedades se mantienen en el tiempo.

En segundo lugar, se exige la existencia de un presupuesto objetivo, y ello por cuanto los datos que pueden dar lugar al nacimiento del derecho al olvido, tienen que ser datos personales de los afectados.

Como acabamos de ver la ley Orgánica de Protección de Datos en su artículo 3.a) define los datos personales como:

> *Cualquier información concerniente a personas físicas identificadas o identificables.*

Finalmente, el artículo 5.f) del Reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter personal añade que:

> *1. A los efectos previstos en este reglamento, se entenderá por:*
> *Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.*

Como no podía ser de otra manera, la Agencia Española de Protección de Datos[22] ha delimitado el concepto de dato de carácter personal y, en este sentido ha dispuesto

> *De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.*

Y, en tercer lugar, dichos datos tienen que ser objeto de un determinado tratamiento, e igualmente el afectado tiene que haber podido conocer de alguna manera la existencia de dicho tratamiento, ya que en caso de que no tenga conocimiento sobre ello difícilmente podrá ejercer su derecho al olvido, lo cual está íntimamente relacionado con el cuarto de los requisitos. En este punto es necesario añadir que la naturaleza de los datos, no es relevante a los efectos del ejercicio del derecho al olvido, y ello por cuanto es indiferente que se trate de datos públicos o privados. Lo verdaderamente relevante, es que se trate de datos personales y que además dichos datos permanezcan de forma permanente en internet y que además puedan menoscabar el derecho a la propia identidad del individuo.

Finalmente, en cuarto lugar, tiene que existir una actuación positiva del afectado en el sentido de que tiene que tiene que haber una voluntad de que sus datos sean eliminados. Evidentemente, como presupuesto previo a este requisito es necesario, como apuntábamos en el párrafo anterior, que sea conocedor del tratamiento que se está llevando a cabo de sus datos personales. Pero no sólo esto, sino que tiene que tener una actitud activa.

Por lo tanto, podemos concluir que para que quepa el ejercicio del derecho al olvido es necesaria la concurrencia de cuatro requisitos: tenemos que encontrarnos

[22] Resolución de la Agencia Española de Protección de Datos número E/03240/2016 de fecha 28 de marzo de 2017.

ante datos personales, de personas físicas (exceptuando los datos personales de las personas físicas cuando actúan en el tráfico mercantil como empresarios), siendo dichos datos 0bjeto de un determinado tratamiento y además debe concurrir la voluntad del afectado de que tales datos sean suprimidos.

IV.3.3. Derecho al olvido y derecho a la información.

Debemos partir de que el derecho al olvido no es absoluto. No siempre los afectados por un determinado tratamiento de datos tienen derecho a la cancelación y eliminación de sus derechos personales, sino que es necesario alcanzar un equilibrio entre el derecho al olvido y el derecho a la libertad de información.

Es evidente que el derecho al olvido entra en conflicto con otros derechos y libertades. El particular entra en conflicto con la libertad de información. Evidentemente, no existe una escala o una jerarquía que determina de manera automática cuál de estos derechos debe prevalecer, sino que es necesario analizar caso por caso e igualmente tratar de alcanzar un equilibrio.

El derecho de información, así como la libertad de expresión son dos derechos consagrados en nuestro ordenamiento, tanto a nivel nacional como a nivel europeo. Así, la Constitución Española en su artículo 20.1.d) reconoce y protege el derecho a:

> *Comunicar o recibir libremente información veraz por cualquier medio de difusión.*

Por su parte, el Pacto Internacional de derecho Civiles y Políticos establece en su artículo 19.2 que:

> *Toda persona tiene el derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.*

En términos similares queda recogido en el Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales. Concretamente en el artículo 10.1 se reconoce: que:

> *Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.*

Finalmente debemos hacer referencia al artículo 11 de la Carta de Derechos Fundamentales de la Unión Europea, que dispone que:

> *1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras";*
> *2. Se respetan la libertad de los medios de comunicación y su pluralismo".*

Pues bien, como hemos avanzado anteriormente, se trata de ponderar tales derechos. Tradicionalmente, la jurisprudencia ha venido dando prioridad a la libertad informativa respecto a otros derechos como el derecho al honor y el derecho a la intimidad. Sírvase a modo de ejemplo la Sentencia del Tribunal Constitucional de fecha 12 de noviembre de 1990[23] en la que se pronunció en los siguientes términos:

> *Dada su función institucional, cuando se produzca una colisión de la libertad de información con el derecho a la intimidad y al honor aquélla goza, en general, de una posición preferente y las restricciones que de dicho conflicto puedan derivarse a la libertad de información deben interpretarse de tal modo que el contenido fundamental del derecho a la información no resulte, dada su jerarquía institucional desnaturalizado ni*

[23] Sentencia del Tribunal Constitucional Número 171/1990 de fecha 12 noviembre (RTC 1990\171)

incorrectamente relativizado -SSTC 106/1986 (RTC 1986\106) y 159/1986 (RTC 1986\159), entre otras-.

Si cuando se ejerce el derecho a transmitir información respecto de hechos o personas de relevancia pública adquiere preeminencia sobre el derecho a la intimidad y al honor con los que puede entrar en colisión, resulta obligado concluir que en esa confrontación de derechos, el de la libertad de información, como regla general, debe prevalecer siempre que la información transmitida sea veraz, y esté referida a asuntos públicos que son de interés general por las materias a que se refieren y por las personas que en ellos intervienen, contribuyendo, en consecuencia, a la formación de la opinión pública. En este caso el contenido del derecho de libre información «alcanza su máximo nivel de eficacia justificadora frente al derecho al honor, el cual se debilita, proporcionalmente, como límite externo de las libertades de expresión e información» (STC 107/1988, fundamento jurídico 2.º) (RTC 1988\107).

A la vista de la Sentencia anteriormente transcrita podemos concluir con que se sacrifica el derecho a la protección de datos por la información veraz sobre asuntos de interés público.

Igualmente, la Agencia Española de Protección de Datos[24] ha dado una serie de pautas para resolver el conflicto existente entre la protección de datos y el derecho a la información y a la libertad de expresión, que son las siguientes:

Por todo ello, cabe proclamar que ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la RED sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación universal como Internet. Si requerir el consentimiento individualizado de los ciudadanos para incluir sus datos personales en Internet o exigir

[24] Resolución de la Agencia Española de Protección de Datos R/02681/2015

mecanismos técnicos que impidieran o filtraran la incorporación inconsentida de datos personales podría suponer una insoportable barrera al libre ejercicio de las libertades de expresión e información a modo de censura previa (lo que resulta constitucionalmente proscrito), no es menos cierto que resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las referidas libertades (por no resultar sus datos personales de interés público ni contribuir, en consecuencia, su conocimiento a forjar una opinión pública libre como pilar basilar del Estado democrático) debe gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la Red de su información de carácter personal.

Especialmente ilustrativa resulta en este punto la Sentencia del Tribunal Supremo de fecha 5 de abril de 2016[25] que delimita claramente la existencia de ambos derechos, así como el límite que el derecho a la información supone para el derecho al olvido:

El llamado "derecho al olvido digital", que es una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento de datos personales, no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos. Tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículo a su gusto, controlando el discurso sobre sí mismos, eliminando de Internet las informaciones negativas, "posicionando" a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones. De admitirse esta tesis, se perturbarían gravemente

[25] Sentencia del Tribunal Supremo Número 210/2016 de fecha 5 de abril de 2016 (RJ 2016\1006)

los mecanismos de información necesarios para que los ciudadanos adopten sus decisiones en la vida democrática de un país.

Pues bien, vemos como el criterio fundamental a la hora de determinar qué derecho prevalece es el del interés público. No obstante, lo anterior, la realidad es que habrá que analizar caso por caso para poder evaluar el interés de los datos personales y con base en ello dictaminar la prevalencia del derecho al olvido o del derecho a la información.

IV.3.4. Facultades de los afectados.

Como hemos visto anteriormente el derecho al olvido se configura como una herramienta del control de los datos de carácter personal. En España esta labor de determinar el alcance del derecho al olvido ha sido principalmente llevada a cabo por la Agencia Española de Protección de Datos, de manera que en diversas resoluciones ase ha pronunciado sobre el hecho de que ningún ciudadano que no sea objeto de un hecho noticiable de relevancia pública tiene que resignarse a que sus datos se difundan en Internet sin poder reaccionar ni corregir su inclusión. Concretamente en su resolución de fecha 7 de abril de 2008[26] se pronuncia en los siguientes términos:

Por todo ello, cabe proclamar que ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la RED sin poder reaccionar ni corregir la inclusión ilegítima de los mismos en un sistema de comunicación universal como Internet. Si requerir el consentimiento individualizado de los ciudadanos para incluir sus datos personales en Internet o exigir mecanismos técnicos que impidieran o filtraran la incorporación inconsentida de datos personales podría suponer una insoportable barrera al libre ejercicio de las libertades de expresión e información a modo de censura previa (lo que resulta constitucionalmente

[26] Resolución de la Agencia Española de Protección de Datos número R/00320/2008 de fecha 4 de abril de 2018.

> *proscrito), no es menos cierto que resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las referidas libertades (por no resultar sus datos personales de interés público ni contribuir, en consecuencia, su conocimiento a forjar una opinión pública libre como pilar basilar del Estado democrático) debe gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la Red de su información de carácter personal.*

La Agencia Española de Protección, configura este derecho desde una doble perspectiva, ya que por un lado reconoce la posibilidad de ejercitar el derecho de cancelación de los datos que la red conserva cuando estos no se contengan en una fuente accesible al público ni exista una finalidad legítima que proteja la publicación, y, por otro lado, reconoce el derecho de oposición. Así lo pone de manifiesto en su memoria anual relativa al ejercicio 2013[27]:

> *En paralelo, los ciudadanos en España han sido pioneros en el ejercicio del denominado derecho al olvido (derecho de cancelación y oposición) para evitar la difusión universal y permanente de sus datos en Internet*

Ambos derechos, como ya hemos visto a lo largo del presente trabajo se encuentran recogidos en la Ley Orgánica de Protección de Datos de Carácter Personal. Así el derecho de oposición es delimitado por la Agencia como[28]:

> *El derecho de oposición es uno de los derechos que la Ley Orgánica de Protección de Datos de carácter personal (LOPD) reconoce a los ciudadanos para que puedan defender su privacidad controlando por sí*

[27] Agencia Española de Protección de Datos. (2013). Memoria anual 2013. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/memorias/memoria2013/Memoria_AEPD_2013.pdf

[28] Agencia española de Protección de Datos. Derecho de Oposición. Disponible en: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/oposicion-ides-idphp.php

mismo el uso que se hace de sus datos personales, y en particular, el derecho a que no se lleve a cabo el tratamiento de éstos o se cese en el mismo cuando no sea necesario su consentimiento para el tratamiento, por la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, y siempre que una Ley no disponga lo contrario.

Por su parte, el derecho de cancelación se define como[29]:

El derecho de cancelación es uno de los derechos que la Ley Orgánica de Protección de Datos de carácter personal (LOPD) reconoce a los ciudadanos para que puedan defender su privacidad controlando por sí mismo el uso que se hace de sus datos personales, y en particular, el derecho a que éstos se supriman cuando resulten inadecuados o excesivos.

Ambas acciones, la cancelación de algunos datos y la oposición frente al tratamiento de los buscadores, no están exentas de problemas relevantes, pues pueden impedir el ejercicio legítimo de otros derechos fundamentales, como la libertad de expresión o la libertad de información, en los términos que hemos visto en el apartado anterior.

IV.3.5. El papel de la Agencia Española de Protección de Datos.

Como hemos puesto de manifiesto con anterioridad, el surgimiento del derecho al olvido en España tiene su origen en las diversas quejas que los ciudadanos plantearon ante la Agencia Española de Protección de Datos y en las que solicitaba que los motores de búsqueda dejaran de indexar informaciones relativas a sus datos personales. Basta con acudir a las diversas memorias de la Agencia Española de

[29] Agencia española de Protección de Datos. Derecho de Cancelación. Disponible en: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/cancelacion-ides-idphp.php

Protección de Datos para ver el aumento en las resoluciones de cancelación y rectificación emitidas por la Agencia:

Año	Cancelación	Oposición	Totales
2008[30]	859	22	881
2009[31]	1366	127	1493
2010[32]	988	107	1095
2011[33]	1053	188	1241
2012[34]	1202	223	1425
2013[35]	1300	209	1509
2014[36]	1047	136	1183

[30]Agencia española de Protección de Datos. Memoria anual del año 2008, página 43. Disponible en: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2008/AEPD_memoria_2008.pdf

[31] Agencia española de Protección de Datos. Memoria anual del año 2009, página 56. Disponible en: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2009/AEPD_memoria_2009.pdf

[32] Agencia española de Protección de Datos. Memoria anual del año 2010, página 55. Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2010/AEPD_Memoria_2010.pdf

[33] Agencia española de Protección de Datos. Memoria anual del año 2011, página 89. Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2011/Memoria_2011.pdf

[34] Agencia española de Protección de Datos. Memoria anual del año 2012, página 73. Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2012/Memoria_2012.pdf

[35] Agencia española de Protección de Datos. Memoria anual del año 2013, página 85. Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2013/Memoria_2013.pdf

[36] Agencia española de Protección de Datos. Memoria anual del año 2014, página 111. Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/Memoria_2014.pdf

2015[37]	1392	130	1522
2016[38]	612	87	699

Vemos como en general se observa una tendencia creciente, que alcanzó su punto álgido en el año 2015, es decir, una vez que se hubo dictado la Sentencia del Tribunal de Justicia de la Unión Europea de fecha 13 de mayo de 2014. Igualmente, es necesario recalcar el brusco descenso en el número de resoluciones emitidas que se ha producido en el año 2016, ya que han pasado a ser prácticamente la mitad.

Los números reflejados en el cuadro hablan por sí solos. Es evidente que la preocupación por parte de los ciudadanos para que desaparezcan o se anonimicen sus datos de Internet. Si bien, a la vista del dato relativo al 2016 parece que se está disipando tal preocupación. Tal y como hemos reflejado en el apartado anterior, la propia Agencia en su Memoria de 2013[39]: expresó que:

> *En paralelo, los ciudadanos en España han sido pioneros en el ejercicio del denominado derecho al olvido (derecho de cancelación y oposición) para evitar la difusión universal y permanente de sus datos en Internet.*

La Agencia Española de Protección de Datos ha mantenido firme su criterio respecto del ejercicio de estos derechos, poniendo de manifiesto que los ciudadanos no tienen por qué resignarse ni tienen que verse expuestos al tratamiento de sus datos en Internet de forma permanente.

[37] Agencia española de Protección de Datos. Memoria anual del año 2015, página 119. Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2015/Memoria_2015.pdf

[38] Agencia española de Protección de Datos Memoria anual del año 2016, página 73. Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2016/Memoria_2016.pdf

[39] Agencia Española de Protección de Datos. (2017). Memoria anual 2013. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/memorias/memoria2013/Memoria_AEPD_2013.pdf

Como veremos en el apartado V.4.2., dicha labor ha sido refrendada por la Sentencia del Tribunal Superior de Justicia de la Unión Europea de fecha 13 de mayo de 2014. Tanto desde el 2007 (fecha en la que la Agencia Española de Protección de Datos emitió la primera resolución relativa al derecho al olvido) como a partir del 13 de mayo de 2014 (fecha en que el Tribunal Superior de Justicia de la Unión Europea dictó su Sentencia relativa al derecho al olvido) la línea que ha seguido ha sido la misma, esto es, estimar las resoluciones de oposición y cancelación del tratamiento de derechos personales en aquellos supuestos en los que no existe una finalidad para el tratamiento legítimo.

Por lo tanto, hay que destacar la labor llevada a cabo por la Agencia Española de Protección de Datos e igualmente hay que recalcar su papel de pionera en el desarrollo del derecho al olvido y en la consolidación del mismo, delimitando claramente cuáles son los límites, y analizando resolución por resolución para sentar unas bases, que han permitido la actual configuración del derecho al olvido.

V. EL DERECHO AL OLVIDO: SUPUESTOS ESPECÍFICOS.

V.1 El derecho al olvido y el derecho de acceso a la documentación judicial.

El objetivo del presente apartado es analizar la relación existente entre el derecho al olvido e igualmente el derecho de acceso a la documentación judicial centrándonos sobre todo en el caso español. A tal efecto debemos tener en cuenta que en España con carácter general hay determinadas resoluciones judiciales que se publican en Boletines Oficiales (del Estado, de la Comunidad Autónoma, Provinciales…) e igualmente en otras fuentes como por ejemplo determinadas bases de datos privadas o en el Centro de Documentación Judicial, con las peculiaridades que ello conlleva.

V.1.1. El derecho a la documentación judicial. Análisis de la situación en distintos Ordenamientos Jurídicos.

Con carácter previo a analizar el caso español, en el presente apartado vamos a hacer una breve referencia al tratamiento de este derecho en otros sistemas judiciales.

Comenzando por el caso de Estados Unidos, debemos acudir a lo dispuesto en la Sexta Enmienda del Texto Constitucional, cuya traducción es la siguiente:

> *En toda causa criminal, el acusado gozará del derecho de ser juzgado pública y expeditamente, por un jurado imparcial del Estado y distrito en que el delito se haya cometido, distrito que habrá sido determinado previamente por la ley; así como de ser informado sobre la naturaleza y causa de la acusación; que se le caree con los testigos en su contra; que se obligue a comparecer a los testigos en su favor y de contar con la ayuda de Asesoría Legal para su defensa.*

Vemos como en el caso de Estados Unidos la publicidad del procedimiento se plantea como una garantía para los derechos de los ciudadanos. Ahora bien, es necesario puntualizar que esa publicidad del procedimiento, no implica un acceso ilimitado a los documentos y resoluciones judiciales.

No podemos obviar la importancia que en el contexto de la justicia americana tiene la publicidad tales resoluciones y ello por las Sentencias constituyen precedentes vinculantes en una determinada jurisdicción, por lo tanto, la publicidad o no de una determinada resolución implica que la misma pueda ser o no empleada como un precedente en un determinado procedimiento. Por lo tanto, es manifiesta la relevancia que en Estados Unidos tiene la publicidad de las resoluciones.

En Estados Unidos son los Tribunales los que deciden cuáles de sus resoluciones se publican, por lo tanto, son los propios Tribunales los que deciden cuáles de sus resoluciones van a ser susceptibles de generar un precedente en su

jurisdicción, de tal manera que podemos observar como tienen un gran poder, no solo por la importancia que puede tener el poder judicial en sí, sino porque además son ellos los que deciden cuáles resultan vinculantes.

Igualmente, hay que poner de manifiesto que en Estados Unidos se ha intentado conjugar el derecho de acceso a las distintas resoluciones judiciales e igualmente el derecho a la privacidad de los intervinientes en el proceso. Esta cuestión está expresamente regulada en una Guía denominada *Guidelines on Access to Court Records for State Courts*, que ha sido elaborada por el *Council of Chiefs Justices* (que es el Presidente de la Corte Suprema de los Estados Unidos) y por la *Conference of State Court Administrators*. Pues bien, en dicha guía se reconoce el derecho de los ciudadanos a acceder a la información judicial, estableciéndose determinados documentos o resoluciones cuyo contenido puede ser limitado por el Juez. Vemos, por lo tanto, como en Estados Unidos existe un amplio acceso a la documentación judicial.

Siguiendo la línea del Common Law, si analizamos el caso de Inglaterra vemos como a pesar de compartir la tradición jurídica se establecen notables diferencias. Igualmente se parte del principio de la publicidad del procedimiento. Ahora bien, efectuada la anterior precisión no se permite un acceso tan amplio a los documentos o resoluciones judiciales. Vemos como no existe un derecho al acceso, lo cual difiere mucho del sistema anteriormente explicado y que precisamente aboga por todo lo contrario, esto es, un amplio acceso por parte de los ciudadanos (aunque no tengan relación alguna con el procedimiento) a tal documentación.

En el caso de Inglaterra hay que diferenciar dos supuestos, ya que las reglas de acceso a la documentación son distintas en función de si nos encontramos en el ámbito civil o penal. Los archivos dictados en procedimientos penales no son accesibles al público, en tanto que en el caso de los civiles sí que es posible el acceso a la Sentencia y a determinada documentación obrante en el expediente judicial por parte de personas que han sido ajenas al procedimiento.

Vemos por lo tanto como (sobre todo en el ámbito penal) prevalece el derecho a la intimidad y al honor de los afectados respecto del derecho al acceso a la documentación judicial, presentando este sistema notables diferencias con el de Estados Unidos.

Finalmente, interesa analizar también el caso de Francia, ya que tanto España como Francia tienen una tradición continental, y no podemos obviar la influencia que en determinados momentos históricos han tenido los textos legales franceses sobre el ordenamiento jurídico español. Nuevamente en el sistema francés es necesario atender al ámbito jurisdiccional, ya que los requisitos son distintos en el ámbito penal y en el resto de ámbitos judiciales.

En el ámbito penal la cuestión se encuentra regulada en el *Code de Procedure Pénale.* Pues bien, las partes de un procedimiento tienen libre acceso a la documentación del procedimiento en el que han sido parte, tal y como ocurre también en el sistema español. Ahora bien, en caso de que sean terceros ajenos al proceso, tienen que solicitarla, y para la obtención de la misma es precisa autorización del Ministerio Fiscal.

En el resto de órdenes judiciales, quiénes han sido parte tienen derecho a la obtención de la documentación judicial (como ocurría en el orden penal) pero los terceros ajenos al procedimiento solo podrán obtener copia de la decisión judicial.

En el caso francés, se da un paso más allá y se contempla en la normativa francesa expresamente la publicidad electrónica de las resoluciones judiciales. Concretamente ello se encuentra contemplado en la *Délibération n°01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence.*

En Francia a la hora de publicar los datos personales en las resoluciones judiciales han optado por disociar los mismos. Como veremos a continuación en España cuando las resoluciones se publican en el Centro de Documentación Judicial también se disocian los datos personales; ahora bien, el problema que ocurre en

relación con Francia es que solamente disocian los datos personales relativos a los nombres, apellidos y direcciones, de tal manera que hay determinados datos personales que no se disocian de las resoluciones y que en su conjunto pueden llevar a la identificación de un determinado sujeto.

Por lo tanto, nos encontramos con que las medidas adoptadas para asegurar la anonimización de los sujetos de los procedimientos no son tan garantistas como a priori pudiera parecer y ello por cuanto las mismas se aplican de manera mecánica, siendo que la medida más adecuada sería analizar caso por caso para ver si qué datos personales es preciso disociar para que no pueda llegar a identificarse a los sujetos afectados.

Una vez efectuado este recorrido por las legislaciones de otros países, vamos a centrarnos en analizar el caso español. El punto de partida a esta cuestión lo encontramos en el artículo 120 de la Constitución Española que dispone que:

1. *Las actuaciones judiciales serán públicas, con las excepciones que prevean las leyes de procedimiento.*
2. *El procedimiento será predominantemente oral, sobre todo en materia criminal.*
3. *Las sentencias serán siempre motivadas y se pronunciarán en audiencia pública.*

Vemos, por lo tanto, como con carácter general se establece la publicidad de los procedimientos. Dicha cuestión, fue posteriormente desarrollada por la Ley Orgánica del Poder Judicial. A tal efecto el artículo 266.1 establece que:

1. Las sentencias, una vez extendidas y firmadas por el juez o por todos los Magistrados que las hubieren dictado, serán depositadas en la Oficina judicial y se permitirá a cualquier interesado el acceso al texto de las mismas.

> *El acceso al texto de las sentencias, o a determinados extremos de las mismas, podrá quedar restringido cuando el mismo pudiera afectar al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda, así como, con carácter general, para evitar que las sentencias puedan ser usadas con fines contrarios a las leyes.*

Y el artículo 235 del mismo texto legal complementa lo anteriormente expuesto, disponiendo que:

> *Los interesados tendrán acceso a los libros, archivos y registros judiciales que no tengan carácter reservado, mediante las formas de exhibición, testimonio o certificación que establezca la ley.*

A la vista de ambas disposiciones, podríamos concluir que inicialmente se habría determinado que el libre acceso por parte de la ciudadanía a las Sentencias, sin más limitaciones que las establecidas en el párrafo segundo del artículo 266.1 de la Ley Orgánica del Poder Judicial. Sin embargo, a pesar de la literalidad de los artículos tanto la jurisprudencia como la Agencia Estatal de Protección de Datos empezaron a establecer límites a este derecho. El punto de inflexión lo encontramos en la Sentencia del tribunal Supremo de fecha 3 de marzo de 1995[40]. En dicho procedimiento la empresa Grupo Interprest, S.A., había solicitado a distintos Tribunales, en el desarrollo de su actividad profesional, una serie de Sentencias para facilitárselas a sus clientes. Dichos Tribunales denegaron esta petición por lo que Grupo Interprest, S.A., presentó recurso de casación.

Pues bien, el Tribunal Supremo entró a analizar la cuestión y delimitó el derecho de terceros a obtener información sobre el procedimiento judicial. Concretamente entendió que el principio de publicidad, al que hacen referencia los artículos 120 de la Constitución Española y los artículos 235 y 266 de la Ley Orgánica del Poder Judicial otorgan a los ciudadanos el derecho a asistir al procedimiento judicial, pero

[40] Sentencia del Tribunal Supremo de fecha 3 de marzo de 1995 (RJ 1995\2292).

no a obtener copia de una Sentencia, ya que a ello solo tienen derecho los interesados, y precisamente aquí es donde se produce la delimitación del derecho a acceder a las resoluciones judiciales, puesto que el Tribunal Supremo entra a analizar qué requisitos han de concurrir para que una persona tenga la condición de interesado. Concretamente en su Fundamento de Derecho Quinto se pronuncia en los siguientes términos:

> *Pues bien, el interés legítimo que es exigible en el caso, sólo puede reconocerse en quien, persona física o jurídica, manifiesta y acredita, al menos «prima facie», ante el órgano judicial, una conexión de carácter concreto y singular bien con el objeto mismo del proceso -y, por ende, de la sentencia que lo finalizó en la instancia-, bien con alguno de los actos procesales a través de los que aquél se ha desarrollado y que están documentados en autos, conexión que, por otra parte, se halla sujeta a dos condicionamientos: a) que no afecte a derechos fundamentales de las partes procesales o de quienes de algún modo hayan intervenido en el proceso, para salvaguardar esencialmente el derecho a la privacidad e intimidad personal y familiar, el honor y el derecho a la propia imagen que eventualmente pudiera afectar a aquellas personas; y b) que si la información es utilizada, como actividad mediadora, para satisfacer derechos o intereses de terceras personas, y en consecuencia adquiere, como es el caso, un aspecto de globalidad o generalidad por relación no a un concreto proceso, tal interés se mantenga en el propio ámbito del ordenamiento jurídico y de sus aplicadores, con carácter generalizado, pues otra cosa sería tanto como hacer partícipe o colaborador al órgano judicial en tareas o actividades que, por muy lícitas que sean, extravasan su función jurisdiccional.*

Vemos como por lo tanto el Tribunal Supremo además de exigir la concurrencia de un interés legítimo introduce dos requisitos más, el primero, que no afecte a derechos fundamentales o procesales de las partes y el segundo que la información obtenida sea para fines judiciales. En el caso que nos ocupa, puesto que las

Sentencias se pretendían obtener con fines comerciales, el Tribunal Supremo confirmó la denegación de acceso a las mismas.

Pues bien, desde que se dictó esa Sentencia, esa ha sido la línea que han mantenido nuestros Tribunales. Así, el Tribunal Supremo en una Sentencia dictada quince años después[41], en relación con dicho extremo se pronuncia en los siguientes términos:

> *El recurso debe ser desestimado porque no concurre en CCT la condición de interesado que requiere el artículo 235 de la Ley Orgánica del Poder Judicial para el acceso a los libros, archivos y registros judiciales. Según la jurisprudencia que lo ha interpretado --en concreto, las sentencias de esta Sala de 3 de marzo de 1995 (RJ 1995, 2292) (recurso 1218/1991), 22 de mayo de 1996 (RJ 1996, 5422) (recurso 755/1993) y 7 de febrero de 2000 (RJ 2000, 1588) (recurso 526/1997)-- es preciso, para que proceda el acceso a ellos, que quien lo reclame haya sido parte en el correspondiente proceso o acredite "al menos "prima facie", ante el órgano judicial, una conexión de carácter concreto y singular bien con el objeto mismo del proceso --y, por ende, de la sentencia que lo finalizó en la instancia--, bien con alguno de los actos procesales a través de los que aquel se ha desarrollado y que están documentados en autos", según dice la primera de esas sentencias, que también erige como límite el siguiente: "que no afecte a derechos fundamentales de las partes procesales o de quienes de algún modo hayan intervenido en el proceso, para salvaguardar esencialmente el derecho a la privacidad e intimidad personal y familiar, el honor y el derecho a la propia imagen que eventualmente pudiera afectar a aquellas personas.*

Igualmente, la Agencia Española de Protección de Datos se ha pronunciado sobre ello. Así en su resolución de fecha 24 de abril de 2008[42] dispone que:

[41] Sentencia del Tribunal Supremo de fecha 1 de febrero de 2010 (RJ 2010\1370).
[42] Resolución de la Agencia Española de Protección de datos R/01239/2007 de fecha 24 de abril de 2008.

De lo hasta ahora expuesto, se acredita que las Sentencias no son públicas, ni se publican para general conocimiento, aunque en virtud del derecho de información, como en el caso que se examina existan noticias relacionadas con el denunciante y los hechos.

Con base en lo anteriormente expuesto, debemos concluir que es necesario delimitar el ámbito de aplicación del principio de publicidad de los procedimientos judiciales, y ello por cuanto es necesario diferenciar entre el libre acceso (salvo las excepciones previstas) al procedimiento y el libre acceso a las Sentencias, que no es tal. Por lo tanto, vemos como el principio constitucional contemplado en el artículo 120 ha sido delimitado tanto por la Agencia Española de Protección de Datos como por la propia jurisprudencia que exigen la concurrencia de una serie de requisitos para que terceros ajenos al procedimiento puedan acceder a las Sentencias dictadas por los Tribunales.

V.1.2. La publicación de las Sentencias en España.

Debemos tener en cuenta que nuestro ordenamiento jurídico ha previsto dos formas de hacer públicas las Sentencias. La primera es mediante su publicación a través de los Boletines Oficiales y la segunda es a través de la publicación en el Centro de Documentación Judicial. Ahora bien, esta duplicidad de fuentes, que a priori pudiera parecer insignificante, tiene una gran relevancia y ello por cuanto la consideración que tienen los datos difiere en función del medio en el que se publiquen.

Respecto de la publicación de las Sentencias en el Centro de Documentación Judicial debemos acudir a lo dispuesto en el apartado primero del artículo 7 del Reglamento 1/2005, de 15 de septiembre de 2005, de los aspectos accesorios de las actuaciones judiciales, que en relación con la publicación de las Sentencias y otras resoluciones dispone que:

Con el objeto de asegurar el cumplimiento de lo dispuesto en el art. 107.10 de la LOPJ, en lo que se refiere a la publicación oficial de las

sentencias y otras resoluciones del Tribunal Supremo y del resto de órganos judiciales, para velar por su integridad, autenticidad y acceso, así como para asegurar el cumplimiento de la legislación en materia de protección de datos personales, todos los Juzgados y Tribunales, bajo la supervisión de sus titulares o Presidentes, o de alguno de los Magistrados en quienes aquellos deleguen a estos efectos, procederán a remitir al Consejo General del Poder Judicial, a través del Centro de Documentación Judicial y con la periodicidad que se establezca, copia de todas las sentencias, así como de otras resoluciones que puedan resultar de interés, que hayan sido dictadas por el respectivo órgano judicial.

Pues bien, la publicación por parte del Centro de Documentación Judicial se efectúa respetando lo dispuesto en el artículo 560.1.10º de la Ley Orgánica del Poder Judicial:

1. El Consejo General del Poder Judicial tiene las siguientes atribuciones:

10.ª Cuidar de la publicación oficial de las sentencias y demás resoluciones que se determinen del Tribunal Supremo y del resto de órganos judiciales.

A tal efecto el Consejo General del Poder Judicial, previo informe de las Administraciones competentes, establecerá reglamentariamente el modo en que habrán de elaborarse los libros electrónicos de sentencias, la recopilación de las mismas, su tratamiento, difusión y certificación, para velar por su integridad, autenticidad y acceso, así como para asegurar el cumplimiento de la legislación en materia de protección de datos personales.

El Tribunal Supremo en su Sentencia de fecha 28 de octubre de 2011 se ha pronunciado sobre la labor que realiza el Centro de Documentación Judicial:[43]

> *No cuesta excesivo esfuerzo ver en el segundo párrafo de ese artículo 107.10, en lugar de una especificación del primero -- como se ha visto, innecesaria-- una adición que sigue donde el primer párrafo termina: en la difusión de las sentencias y otras resoluciones judiciales en condiciones de garantía de su autenticidad, integridad y acceso y de la obligada protección de los datos personales. Digo que no cuesta excesivo esfuerzo porque eso es lo que venía y viene haciendo el CENDOJ desde hace años y está permitiendo la reutilización en la práctica. A esta faceta de la actividad del Consejo General del Poder Judicial se dirigen las normas reglamentarias, no para regular el uso que terceros hagan con otros terceros de esa información, sino la actuación administrativa del propio Consejo General del Poder Judicial consistente en suministrar a quien lo desee, en condiciones de igualdad, a través de uno de sus órganos técnicos, el CENDOJ, las sentencias y resoluciones que se quieren difundir ulteriormente con valor añadido o sin él.*

Vemos por lo tanto como el Centro de Documentación Judicial se constituye como un servicio público que garantiza el acceso a determinadas resoluciones judiciales, ahora bien, siempre respetando el derecho a la protección de datos de las partes del proceso.

Pues bien, una vez que hemos visto como el Centro de Documentación Judicial se constituye como una de las principales fuentes de acceso a la jurisprudencia, es necesario hacer referencia a la otra de las fuentes que hemos mencionado, esto es, los Boletines Oficiales, que como veremos a continuación constituyen una excepción al sistema de anonimización que rige en el ordenamiento jurídico español.

[43] Sentencia del Tribunal Supremo de fecha 28 de octubre de 2011 (RJ 2012\1691).

El punto de partida a esta cuestión, lo encontramos en el artículo 3.j) de la Ley Orgánica de Protección de Datos, en el que se definen las fuentes accesibles al público como:

> *Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.*

Igualmente, el carácter de fuente accesible al público de los Boletines Oficiales queda recogido en el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos. Así, en su artículo 7.1 establece que:

> *A efectos del artículo 3, párrafo j) de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público:*
> *d) Los diarios y boletines oficiales.*

Debemos tener en cuenta que únicamente cuando nos encontremos ante uno de los supuestos contemplados o bien en la Ley Orgánica de Protección de Datos o bien en el Reglamento que la desarrolla nos encontraremos ante una fuente accesible al público. En este sentido resulta especialmente ilustrativa la Sentencia de la Audiencia Nacional de fecha 24 de abril de 2007:

> *Del tenor literal de dicho precepto, se desprende con claridad que recoge un número clausus o enumeración cerrada de las fuentes que pueden calificarse como accesibles al público, lo que se remarca con el empleo*

del término "exclusivamente" que se anuda a las concretas fuentes que enumera. Criterio éste que es el seguido por la Sala entre otras en las SSAN, Sec 1ª, de 18-5-2006 (Rec 35/2005), 17 de marzo 2006 (Rec 62/2004), 18-1-2007 (Rec 240/2005) etc.

Por lo tanto, de lo anteriormente expuesto podemos concluir que el Centro de Documentación Judicial no tiene la consideración de fuente accesible al público, en tanto que los Boletines Oficiales sí que la tienen.

Por lo tanto, en el primero de los supuestos existe una obligación de anonimizar las resoluciones que se publican, en tanto que en el segundo de los supuestos desaparece dicha obligación. Es decir, no rige la normativa relativa a la protección de datos para los casos de las publicaciones que se efectúen en los Boletines Oficiales.

Dicha situación no deja de ser paradójica. Pensemos en la situación que se produce si una misma resolución es publicada en ambos medios (esto es, en el Centro de Documentación Judicial y en un Boletín Oficial). En el primero de los casos se modifican los datos personales de las partes en el proceso, en tanto que en el segundo no. Evidentemente, la labor consistente en eliminar los datos personales de los afectados por el Centro de Documentación Judicial es inocua y ello por cuanto dichos datos aparecerán en la resolución que se publique en el Boletín Oficial, puesto que tiene la consideración de fuente accesible al público y por lo tanto no se modifican los datos personales de las personas intervinientes en el procedimiento judicial.

Evidentemente el problema planteado se agrava al existir no solo la versión en papel de los Boletines Oficiales, sino también una versión digital. De tal manera que, si bien determinados datos se encuentran omitidos en la versión de la resolución publicada en el Centro de Documentación Judicial, pudiera ser que, al publicarse de manera íntegra en el Boletín Oficial correspondiente en su versión digital, con teclear el nombre de una de las partes en cualquier buscador, aparecería dicha resolución. Por lo tanto, ningún efecto tendría la labor de omitir los datos personales que lleva a cabo el Centro de Documentación Judicial.

También esta situación de anonimización se ve totalmente desvirtuada en ocasiones, a través de la labor que realiza la prensa. Así ocurrió en el caso Noos. La Sentencia publicada en el Centro de Documentación Judicial, modifica los nombres con el objetivo de disociar los datos personales. Pues bien, en el caso de Doña Cristina Federica Victoria Antonia de la Santísima Trinidad de Borbón y Grecia de Borbón, así como de Don Iñaki Urdangarín, dicho intento de disociar sus datos personales ha sido inocuo, y ello por cuanto la prensa española[44] se ha encargado de publicar los nombres que han sido empleados para sustituir los suyos, siendo Eva y Julio los nombres sustitutos empleados. Por lo tanto, en el caso de gente conocida para la sociedad, vemos como la prensa puede llegar impedir esa labor de anonimización llevada a cabo por el Centro de Documentación Judicial.

V.2 El derecho al olvido en las redes sociales.

Las redes sociales constituyen uno de los principales fenómenos que están directamente relacionados con el derecho al olvido, y ello por cuanto es manifiesto que la sociedad tiende, cada vez con mayor frecuencia, a exponer datos de su vida privada a través de dichos medios.

Es evidente que en este terreno se ha producido una gran evolución y ello por dos factores:

- En primer lugar, porque se ha producido una gran proliferación de las redes sociales, de tal manera que cada vez nos encontramos con una mayor variedad, así, por ejemplo, algunas de las más conocidas son Facebook, Twitter o Instagram.

- Y, en segundo lugar, porque ha aumentado el número de usuarios de las mismas.

[44] Sírvase a modo de ejemplo: https://confilegal.com/20170306-infanta-cristina-urdangarin/

Por lo tanto, nos encontramos con un gran número de usuarios que comparten información no solo de su vida privada, sino en determinadas ocasiones también información sobre la vida privada de terceros.

En este escenario es preciso distinguir dos situaciones:

- Aquellos supuestos en los que existe el consentimiento del usuario a la publicación de dicha información.

- Aquellos supuestos en los que no se ha recabado el consentimiento previo del afectado, en los términos que exige la normativa.

Pues bien, efectuadas las anteriores precisiones acerca del consentimiento, hemos de entrar a valorar cómo puede actuar un usuario si desea eliminar datos relativos a su vida privada que han sido publicados en una red social.

Si el afectado no ha prestado su consentimiento para que sus datos sean publicados podrá ejercitar su derecho a que dichos datos sean cancelados o, en su caso, rectificados. Por lo tanto, en aquellos supuestos en los que un usuario comparte en su red social una información sobre la vida privada de un tercero (una foto, un vídeo…), este podrá oponerse a dicha publicación mediante el ejercicio del derecho de cancelación.

Supuesto distinto es aquel en el que el usuario publica en su red social información sobre su persona y posteriormente desea que la misma sea eliminada. Pues bien, debemos tener en cuenta que el consentimiento es, con carácter general, revocable, tal y como así dispone el apartado tercero del artículo 6 de la Ley Orgánica de Protección de Datos:

> *El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.*

Por lo tanto, en ambos supuestos (esto es, tanto si existe consentimiento como si no existe el mismo) es posible que el afectado ejerza su derecho a la cancelación de los datos. Ahora bien, debemos tener en cuenta que para el primero de los supuestos (esto es, cuando existe consentimiento previo e inequívoco del afectado) debe existir causa justificada para ello.

Ahora bien, en este punto debemos plantearnos si mediante los mecanismos de cancelación (y, en su caso de rectificación) son suficientes para salvaguardar los derechos de los afectados, y la respuesta debe ser negativa. Debemos tener en cuenta que hoy en día las diversas opciones que dan las distintas redes sociales son muy amplias, siendo una de estas funciones la de poder compartir las publicaciones que otros usuarios han publicado. A ello hay que añadir que una vez publicadas, las distintas informaciones han podido ser copiadas. Por lo tanto, vemos que en estos supuestos podría suceder que la eliminación de tales datos no fuera total, puesto que los mismos han podido ser reproducidos o copiados por terceros.

Tal y como advierte Pere Simón Castellano[45], en estos supuestos la mejor solución pasa por una buena política de prevención, para lo cual se desarrollan diversas campañas cuyo objetivo es alertar a los usuarios de los riesgos de la exposición pública de su intimidad. En este sentido cabe destacar campañas como la iniciativa *REDponsables* llevada a cabo por la Consejería de Desarrollo Económico y el Colegio de Ingenieros Técnicos en Informática de Murcia o la *Conéctate seguro* cuyo objetivo es la prevención del acoso en Internet, llevada a cabo la Secretaría Nacional de Tecnología de la Información y Comunicación (Senatics), la Secretaría de la Niñez y la Adolescencia (SNNA) y la Secretaria de Información y Comunicación (Sicom).

[45] SIMÓN CASTELLANO, Pere (2012). El régimen constitucional del derecho al olvido digital, Madrid, Tirant lo Blanch.

La Agencia Española de Protección de Datos en su página web[46] contempla el protocolo que hay que seguir para poder ejercer el derecho al olvido en las redes sociales.

Finalmente, hay que poner de manifiesto que en principio la Comisión Europea va a presentar una propuesta legislativa que incluiría la protección del derecho al olvido en las redes sociales, lo que permitiría que todos los contenidos que los usuarios suben a una determinada red social quede eliminado una vez que se borra dicha cuenta. El objetivo de la Comisión Europea es, obviamente, reforzar la privacidad de millones de usuarios desprotegidos ante el poder de esas compañías. Por lo tanto, habrá que esperar a si la Comisión lleva a cabo este nuevo Proyecto.

V.3 El derecho al olvido respecto de los motores de búsqueda. Normativa.

En primer lugar, y de cara a tener una idea más clara acerca de los motores de búsqueda, hemos de analizar qué se entiende por motores de búsqueda. Así según Valentina Giraldo un motor de búsqueda es *un sistema encargado de buscar archivos almacenados en los servidores web.*[47]

Efectuada la anterior precisión, vamos a centrarnos en la problemática que se plantea en relación con estos instrumentos. Como punto de partida, debe tenerse en cuenta la importancia que tienen los motores de búsqueda en la difusión de la información en una sociedad como la actual.

La responsabilidad de los motores de búsqueda está contemplada en el artículo 17.1 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico que dispone que:

46 Agencia Española de Protección de Datos. Eliminar fotos y vídeos de internet. Recuperado de http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/eliminar_fotos_videos/index-ides-idphp.php.

47 Giraldo, Valentina. Los motores de Búsqueda y la utilidad que tienen. Recuperado de https://marketingdecontenidos.com/motores-de-busqueda/.

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o
b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

Vemos como el artículo anteriormente transcrito imputa la responsabilidad a los buscadores en aquellos supuestos en los que tienen un conocimiento efectivo de la ilicitud o de la información que enlazan. En este punto es necesario analizar qué ha de entenderse por “conocimiento efectivo”.

Pues bien, como no podía ser de otra manera, dicha cuestión ha sido analizada por nuestros tribunales. Así, la Audiencia Provincial de Madrid[48] se ha pronunciado en los siguientes términos:

[48] Sentencia de la Audiencia Provincial de Madrid Número 95 /2010 de fecha 19 de febrero de 2010 (JUR 2010\133011).

Con relación a que se entiende que ha existido ese conocimiento efectivo de la ilicitud de la información por parte del prestador del servicio , el propio legislador en aras de ese principio recogido en la Directiva Comunitaria que parte de que no puede imponerse a los prestadores de servicios una supervisión previa de dichos contenidos, da una definición y alcance que debe darse a conocimiento efectivo, que solo existirá cuando un órgano competente haya declarado la ilicitud de los datos ordenando su retirada, o se hubiera declarado la existencia de la lesión, lo que ha de entenderse que hasta ese momento , es decir que el prestador del servicio , en este caso GOOGLE , haya tenido conocimiento de la correspondiente resolución, en el ordenamiento jurídico español una resolución judicial, que haya ordenado la retirada de tales datos, o bien se haya declarado la existencia de la lesión, en el presente caso se hubiera dictado la correspondiente resolución judicial declarando que tales datos suponen una intromisión ilegítima en el honor del ahora apelante, pues hasta ese momento no puede entenderse que el proveedor del servicio haya tenido conocimiento efectivo y por lo tanto tenga que actuar con diligencia a los efectos de suprimir o inutilizar el enlace correspondiente.

El Tribunal Supremo[49], efectúa una interpretación más amplia del término "conocimiento efectivo":

Esta Sala en STS de 9 de diciembre de 2009 (RJ 2010, 131) , RC n.º 914/2006 y en STS 10 de febrero de 2011 (RJ 2011, 313) , RC n.º 1953/2008 realizó una interpretación del concepto de «conocimiento efectivo» a la luz de la Directiva traspuesta. Así se señaló que la LSSICE no se limitaba a incluir en los supuestos de exención de responsabilidad el conocimiento por parte del proveedor de resolución dictada por órgano competente que declarara la ilicitud, sino que incluía también, de conformidad con el artículo 16 de la LSSICE, la posibilidad de " otros medios de conocimiento efectivo que pudieran establecerse " -, como el conocimiento «que se obtiene por el prestador del servicio a partir de

[49] Sentencia del Tribunal Supremo Número 144/2013 de fecha 4 de marzo de 2013 (RJ 2013\338).

> *hechos o circunstancias aptos para posibilitar, aunque mediatamente o por inferencias lógicas al alcance de cualquiera, una efectiva aprehensión de la realidad de que se trate» o en palabras de la Directiva, en su artículo 14, « hechos o circunstancias por los que la actividad o la información revele su carácter ilícito ».*

Por lo tanto, nos encontramos con una acepción amplia del término "conocimiento efectivo" y ello por cuanto los motores serán conocedores de la ilicitud de una determinada actividad o información que enlazan no solo en los supuestos en que tal ilicitud haya sido declarada por el órgano competente, sino también en otros supuestos, como por ejemplo la comunicación por parte del afectado de la vulneración de sus derechos.

La respuesta lógica que cabría esperar por parte de los motores de búsqueda en aquellos casos en los que son conocedores de tal ilicitud, sería la retirada y desindexación de la información ilícita. Ahora bien, para el supuesto que no sea así, se arbitra en la Ley de servicios de la sociedad de la información y de comercio electrónico un procedimiento subsidiario para proteger los derechos de los ciudadanos. Concretamente en el artículo 8.1 del mencionado texto legal se dispone que:

> *En caso de que un determinado servicio de la sociedad de la información atente o pueda atentar contra los principios que se expresan a continuación, los órganos competentes para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas necesarias para que se interrumpa su prestación o para retirar los datos que los vulneran.*

Por lo tanto, vemos como la Ley arbitra un mecanismo para que los órganos competentes adopten las medidas necesarias para retirar las informaciones ilícitas. Por lo tanto, vemos como en estos supuestos se produce una confluencia de dos textos legales, esto es, la Ley Orgánica de Protección de Datos de Carácter Personal y la Ley de servicios de la sociedad de la información y de comercio electrónico que

permiten no solo exigir la cancelación de los datos personales, sino también ordenar y exigir directamente a los motores de búsqueda su retirada.

V.4 El derecho al olvido respecto de los motores de búsqueda. Evolución jurisprudencia. Principales controversias.

V.4.1. Sentencia de la Audiencia Provincial de Barcelona de fecha 8 de febrero de 2013.[50]

La primera Sentencia que reconoció el derecho al olvido como tal en España fue la sentencia de la Audiencia Provincial de Barcelona de fecha 8 de febrero de 2013.

El supuesto de hecho hacía referencia a la demanda interpuesta frente a un medio digital en la que se solicitara que se declarara que la noticia publicada por dicho medio constituía una intromisión ilegítima en su honor. En dicha noticia se ponía de manifiesto que el demandante había participado en el rapto de un empresario, que tenía numerosos antecedentes y que fue abatido de un tiro por la policía; y además se le calificaba de “implicado”, “sospechoso” y “delincuente”, añadiendo además que acumulaba más de media docena de detenciones y tenía diversas órdenes de búsqueda y captura, además de antecedentes por estafa, atentado contra agentes de la autoridad, tráfico de estupefacientes, robos de vehículos y delitos contra la seguridad del tráfico. A tal efecto, el demandante manifiesto además que la información no era veraz y que sus antecedentes penales habían sido cancelados.

La demanda fue desestimada por el Juzgado de Primera Instancia de Barcelona número CUATRO[51] que entendió que, puesto que se trataba de un personaje notorio, y que la noticia era de interés general, al ser además la información objetiva, era procedente el mantenimiento de dichos datos personales.

[50] Sentencia de la Audiencia Provincial de Barcelona Número 86/2013 de fecha 8 de febrero de 2013 (JUR 2013\111097).
[51] Sentencia del Juzgado de Primera Instancia de Barcelona número 4 de fecha 3 de septiembre de 2012 (JUR 2013\366988).

Dicha Sentencia fue recurrida por el demandante en apelación, y dio lugar a la Sentencia Número 86/2013 dictada por la Sección 14ª de la Audiencia Provincial de Barcelona que estimó el recurso de apelación interpuesto por el este.

Varias son las cuestiones que se analizan en la Sentencia de la Audiencia Provincial, que viene a hacer un análisis de los requisitos para que sea legítimo el mantenimiento de los datos en Internet.

Comienza en primer lugar analizando el interés legítimo de la información publicada, y a tal efecto pone de manifiesto que el hecho de que la policía persiga a una persona que no se detiene ante sus requerimientos y tenga que abatirlo con un tiro es de interés público y de suficiente entidad como para justificar la prevalencia del Derecho a la información sobre el derecho al honor y a la intimidad personal, y por ello concluye diciendo que:

> *El hecho noticioso era que no se detuvo ante los requerimientos de la policía y que por ello se disparó contra él (y eso, aunque comprobaciones posteriores hubiesen llevado a un desmentido). Si la noticia se hubiera limitado a estos hechos, estaría justificado referir el nombre completo del actor.*

Ahora bien, el problema que se planteó en el caso que nos ocupa, fue que junto con el hecho noticioso (que era verídico) se incluyó una descripción de los antecedentes penales que no era veraz, por lo que entendió que se lesionaba el derecho a la intimidad. Concretamente, analizando dicho extremo, la Audiencia Provincial se pronunció en los siguientes términos:

> *La mención de antecedentes delictivos faltos de veracidad por ser jurídicamente inexistentes y por omitir su antigüedad es suficiente para considerar infringido el derecho al honor, porque la noticia gira en torno a la fuga ante el requerimiento de detención por parte de los agentes de la autoridad y su implicación en la investigación del secuestro, hechos que el actor no niega, pero esta información inveraz en la forma de ser*

presentada implica un plus de afectación negativa de la afectación de la autoestima y en la consideración ajena.

Para finalmente concluir:

La parte apelada viene a sugerir que resolver la cuestión ahora atendiendo al llamado "derecho al olvido" alteraría los términos del debate, pero no es así porque ya en la demanda quedó claro que lo que pretendía el actor era que se reconociera afectado su honor al haber dado a conocer como ciertos, en términos de tiempo presente, unos antecedentes penales que ya estaban cancelados.

Todo ello conllevó la estimación parcial del recurso de apelación, condenando al medio digital, a abonar una indemnización que ascendía a 5.000.- euros, a la publicación de la Sentencia en versión papel y a que retirara de su página web la noticia en cuestión

Vemos por lo tanto como se produce un reconocimiento del derecho al olvido conectado con el derecho a la intimidad personal. Lo peculiar de esta Sentencia es que no nos encontramos con el ejercicio en vía administrativa de los derechos de cancelación u oposición ante la Agencia Española de Protección de Datos y, en su caso, el posterior recurso contencioso administrativo interpuesto frente a la resolución de esta ante la Audiencia Nacional, dando lugar al correspondiente procedimiento administrativo; sino que es la primera Sentencia de la jurisdicción civil en la que se ejercitan este tipo de pretensiones, sin ejercitar propiamente los derechos de cancelación y oposición en el procedimiento administrativo habilitado a tal efecto.

V.4.2. Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014[52].

El 13 de mayo de 2014 se publicó la Sentencia del Tribunal de Justicia de la Unión Europea mediante la que se daba respuesta a una serie de cuestiones que

[52] Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 (TJCE 2014\85).

habían sido planteadas por la Audiencia Nacional en el procedimiento contencioso administrativo surgido entre la Agencia Española de Protección de Datos y la entidad Google Inc., y su filial española, siendo el objeto de la controversia el derecho al olvido en Internet.

Antecedentes

En 1998 el diario La Vanguardia publicó dos anuncios referentes a la subasta de unos inmuebles provenientes de un embargo derivado de las deudas de un ciudadano español con la Seguridad Social. Evidentemente en el año 1998 la publicación de tales anuncios se efectuó en papel. Ahora bien, años después La Vanguardia decidió digitalizar su información, y por lo tanto los anuncios a los que hemos hecho referencia se incorporaron en su web.

El afectado por esta información contactó con los responsables de La Vanguardia y les solicitó que eliminaran los enlaces a esa información puesto que se trataba de una deuda ya saldada y el embargo se había resuelto y solucionado hace años Paralelamente, el afectado se dirigió a Google para solicitarle también la eliminación de tales enlaces. Dado que no se atendieron sus peticiones, el afectado interpuso una reclamación ante la Agencia Española de Protección de Datos frente a la Vanguardia y frente a Google. Dicha reclamación fue desestimada respecto del periódico la Vanguardia, ya que la Agencia Española de Protección de Datos entendió que la información estaba legalmente justificada atendiendo al principio de libertad de información.

Sin embargo, estimó la reclamación respecto de Google, ya que la Agencia entendió que la actividad llevada a cabo por los buscadores puede considerarse un tratamiento de datos y le exigió la adopción de las medidas necesarias para eliminar los datos de los resultados de búsqueda para impedir así el acceso a los mismos. Google rechazó esta petición y recurrió la resolución ante la Audiencia Nacional solicitando su nulidad.

La Audiencia Nacional planteó entonces tres cuestiones prejudiciales al Tribunal Superior de Justicia de la Unión Europea, que fueron las siguientes:

1) El ámbito territorial de aplicación de la Directiva de protección de datos 95/46/CE, y consecuentemente de la Ley Orgánica de Protección de Datos.

2) El papel del responsable de tratamiento de datos respecto de las actividades realizadas por el buscador a efectos de la Directiva 95/46/CE.

3) El alcance de los derechos de oposición y cancelación en relación con el derecho al olvido.

Pues bien, tal y como veremos a continuación el Tribunal Superior de Justicia de la Unión Europea se apartó por la postura mantenida por el Abogado General del Estado en su escrito de conclusiones, por ello a continuación, y con carácter previo a analizar la fundamentación de la Sentencia, haremos una breve mención al contenido de tales conclusiones.

Conclusiones del Abogado General del Estado

Respecto de la primera de las cuestiones, debemos tener en cuenta que para que resulte de aplicación la Directiva y la Ley Orgánica de Protección de Datos es preciso que se esté llevando un tratamiento de datos personales en un establecimiento del responsable que se encuentre ubicado en un estado miembro. A tal efecto Google alegó que en España no se estaba llevando cabo ningún tratamiento de datos. En este punto, el Abogado General concluye con que la actividad de los motores de búsqueda sí que constituye un tratamiento de datos y además también entiende que la normativa nacional en materia de protección de datos se le aplica a un buscador cuando este tiene un establecimiento en un Estado miembro que está orientado claramente a los habitantes de dicho Estado miembros.

Respecto del papel de Google en el tratamiento de datos, entiende que, si bien los motores de búsqueda de datos implican el tratamiento de tales datos, no puede

entenderse que Google sea responsable de dicho tratamiento y ello por cuanto se trata de una mera herramienta de búsqueda, sin que de ello pueda extrapolarse que tienen el control sobre todos los datos. Por lo tanto, el Abogado del Estado excluye la responsabilidad de los buscadores por tales motivos.

Finalmente, respecto del derecho al olvido, entiende que en la Directiva no aparece contemplado el mismo, y que solicitar a los buscadores que eliminen información legítima y legal implicaría una vulneración del derecho de expresión del editor de una determinada página web.

Contenido de la Sentencia del Tribunal Superior de Justicia de la Unión Europea.

En lo único que coincide el Tribunal y el Abogado General es en la cuestión relativa a la aplicabilidad de la Ley Orgánica de Protección de Datos, ya que al igual que el Abogado del Estado el Tribunal entiende que tanto la Directiva como la Ley Nacional (en este caso la Ley Orgánica de Protección de Datos) puede ser aplicada a un motor de búsqueda si dicho buscador tiene un establecimiento en el territorio de la normativa nacional que está orientado a los nacionales de dicho país. Por lo que, concluye que tanto la Directiva como la Ley Orgánica de Protección de Datos resultan aplicables al supuesto que nos ocupa.

Respecto de la segunda de las cuestiones, parte de la misma postura que el Abogado del Estado en el sentido de considerar que la actividad llevada a cabo por Google constituye un tratamiento de datos personales, pero discrepa en cuanto a la responsabilidad de los motores de búsqueda. Hemos de recordar que el Abogado General les eximía de toda responsabilidad por cuanto entendía que no tenían control sobre los datos; pues bien, el Tribunal entiende que sí que son responsables por cuanto son los que determinan los fines y los medios de dicha actividad. Por lo tanto, a partir de dicha afirmación, podemos concluir con que los prestadores de servicios de Internet también son responsables de los datos personales, en la medida en que sus servicios le permitan establecer un perfil más o menos detallado del interesado.

Finalmente, respecto de la cuestión del derecho al olvido entiende que la Directiva ampara el derecho de los ciudadanos a exigir a los motores de búsqueda la eliminación de la lista de resultados de aquellos enlaces que contienen datos personales, ahora bien, no en todos los casos, sino únicamente en los supuestos en los que el tratamiento de los mismos sea ilegítimo o devenga ilegítimo por el paso del tiempo. Sobre este último extremo el Tribunal señala en su Fundamento de Derecho 93º:

> *Incluso un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron.*

Por lo tanto, nos encontramos con un reconocimiento expreso del derecho al olvido por cuanto impone a los motores de búsqueda el deber de respetar los derechos de cancelación y oposición de los ciudadanos, debiendo consecuentemente eliminar los vínculos a otras páginas que contengan datos personales de los mismos siempre y cuando la información sea inadecuada, impertinente o innecesaria respecto del fin para el que la misma se trató.

V.4.3. Sentencia de la Audiencia Provincial de Barcelona de fecha 17 de julio de 2014[53].

Pues bien, nuevamente es la Audiencia Provincial de Barcelona, esta vez la Sección 16ª, la que dicta una Sentencia con unos pronunciamientos muy relevantes a nuestros efectos, ya que reconoce formalmente el derecho al olvido en España, en tanto que la primera realizaba un reconocimiento mucho más genérico directamente relacionado con los derechos de la personalidad.

[53] Sentencia de la Audiencia Provincial de Barcelona Número 364/2014 de fecha 17 de julio de 2014 (AC 2014\1661).

Los antecedentes son los siguientes: El Boletín Oficial del Estado de 18 de septiembre de 1999 publicó el Real Decreto de 27 de agosto de 1999 por el que se indultó al interesado la pena privativa de libertad pendiente de cumplimiento, a la que había sido condenado en sentencia de la Sala Segunda del Tribunal Supremo de 18 de enero de 1990. Esta sentencia resolvía el recurso de casación interpuesto contra otra de la Sección Quinta de la Audiencia Provincial de Madrid, de 26 de junio de 1986, que le condenaba como autor de un delito contra la salud pública, por hechos cometidos en el año 1981.

Posteriormente el interesado se dirigió al Boletín Oficial del estado y le explicó la problemática ante la que se encontraba puesto que cada vez que tecleaba su nombre y apellidos en Google, aparecía indexada una página de dicho Boletín que informaba sobre su indulto. A tal efecto hay que precisar que el indulto fue concedido en 1999 por un delito que se cometió en 1981. Por ello solicitaba al Boletín Oficial del Estado que procediera a la retirada de sus datos personales, ya que ello le estaba causando graves perjuicios. El Boletín Oficial del Estado le contestó aduciendo la obligatoriedad de la publicación de los Reales Decretos de Indulto en los términos en que exigía el artículo 30 de la Ley 1/1988, de 14 de enero, por la que se modifica la Ley de 18 de junio de 1870, estableciendo reglas para el ejercicio de la Gracia de Indulto.

Paralelamente, el interesado se dirigió a los buscadores Yahoo, y Google Spain para que retiraran las páginas del buscador que contenían sus datos personales. Ante dichas peticiones, Yahoo contestó al interesado requiriéndole para que le facilitara una serie de información con el objetivo de poder atender sus pretensiones, sin que dicha información fuera facilitara por el afectado. En cambio, Google Spain contestó mediante una respuesta automatizada.

Posteriormente, el interesado formuló ante la Agencia Española de Protección de Datos una solicitud de reclamación frente el Boletín Oficial del Estado, Google Spain y Yahoo. Dicho procedimiento finalizó mediante la resolución del Director de la

Agencia Española de Protección de Datos[54] mediante la que desestimaba la reclamación formulada frente al Boletín Oficial del Estado, estimaba la reclamación y el derecho de oposición frente a Google Spain instándole a que adoptara las medidas necesarias para evitar el acceso a tales datos e igualmente estimaba la reclamación frente a Yahoo al considerar pertinente la eliminación de tales datos (si bien, teniendo en cuenta que el buscador se había dirigido al afectado solicitándole una serie de datos para poder atender sus peticiones, no siendo dicha solicitud atendida por parte del interesado).

Poco después, el interesado remitió a Telefónica y a Lycos un correo electrónico en los que hacía referencia a los buscadores Terra y Lycos y nuevamente solicitó que se retiraran las páginas del buscador que contenían sus datos personales. Telefónica respondió y a tal efecto puso de manifiesto que los datos personales del afectado no aparecían cuando se realizaba una búsqueda en la página de Terra y adjuntaba una copia de pantalla. Nuevamente, el afectado inició otro procedimiento esta vez frente a las entidades Telefónica y a Lycos, que fue estimado[55] respecto de Telefónica por motivos formales (ya que había cancelado los datos fuera de plazo) y la desestimó contra Lycos porque no constaba la recepción por esta empresa de la solicitud del demandante y porque no existía información acerca del administrador de la empresa en España.

La demanda que dio origen a este procedimiento finalmente se presentó frente a Google Spain, Telefónica, y Yahoo y fue presentada una vez que se habían emitido las resoluciones de la Agencia Española de Protección de Datos. La petición del demandante era que se declarara que se había vulnerado su derecho a la intimidad personal y familiar, a la imagen y al honor, que se ordenara a los buscadores retirar sus datos personales de las indexaciones y que se le indemnizara como consecuencia de los daños sufridos al haberse vulnerado su derecho a la protección de datos de carácter personal.

[54] Resolución de la Agencia Española de Protección de Datos R/02694/2009 de fecha 19 de enero de 2010.

[55] Resolución de la Agencia Española de Protección de Datos R/01553/2010 de fecha 8 de julio de 2010.

Evidentemente y, a diferencia de lo que ocurría con la Sentencia dictada por la sección 14ª de la Audiencia Provincial de Barcelona, en este caso existía un pronunciamiento previo por parte de la Agencia Española de Protección de Datos. Pues bien, una vez que la demanda fue admitida, las distintas entidades demandadas procedieron a eliminar los datos en cuestión, por lo que el demandado en la Audiencia Previa renunció a dicha pretensión. Sin embargo, siguió adelante con la pretensión indemnizatoria ejercitada por los daños causados. La Sentencia dictada en primera instancia por el Juzgado Número Ocho de Barcelona[56] fue íntegramente desestimada y ello por varias razones:

- En primer lugar, consideró que en el momento en que se había interpuesto la demanda, la acción había caducado, al haber transcurrido ya el plazo de cuatro años. A tal efecto, fijó como *dies a quo* el día en que el afectado tuvo conocimiento de que tras introducir sus datos personales en los buscadores aparecían sus datos personales.

- En segundo lugar, entendió que no era posible atender su petición de indemnización con base en el artículo 1902 del Código Civil al no resultar aplicable el mismo atendiendo al principio de especialidad normativa.

- Y finalmente, respecto de la vulneración del derecho a la protección de datos, el Juzgador de Primera Instancia entendió que los buscadores no podían ser responsables de los daños y perjuicios derivados del acceso al contenido en el Boletín Oficial del Estado hasta la publicación y notificación de las resoluciones de la Agencia Especial de Protección de Datos, y, al no ser firmes las mismas, no procedía tampoco una indemnización de daños y perjuicios por la vulneración de dicho derecho.

[56] Sentencia del Juzgado de Primera Instancia Número 8 de Barcelona de fecha 14 de noviembre de 2011 (JUR 2015\296352).

Dicha Sentencia fue recurrida por el demandante ante la Audiencia Provincial de Barcelona, y dicho recurso fue parcialmente estimado, tal y como veremos a continuación.

Como punto de partida, entiende la Audiencia Provincial que el afectado goza de una doble protección: por un lado tiene la posibilidad de acudir a la Agencia Española de Protección de Datos para la salvaguarda de sus derechos y por otro lado puede acudir a la vía civil para la reclamar la correspondiente indemnización, sin que sea necesario como requisito previo para solicitar una reclamación en la vía civil, el haber interpuesto previamente una reclamación ante la Agencia Española de Protección de Datos. Concretamente, en su Fundamento de Derecho Diecisieteavo se pronuncia en los siguientes términos:

> *Ya se han distinguido los dos planos de la actuación que la normativa de protección de datos atribuye al afectado: la reclamación ante la AEPD y la acción civil de indemnización. Ésta última, objeto del juicio, no exige como presupuesto la reclamación administrativa, sino: (1) un incumplimiento del responsable o encargado del tratamiento de datos personales y (2) que ese incumplimiento haya causado un daño indemnizable.*

Pues bien, una vez que efectuó dicha precisión, la Audiencia Provincial de Barcelona entró a analizar el fondo de la cuestión, y sus pronunciamientos fueron bastante dispares respecto de la Sentencia dictada en primera instancia, tal y como se expone a continuación:

- En primer lugar, entiende que no se ha producido la caducidad de la acción, y ello por cuanto el dies a quo a partir del cual deben computarse los cuatro años es aquel en el que los motores de búsqueda demandados dejaron de publicar los datos personales del demandado.

- En segundo lugar, entiende que se vulneran los derechos al honor y a la intimidad del demandante por parte de los buscadores al enlazar a los usuarios

de internet con el contenido del Boletín Oficial del Estado en el que se publicaba los datos relativos al indulto del afectado.

Pues bien, la Audiencia Provincial desestimó el recurso respecto de telefónica y ello por cuanto no se había acreditado la titularidad de esta del buscador Lycos y porque tampoco se había acreditado que mediante el buscador Terra (que era de su propiedad) se hubiera producido una infracción de los derechos del recurrente.

La Audiencia también desestimó la solicitud de condena de Yahoo, ya que no se había atendido la petición de Yahoo en relación a los enlaces que deseaba que no fueran demostrados y porque además cuando presentó la reclamación ante la Agencia Española de Protección de Datos, dichos enlaces ya estaban bloqueados.

Finalmente, y con base en la Sentencia del Tribunal Superior de Justicia de la Unión Europea, la Audiencia entendió que había habido un incumplimiento de la normativa de protección de datos por parte de Google y ello porque el enlace a la página del Boletín Oficial del Estado en que se publicaba el indulto concedido al demandante aparecía destacado en la lista de resultados de las búsquedas que se hacían en Google utilizando su nombre.

Entendió que la conducta de Google era antijurídica, y por lo tanto contraria a la normativa de protección de datos porque Google, a pesar de conocer la ilicitud del tratamiento de datos que llevaba a cabo (porque así se plasmó en la resolución de la Agencia Española de Protección de Datos) no eliminó los mismos hasta después de interpuesta la demanda, produciéndose un daño en el afectado desde el periodo que medió entre la notificación de la resolución de la Agencia Española de Protección de Datos y el momento en que se produjo la retirada de tal información. Concretamente, la Audiencia Provincial se pronuncia en los siguientes términos:

> *Consideramos que es la decisión de la AEPD (R/02694/2009, del procedimiento TD/00921/2009) de 19 de enero de 2010, que estimó la reclamación del actor contra Google Spain y que instó a esta entidad a que adoptara las medidas necesarias para retirar los datos de su índice e*

imposibilitar el acceso futuro a los mismos -o más exactamente, la notificación de esa resolución- la que marca el momento en que el mantenimiento del resultado controvertido en el índice del buscador deviene incumplimiento culpable de las normas legales de protección de datos. Con la lectura de la resolución motivada de la AEPD, Google Spain debía conocer la antijuricidad de su actuación.

Para finalmente concluir con que:

La conclusión es la ya expuesta: la demandada incumplió la legislación de protección de datos personales en el periodo de 22 de enero a 29 de noviembre de 2010.

Es decir, la Audiencia entendió que, durante un plazo de diez meses, y a pesar de la resolución de la Agencia Española de Protección de Datos se mantuvieron los datos personales del recurrente en el índice del buscador, vulnerándose así sus derechos.

Es muy importante el matiz que se introduce en la Sentencia, y es que la Audiencia Provincial niega la correlación entre incumplimiento de la normativa de protección de datos y el derecho a obtener una indemnización por ello, es decir, no todo incumplimiento conlleva una indemnización.

En el caso concreto, la Audiencia Provincial entendió que se había producido un daño moral por el tratamiento de los datos personales del demandante durante el periodo de diez meses al que hemos hecho referencia vulnerándose su derecho al honor y a la intimidad, por lo que fijó una indemnización de 8.000 euros.

Pues bien, la Sentencia que nos ocupa es muy relevante por dos cuestiones:

- En primer lugar, porque reconoce formalmente y de forma más precisa el derecho al olvido, ya que conecta las facultades de cancelación y oposición de

datos con el derecho fundamental a la protección de datos de carácter personal.

- Y, en segundo lugar, porque determina el momento a partir del cual empieza a correr el plazo de caducidad de cuatro años para el ejercicio de la acción, entendiendo que dicho plazo de caducidad no empieza a contar hasta que la intromisión ilegítima que afecte a los derechos de la personalidad no cese.

Ahora bien, la importancia de esta Sentencia no se queda aquí, y ello por cuanto la misma fue además recurrida ante el Tribunal Supremo. Así, se interpuso por parte de Google recurso de casación y recurso extraordinario por infracción procesal contra la Sentencia de la Audiencia Provincial de Barcelona que nos ocupa, recursos que fueron admitidos por el Tribunal Supremo mediante Auto[57] de fecha 9 de septiembre de 2015, y cuyo análisis se efectuará en el apartado V.4.5., del presente trabajo.

V.4.4. Sentencia del Tribunal Supremo de fecha 15 de octubre de 2015[58]: primera Sentencia del Tribunal Supremo que reconoce el derecho al olvido.

Si bien en el apartado anterior hemos hecho referencia a la Sentencia del Tribunal Supremo de fecha 5 de abril de 2016 entendemos que resulta pertinente, antes de entrar a analizar el contenido de esta, proceder a estudiar la dictada por el Tribunal Supremo con fecha 15 de octubre de 2015 y ello por cuanto nos encontramos con la primera Sentencia dictada por el Tribunal Supremo relativa al derecho al olvido.

Para una mejor comprensión, comenzaremos por hacer un breve resumen de los antecedentes al fallo del Tribunal Supremo. Los actores son dos personas que fueron detenidas por tráfico de drogas, quienes además en el momento de su detención hirieron a una serie de personas, siendo una de ellas, el familiar de un político.

[57] Auto del Tribunal Supremo de fecha 9 de septiembre de 2015 (JUR 2015\216224).

[58] Sentencia del Tribunal Supremo Número 545/2015 de fecha 15 octubre de 2015(RJ 2015\4417).

Dicha noticia fue publicada por un periódico de tirada nacional, El País, (obviamente en versión papel) y en la misma se recogieron los hechos acaecidos, incluyendo además el tratamiento médico facilitado a los detenidos para atener su síndrome de abstinencia. En dicha noticia, los detenidos estaban perfectamente identificados. Finalmente, los detenidos (y, posteriormente los demandantes) fueron condenados por un delito de contrabando.

Prácticamente veinte años después, El País, elaboró una hemeroteca digital de libre acceso, sin que la misma tuviera ningún tipo de protección para la noticia que nos ocupa, de tal manera que si se tecleaban en un motor de búsqueda los datos personales de los demandantes, aparecía el enlace a la versión digital de dicha hemeroteca, y consecuentemente a la noticia descrita anteriormente, relativa a la detención de los mismos.

Por todo ellos los afectados se dirigieron al citado periódico, para solicitar que cesara el tratamiento de sus datos personales en la página web, o en su defecto que los anonimizara mediante el empleo únicamente de sus iniciales, así como que adoptara las medidas necesarias para que la página web de la noticia no fuera indexada por los motores de búsqueda de Internet.

Dicha petición fue denegada amparándose para ello el País en el derecho de libertad de información, lo cual conllevó que se interpusiera por los afectados la correspondiente demanda en la que solicitaban 1) Que se declarara que la difusión de sus datos personales efectuada por El País a través de su página web, suponía una vulneración del derecho a la intimidad y al honor, 2) Que se condenara a la entidad demandada a que cesara en el uso de sus datos personales o que se anonimizaran los mismos, 3) Que se obligara al País a implantar las medidas necesarias para evitar que sus datos personales fueran indexados por los proveedores de servicios de intermediación de búsqueda cuando se realizara una búsqueda introduciendo sus datos personales incluida la búsqueda en la propia hemeroteca, 4) Que se les indemnizara por los daños causados, 5) Que se le condenara a no publicar en ninguna noticia sus datos personales, 6) Y finalmente, que se notificara la Sentencia a los distintos proveedores de servicios de intermediación de búsqueda.

El Juzgado de Primera Instancia[59] estimó la demanda y declaró que la difusión de la noticia realizada por Ediciones El País suponía una vulneración del derecho al honor, intimidad y protección de datos de los demandantes, ya que entendió que la publicación de dicha noticia no tenía una finalidad legítima, puesto que la finalidad de información tuvo lugar cuando se publicó por primera vez, y sin embargo el volcado de dicha noticia en la versión digital únicamente tenía una finalidad mercantilista, sin que esta pudiera prevalecer sobre los derechos al honor, a la intimidad y a la protección de datos de los demandantes.

El País interpuso Recurso de Apelación frente a la Sentencia del Juzgado de Primera Instancia de Barcelona, alegando la caducidad de la acción y la ausencia vulneración de los derechos fundamentales al honor, la intimidad y la protección de datos.

Los demandantes, no solo se opusieron al recurso de apelación, sino que también recurrieron la Sentencia dictada en Primera Instancia al entender que la misma adolecía de un vicio de incongruencia omisiva, ya que no el Juez no se había pronunciado sobre su petición de cese del tratamiento de sus datos personales o de sustitución de los mismos por sus iníciales, ni tampoco sobre su petición relativa a la omisión de tales datos en cualquier noticia que fuera publicada por El País.

La sentencia de la Audiencia Provincial[60] desestimó el recurso de apelación de Ediciones El País estimó el recurso interpuesto por los afectados, declarando la obligación del periódico de cesar en el uso de los datos personales en la página web que contenía la noticia e igualmente, a no mencionarlos en cualquier noticia que se publicara relacionada con el caso.

[59] Sentencia del Juzgado de Primera Instancia 21 de Barcelona de fecha de 4 octubre 2012 (JUR 2014\4375).
[60] Sentencia de la Audiencia Provincial de Barcelona Número 486/2013 de fecha 11 octubre de 2013 (AC 2013\1921).

La Sentencia de la Audiencia Provincial de Barcelona fue recurrida por El País ante el Tribunal Supremo, siendo admitido dicho recurso mediante Auto[61] de fecha 9 de septiembre de 2014.

Los motivos en los que se fundamenta el recurso de casación son dos:

- Caducidad de la acción.
- En segundo lugar, entiende que su actuación está amparada por la libertad de expresión y formación, que los hechos de la noticia tienen son de interés público, y que el transcurso del tiempo no hace que el mismo desaparezca y que el tratamiento de datos personales que efectúa está amparado por la libertad de información.

Respecto de la caducidad de la acción, y en los mismos términos en lo que ya se había pronunciado, entre otras, la Audiencia Provincial de Barcelona en su Sentencia de fecha 17 de julio de 2014 anteriormente analizada, entiende que no se ha producido la caducidad de acción y ello por cuanto nos encontramos ante un daño continuado, y por lo tanto hasta que no se produzca el cese del daño, no empieza a computar el plazo de cuatro años.

Respecto de la segunda de las cuestiones, entra en primer lugar a analizar la responsabilidad de los editores de la página web y como no podía ser de otra manera, entiende que resultan responsables de los tratamientos de datos personales que en las mismas se efectúen. Concretamente, en su Fundamento de Derecho Quinto se pronuncia en los siguientes términos:

> *Aunque la STJUE del caso Google analizó la responsabilidad de los gestores de motores de búsqueda en Internet (tales como Google, Yahoo, Bing, etc.) por el tratamiento de datos personales en informaciones contenidas en páginas web cuyos vínculos aparecían en la lista de resultados de tales buscadores cuando los datos personales (en concreto el nombre y apellidos) eran utilizados como palabras clave para la*

[61] Auto del Tribunal Supremo de fecha 9 septiembre 2014 (JUR 2014\246001).

> *búsqueda, ello no significa que los editores de las páginas web no tengan la condición de responsables del tratamiento de esos datos personales, con los consiguientes deberes de respetar el principio de calidad de datos y atender el ejercicio de los derechos que la normativa de protección de datos otorga a los afectados, y la responsabilidad derivada de no respetar estas exigencias legales. Los editores de páginas web tienen la posibilidad de indicar a los motores de búsqueda en Internet que desean que una información determinada, publicada en su sitio, sea excluida total o parcialmente de los índices automáticos de los motores, mediante el uso de protocolos de exclusión como robot.txt, o de códigos como noindex o noarchive. Así lo recuerda la STJUE del caso Google en su párrafo 39.*

Posteriormente, entra a ponderar el tratamiento de los datos personales con el derecho a la información, partiendo para ello de la veracidad de los datos. Ahora bien, debe tenerse en cuenta que la veracidad de los datos, no implica que el tratamiento de los mismos sea lícito, y ello por cuanto debe tenerse en cuenta la finalidad con la que los mismos fueron recogidos. Finalidad que debe analizarse tanto en el momento de su recogida, como durante todo el tiempo en el que se produce dicho tratamiento, por lo que se centra el Tribunal en analizar si la digitalización de la hemeroteca del País conlleva un tratamiento lícito de tales datos que justifique el mantenimiento de los mismos.

Con base en la jurisprudencia del Tribunal Europeo de los Derechos Humanos el Tribunal Supremo entiende que hay que distinguir la función que tiene la empresa, por cuanto informa a la sociedad de los diversos acontecimientos que tienen lugar, de la función de las hemerotecas creadas, ya que en este segundo caso, la labor propiamente informativa pasa a un segundo plano, de tal manera que son los Estados miembros los que tienen que entrar a valorar el equilibrio entre el derecho a la protección de datos, a la intimidad personal, familiar, el derecho al honor y el derecho a la información a través de las hemerotecas. Entiende el Tribunal Supremo que, en determinados casos, y a pesar del transcurso del tiempo, la publicación de determinados datos personales está justificado por el interés público. Especialmente relevante resulta la diferencia que establece entre “interés del público” e “interés

público" como criterio para sostener la procedencia o no de un determinado tratamiento de datos. Por su claridad, transcribimos dicho apartado:

> *Este interés no puede confundirse con el gusto por el cotilleo o la maledicencia. Como ha dicho algún autor, lo relevante no es tanto el "interés del público" (si se considerara que es amplio el sector de la población que quiera conocer las miserias de sus conciudadanos, aun las sucedidas mucho tiempo antes), sino el "interés público", esto es, el interés en formarse una opinión fundada sobre asuntos con trascendencia para el funcionamiento de una sociedad democrática. Este interés puede justificar que, cuando se trata de personas de relevancia pública, una información sobre hechos que afectan a su privacidad o a su reputación, aun sucedidos mucho tiempo atrás, esté vinculada a sus datos personales en un tratamiento automatizado como el que suponen las consultas a través de motores de búsqueda en Internet que indexan los datos personales existentes en las hemerotecas digitales. Las relaciones sociales se basan en buena medida en la información que tenemos de los demás, y el capital moral con que cuenta cada persona depende, en parte, del grado de confianza que inspire su trayectoria vital. Por eso, cuando concurra este interés en la información, está justificado que puedan ser objeto de tratamiento automatizado informaciones lesivas para la privacidad y la reputación, vinculadas a los datos personales, siempre que sean veraces, cuando se trata de personas de relevancia pública, aunque los hechos hayan sucedido hace mucho tiempo.*

Pues bien, en el caso analizado, los afectados eran personas anónimas, y por lo tanto carentes de interés público. Evidentemente, la comisión de un delito de contrabando tiene por sí solo relevancia a efectos de su conocimiento por parte de la sociedad. Ahora bien, sobre dicho extremo entiende el Tribunal Supremo que el denominado "interés público" se vio satisfecho en el momento en que se publicó la Sentencia a través de la versión papel, pero no se puede emplear el recurso al "interés público" para justificar el tratamiento de los datos personales de los afectados, de tal manera que cada vez que se realice una búsqueda en internet empleado sus nombres

y apellidos, aparezcan los enlaces a la hemeroteca digital, y ello por cuanto tales acontecimientos han perdido interés histórico como consecuencia del anonimato de los sujetos y del transcurso del tiempo.

Por lo tanto, a pesar de la veracidad de la información, entiende el Tribunal Supremo que no concurre el requisito de pertinencia, causando el tratamiento un daño injustificado a los afectados. Por su claridad, se transcribe a continuación el fragmento de la Sentencia:

> *Ciertamente eran hechos veraces. Pero la licitud del tratamiento de los datos personales no exige solamente su veracidad y exactitud, sino también su adecuación, pertinencia y carácter no excesivo en relación con el ámbito y las finalidades para las que se haya realizado el tratamiento (art. 6.1.d de la Directiva y 4.1 LOPD). Y esos requisitos no concurren en un tratamiento de estos datos personales en que una consulta en un motor de búsqueda de Internet que utilice sus nombres y apellidos permita el acceso indiscriminado a la información más de veinte años después de sucedidos los hechos, y cause un daño desproporcionado a los afectados. El tratamiento de esos datos personales pudo cumplir estos requisitos de calidad de los datos en las fechas cercanas al momento en que los hechos se produjeron y conocieron, pero el paso del tiempo ha supuesto que el tratamiento de estos datos vinculados a hechos pretéritos sea inadecuado, no pertinente y excesivo para la finalidad del tratamiento (en este sentido, STJUE del caso Google, párrafos 92 y 93).*

Evidentemente el mero hecho de que transcurra el tiempo, y el tratamiento de datos pierda la finalidad originaria, no implica que el editor por su propia iniciativa tenga que eliminar tales datos. Ahora bien, sí que le es exigible que atienda las peticiones de los afectados que ejerciten sus derechos de cancelación y oposición, siempre y cuando concurran los requisitos para ello.

Sin duda alguna, el pronunciamiento más importante de la Sentencia lo encontramos en el apartado octavo del Fundamento de Derecho Quinto, y ello por

cuanto es la primera vez que se produce la delimitación del derecho al olvido por parte de la Sala Civil del Tribunal Supremo, disponiendo que:

> *8.- El llamado "derecho al olvido digital", que es una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento de datos personales, no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos.*
>
> *Tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículo a su gusto, controlando el discurso sobre sí mismos, eliminando de Internet las informaciones negativas, "posicionando" a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones. De admitirse esta tesis, se perturbarían gravemente los mecanismos de información necesarios para que los ciudadanos adopten sus decisiones en la vida democrática de un país.*
>
> *Pero dicho derecho sí ampara que el afectado, cuando no tenga la consideración de personaje público, pueda oponerse al tratamiento de sus datos personales que permita que una simple consulta en un buscador generalista de Internet, utilizando como palabras clave sus datos personales tales como el nombre y apellidos, haga permanentemente presentes y de conocimiento general informaciones gravemente dañosas para su honor o su intimidad sobre hechos ocurridos mucho tiempo atrás, de modo que se distorsione gravemente la percepción que los demás ciudadanos tengan de su persona, provocando un efecto estigmatizador e impidiendo su plena inserción en la sociedad, inserción que se vería obstaculizada por el rechazo que determinadas informaciones pueden causar en sus conciudadanos.*

Pues bien, el Tribunal Supremo se aleja del fallo de la Audiencia Provincial de Barcelona (que recordemos que estimó íntegramente el recurso de apelación de los afectados y desestimó el interpuesto por El País) y estima parcialmente el recurso interpuesto por el periódico al entender que no resultan procedentes las medidas consistentes en impedir la descripción de las noticias, así como la imposibilidad de buscar en la propia hemeroteca la noticia relativa a los afectados. Por todo ello confirmó parcialmente la Sentencia de la Audiencia Provincial, revocando los pronunciamientos relativos a la supresión de los datos personales en el código fuente y del nombre, apellidos o incluso iniciales, y a la prohibición de indexar los datos personales para su uso por el motor de búsqueda interno de la hemeroteca digital.

Vemos como con esta Sentencia se da un paso más allá, por cuanto hasta ahora los principales pronunciamientos que habían tenido lugar en relación con el derecho al olvido, se centraban en el análisis de la responsabilidad de los motores de búsqueda, y en esta Sentencia se da un paso más y se amplía el ámbito subjetivo del mentado derecho por cuanto también se extrapola a los editores de contenidos digitales.

V.4.5. Sentencia del Tribunal Supremo de fecha 5 de abril de 2016[62].

Con fecha 5 de abril del 2016 el Tribunal Supremo resolvió los recursos interpuestos contra la Sentencia de la Audiencia Provincial de Barcelona de fecha 17 de julio de 2014 y a los que hemos hecho referencia en el apartado V.4.3. del presente trabajo.

En primer lugar y respecto de la falta de legitimación pasiva aducida por parte de Google, el Tribunal Supremo entendió, que Google Spain puede ser considerada en sentido amplio como responsable del tratamiento de datos, y ello a pesar de que Google Inc. es el responsable de tratamiento de datos tal y como así se plasma en la Sentencia del Tribunal de Justicia de la Unión Europea. Consecuentemente, y al poder considerarse a Google Spain como responsable del tratamiento de datos está legitimada pasivamente para ser parte demandada, ratificando así el pronunciamiento

[62] Sentencia del Tribunal Supremo Número 210/2016 de fecha 5 de abril de 2016 (RJ 2016\1006).

que había efectuado sobre dicho extremo la Audiencia Provincial de Barcelona. Concretamente, en su Fundamento de Derecho Tercero apartado sexto dispone que:

> *Sentado lo anterior, siendo cierto que Google Inc, en tanto que gestor del motor de búsqueda Google Search, es responsable del tratamiento de datos, y así lo declara la STJUE del caso Google al resolver, en la primera parte de la sentencia, la cuestión de si la actividad de un motor de búsqueda constituye tratamiento de datos personales en el sentido del art. 2.b de la Directiva (apartado 33), también lo es que Google Spain puede ser considerada, en un sentido amplio, como responsable del tratamiento de datos que realiza el buscador Google Search en su versión española (www.google.es), conjuntamente con su matriz Google Inc y, por tanto, está legitimada pasivamente para ser parte demandada en los litigios seguidos en España en que los afectados ejerciten en un proceso civil sus derechos de acceso, rectificación, cancelación y oposición, y exijan responsabilidad por la ilicitud del tratamiento de datos personales realizado por el buscador Google en su versión española.*
>
> *Por ello debe considerarse correcta la afirmación de la Audiencia Provincial de que Google Spain está legitimada pasivamente para soportar la acción ejercitada por una persona afectada por el tratamiento de esos datos personales realizado por el buscador Google en defensa de sus derechos de la personalidad y de su derecho a la protección de datos personales.*

Pues bien, igual que sucedía en la anterior Sentencia del Tribunal Supremo, nuevamente se establece que el hecho de que unos determinados datos personales sean exactos y verdaderos no implica que el tratamiento de los mismos sea lícito, sino que con el paso del tiempo dicho tratamiento puede devenir ilícito. Concretamente, se pronuncia en los siguientes términos:

> *10.- Ahora bien, un tratamiento de datos que es lícito inicialmente, por respetar las exigencias de calidad de datos, puede, con el paso del*

tiempo, dejar de serlo. El factor tiempo tiene una importancia fundamental en esta cuestión, puesto que el tratamiento de los datos personales debe cumplir con los requisitos que determinan su carácter lícito y, en concreto, con los principios de calidad de datos (adecuación, pertinencia, proporcionalidad y exactitud), no solo en el momento en que son recogidos e inicialmente tratados, sino durante todo el tiempo que se produce ese tratamiento. Un tratamiento que inicialmente pudo ser adecuado a la finalidad que lo justificaba puede devenir con el transcurso del tiempo inadecuado para la finalidad con la que los datos personales fueron recogidos y tratados inicialmente, y el daño que cause en derechos de la personalidad como el honor y la intimidad, desproporcionado en relación al derecho que ampara el tratamiento de datos.

En este sentido, el apartado 93 de la STJUE del caso Google declaraba que «incluso un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron. Este es el caso, en particular, cuando son inadecuados, no pertinentes o ya no pertinentes o son excesivos en relación con estos fines y el tiempo transcurrido».

Lo cual lleva al Tribunal Supremo a ratificar el pronunciamiento que sobre dicho extremo había efectuado la Audiencia Provincial de Barcelona.

Finalmente, se alega por parte de Google que se ha vulnerado por parte de la Audiencia Provincial el principio de seguridad jurídica ya que en su Sentencia dictaminó que se había producido un incumplimiento del derecho de que no existía cuando sucedieron los hechos enjuiciados, al no estar contemplado en ningún texto legal y al no haberse dictado aún la Sentencia del Tribunal de Justicia de la Unión Europea de fecha 13 de mayo de 2014.

Resuelve acertadamente el Tribunal Supremo poniendo de manifiesto que el objeto de la Sentencia del Tribunal de Justicia de la Unión Europea de fecha 13 de

mayo de 2014 fue atender una serie de cuestiones prejudiciales planteadas por la Audiencia Nacional, sin que de ello quepa extrapolar que fue en esa Sentencia en la que se estableció la regulación del derecho al olvido, ya que el objeto de la misma fue interpretar la normativa en materia de protección de datos aplicable al caso en cuestión. Nuevamente el Tribunal Supremo en esta Sentencia delimita el alcance del derecho al olvido, y a tal efecto determina que:

> *El derecho al olvido digital no fue, por tanto, una creación del TJUE, ni lo fueron las normas en las que este se sustenta. El TJUE declaró qué interpretación debía darse a unas normas preexistentes, y más concretamente, a la Directiva 95/46/CE (LCEur 1995, 2977) 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. El derecho al olvido digital es, pues, una concreción en el ámbito de Internet de los derechos derivados de los requisitos de calidad del tratamiento de datos personales, y más concretamente de los arts. 2 , 6 , 7 , 9 , 12 y 14 de la Directiva, así como el art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (RCL 1999, 1190, 1572) , que establece el derecho al respeto de la vida privada y familiar, convenio cuya trascendencia en el Derecho de la Unión resulta de los arts. 52 y 53 de la Carta de Derechos Fundamentales de la Unión Europea (LCEur 2000, 3480) , que se encontraban en vigor cuando sucedieron los hechos que han motivado el pronunciamiento condenatorio de Google Spain que aquí se recurre.*

V.4.6. Discrepancias de las Sentencias de las distintas Salas del Tribunal Supremo.

La problemática se plantea en relación al concepto de responsable de tratamiento de datos, siendo diferente la postura adoptada por la Sala de lo Civil del Tribunal Supremo de la adoptada por la sala de lo Contencioso Administrativo.

Como hemos visto en el apartado V.4.5., el Tribunal Supremo en su Sentencia de fecha 5 de abril de 2016 interpreta, entre otras cosas, el concepto de responsable de tratamiento de datos personales. Concretamente, se centran en analizar si la filial Google Spain (domiciliada en España) puede ser considerada del tratamiento de datos realizado por el buscador Google, y que es directamente gestionado por Google Inc. (domiciliado en Estados Unidos). Pues bien, aunque parezca inverosímil, las posturas que se recogen en las Sentencias emitidas por las distintas Salas son contradictorias.

La primera Sala que se pronunció sobre la responsabilidad de Google Spain, fue la Sala de lo Contencioso Administrativo[63], que entendió que Google Spain no podía ser responsable del tratamiento de datos y ello por cuanto se había acreditado que Google Inc era el encargado de la gestión el buscador. Se transcribe a continuación el extracto de la Sentencia en el que exonera de responsabilidad a Google Spain:

> *Hablar de corresponsabilidad supone un examen de la situación fáctica y comprobar que la entidad en cuestión tiene una participación concreta e identificada en la determinación de los fines y medios del tratamiento de que se trate, tratamiento que en este caso y según se declara por el TJUE al dar respuesta a la cuestión prejudicial planteada por la Sala de instancia, " consiste en hallar información publicada o puesta 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". En este caso no se identifica por la Sala de instancia ninguna actividad de Google Spain que suponga la participación en esa actividad del motor de búsqueda. Por el contrario, y como recoge el TJUE en el fundamento 46 de la citada sentencia, el tribunal remitente señala que Google Inc. gestiona técnica y administrativamente Google Search y que no está probado que Google Spain realice en España una actividad directamente vinculada a la indexación o almacenamiento de información o de datos contenidos en los sitios de Internet de terceros*

[63] Sentencia del Tribunal Supremo Número 574/2016 de fecha 14 marzo de 2016 (RJ 2016\1071).

Por lo que acaba concluyendo:

> *De ahí que solo Google Inc. es la responsable del tratamiento pues a ella corresponde en exclusiva la determinación de los fines, las condiciones y los medios del tratamiento de datos personales.*

Pues bien, menos de un mes después la Sala de lo Civil del Tribunal Supremo en su Sentencia de fecha 5 de abril de 2016 se apartó del criterio establecido por la Sala de lo Contencioso Administrativo e imputó responsabilidad en el tratamiento de los datos a Google Spain en los siguientes términos:

> *Sentado lo anterior, siendo cierto que Google Inc, en tanto que gestor del motor de búsqueda Google Search, es responsable del tratamiento de datos, y así lo declara la STJUE del caso Google al resolver, en la primera parte de la sentencia, la cuestión de si la actividad de un motor de búsqueda constituye tratamiento de datos personales en el sentido del art. 2.b de la Directiva (apartado 33), también lo es que Google Spain puede ser considerada, en un sentido amplio, como responsable del tratamiento de datos que realiza el buscador Google Search en su versión española (www.google.es), conjuntamente con su matriz Google Inc y, por tanto, está legitimada pasivamente para ser parte demandada en los litigios seguidos en España en que los afectados ejerciten en un proceso civil sus derechos de acceso, rectificación, cancelación y oposición, y exijan responsabilidad por la ilicitud del tratamiento de datos personales realizado por el buscador Google en su versión española.*

Es necesario poner de manifiesto que, en el procedimiento civil, Google Spain había aportado entre otras, la Sentencia de la Sala de lo Contencioso Administrativo del Tribunal Supremo de fecha 14 de marzo de 2016, y ello para refrendar la falta de legitimidad pasiva. Pues bien, la Sala del Tribunal Supremo se pronunció sobre este hecho, y entendió que nos encontramos ante dos jurisdicciones distintas, y que tienen

criterios distintos. Concretamente, y por lo sorprendente que resulta dicho pronunciamiento, lo transcribimos a continuación:

> *Debe recordarse la existencia de distintos criterios rectores en las distintas jurisdicciones, por la diversidad de las normativas que con carácter principal se aplican por unas y otras…", destacando que en "las sentencias de la Sala de lo Contencioso Administrativo se está resolviendo con relación a resoluciones dictadas en un procedimiento administrativo seguido ante la AEPD, mientras que esta sentencia se dicta en un proceso civil que tiene por objeto la protección de los derechos fundamentales del demandante, en concreto los derechos al honor, a la intimidad y a la protección frente al tratamiento automatizado de sus datos de carácter personal." Pese a esa afirmación, lo cierto es que tanto en uno como en otro caso de lo que se trata sobre este particular es de determinar si Google Spain SL es "responsable del tratamiento" en el sentido del artículo 2.d) de la Directiva 95/46/CE -art. 3.d) de la LOPD-, lo que en el asunto al que se refiere la STS de 5 de abril resulta presupuesto del derecho a indemnización de los interesados con base en el artículo 19 LOPD (art. 23.1 de la Directiva 95/46/CE).*

Pues bien, la Sala de lo Civil justifica además su decisión en un aspecto práctico, en tanto entiende que para los afectados resultaría mucho más costoso demandar a una empresa extranjera que la filial española. Así, en el apartado onceavo de su Fundamento de Derecho Tercero dispone que:

> *Incluso en el caso de litigar en España, la inmensa mayoría de las personas tendría enormes dificultades prácticas para interponer la demanda de protección de sus derechos fundamentales contra una sociedad domiciliada en Estados Unidos y obtener la tutela judicial efectiva de sus derechos en un plazo razonable, tanto por el elevado coste que supone la traducción al inglés de la demanda y la documentación que le acompaña, como por la dilación que implicaría la inevitable tardanza en el emplazamiento de dicha sociedad, al tener que acudir a los*

> *instrumentos de auxilio judicial internacional, con lo que se prolongaría la situación de vulneración de sus derechos fundamentales. Y, sobre todo, en caso de obtener una sentencia condenatoria, si la demandada no le diera cumplimiento voluntariamente, el ciudadano afectado debería solicitar el reconocimiento y la ejecución de la sentencia en los Estados Unidos de América, con el coste y las dificultades, tanto de orden teórico como práctico, que ello trae consigo.*

Tal y como apunta Marina Sancho López[64], *"teniendo como referencia la sentencia del TJUE en el caso Google, el Tribunal Supremo ha dictado sentencias resolviendo sobre la legitimación procesal del motor de búsqueda Google Spain que, en cuestión de pocos días de diferencia, han dado lugar a pronunciamientos contradictorios por parte de la Sala Civil y la Contencioso-Administrativo del mismo."*

Vemos por lo tanto como mientras que la Sala de lo Contencioso Administrativo ha aplicado un concepto estricto de responsabilidad, la sala de lo asume un concepto amplio, a fin de facilitar la protección eficaz y completa de los derechos fundamentales afectados.

En este punto tenemos que compartir la opinión de Pedro de Miguel Asensio[65], que entiende que es mejor la posición adoptada por la Sala de lo Contencioso Administrativo, por cuanto es más acorde con el principio de seguridad jurídica el análisis de la situación concreta para delimitar la responsabilidad o no de una filial, en lugar de establecer un criterio atendiendo a razones prácticas. Concretamente, Pedro de Miguel Asensio se pronuncia en los siguientes términos:

> *Básicamente, la sentencia fundamenta su criterio en la circunstancia de que tener que demandar en España a una empresa extranjera (y no a su*

[64] Sancho López, Marina (2016). Consideraciones procesales del ejercicio del derecho al olvido: examen de jurisprudencia reciente y nuevo marco legal. *Revista Aranzadi de Derecho y Nuevas Tecnologías num. 41/2016.*

[65] De Miguel Asensio, Pedro (2016, 19 de abril). Las recientes sentencias del Tribunal Supremo sobre Google Spain SL y Google Inc. desde la perspectiva del Derecho internacional privado. Recuperado de: http://pedrodemiguelasensio.blogspot.com.es/2016/04/las-recientes-sentencias-del-tribunal.html

> *filial española) supone en este caso frustrar el objetivo de asegurar una protección eficaz de los derechos fundamentales, obstaculizando la efectividad de las normas que tutelan el derecho fundamental a la protección de datos, que va referido a personas físicas. Aunque esas afirmaciones puedan ser tenidas en cuenta en el plano práctico (por ejemplo, para cuestionar eventualmente la exigencia de traducción a un idioma extranjero de la demanda frente a una empresa que ofrece de manera generalizada sus servicios en español), no parecen determinantes para apreciar la condición de responsable del tratamiento en la legislación sobre datos personales, a cuyos efectos parecería más relevante, como señaló la Sala de lo Contencioso-Administrativo, haber valorado la situación fáctica y la eventual participación de la filial en la determinación de los fines y medios del tratamiento de que se trate.*

En el mismo sentido que se pronuncia dicho autor, entendemos que la decisión relativa a si una determinada entidad puede o no considerarse responsable de un tratamiento de datos no puede depender de la dificultad o de la facilidad que tengan los afectados para llevar a cabo la defensa de sus derechos fundamentales.

La realidad es que con independencia de del orden jurisdiccional en el que nos encontremos, lo lógico es que se apliquen unos criterios uniformes para determinar si una entidad tiene o no la consideración de responsable de tratamiento de datos. A la vista de las Sentencias anteriormente analizadas, en función del orden jurisdiccional ante el que nos encontremos una determinada entidad estará obligada o no al cumplimiento de los deberes que impone la normativa en materia de protección de datos.

Es evidente que el ciudadano, en casos como en que nos ocupa (es decir, en casos en los que un motor de búsqueda tenga un establecimiento en España y no realice directamente una actividad de almacenamiento de datos, sino que dicho cometido sea llevado a cabo por otra entidad del grupo) y siempre que pueda elegir, acudirá a la vía civil, ya que facilita notablemente el ejercicio de sus derechos, puesto que proporciona una mayor protección.

A nuestro juicio lo que debería hacerse es analizar caso por caso, y en función de los hechos concretos, es decir, en función de si existe propiamente o no un tratamiento de datos personales declarar la responsabilidad (o no) de una determinada entidad. A la vista de la jurisprudencia, habrá que esperar a ver como continúan los pronunciamientos en este sentido, si bien, al tratarse de Sentencias dictadas por el Tribunal Supremo es de esperar que cada Sala siga el precedente sentado o por la Sentencia de fecha 5 de abril de 2016 de la Sala de lo Civil del Tribunal Supremo o por la Sentencia de fecha 14 de marzo de 2016 de la Sala de lo Contencioso Administrativo del Tribunal Supremo respectivamente.

VI. EL DERECHO AL OLVIDO EN EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS.

V.1. Antecedentes normativos.

La preocupación por la protección de datos en la Unión Europea es una realidad desde hace tiempo, siendo el Reglamento General de Protección de Datos una nueva muestra de ello.

Cuando se constituyó la Comunidad Europea, los Tratados constitutivos no incluyeron un catálogo de derechos y ello por cuanto entendieron que los mismos ya se encontraban plasmados en el Convenio Europeo de Derechos Humanos.

Evidentemente, cuando se promulgaron los primeros derechos europeos de protección de derechos, no se contemplaba el derecho a la protección de datos, y ello por cuanto como hemos visto el derecho a la protección de datos nace como consecuencia del surgimiento y avance de la era digital.

Si acudimos al artículo 12 de la Declaración Universal de los Derechos en el mismo se establece que:

> *Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*

Vemos como queda recogida en dicho precepto la preocupación por la intimidad, así como por la vida privada de los seres humanos. Evidentemente, en similares términos se ha ido plasmando en otros textos legales europeos como el Pacto Internacional de Derechos Civiles y Políticos o la convención sobre Derechos del Niño de 1989. Ahora bien, en ninguno de estos textos legales se producía un reconocimiento como tal del derecho a la protección de datos.

El primer texto legal europeo que realiza tal reconocimiento fue el convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de fecha 29 de enero de 1981, cuyo artículo primero dispone que el objeto de dicho texto legal es:

> *El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»).*

Igualmente, si acudimos al artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, vemos como también queda plasmado el derecho a la protección de datos:

> *1.Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
> *2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene*

derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedar· sujeto al control de una autoridad independiente.

Vemos como en la carta de Carta de los Derechos Fundamentales de la Unión Europea se da un paso más y no solo se produce el reconocimiento expreso del derecho, sino que se hace referencia a lo que posteriormente se denominará derecho de calidad y del fin del tratamiento, e igualmente se contempla ya en derecho de acceso y de rectificación.

Sin duda alguna la principal norma en esta materia la constituye la Directiva 95/46/CE en materia de protección de datos personales, cuyo principal objetivo fue establecer un equilibrio entre la protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea. Como sabemos dicha Directiva fue incorporada a nuestro Ordenamiento Jurídico mediante la Ley Orgánica de Protección de Datos de Carácter Personal.

VI.2. El artículo 17 del Reglamento.

Pues bien, una vez que hemos analizado los antecedentes relativos al derecho de protección de datos, es necesario hacer referencia a la última norma aprobada por la Comisión Europea que ha sido la aprobación del Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de los datos.

El objetivo que se pretende con la implantación del Reglamento es mejorar la situación actual en materia de protección de datos. Por ello parte de la validez de los principios y de los objetivos de la Directiva 95/46/CE sin embargo pretende homogeneizar todas las legislaciones nacionales para que el derecho en materia de protección de datos no se aplique de forma fragmentada con la inseguridad jurídica que ello conlleva.

Pues bien, es el artículo 17 del citado Reglamento el que contempla el derecho al olvido y en el que se introducen importantes novedades:

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 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.

Vemos como el artículo recoge todas las previsiones que hasta ahora se habían desarrollado tanto por las agencias de protección de datos como por la propia jurisprudencia (nacional y europea).

A tal efecto, dicho precepto recoge una serie de supuestos en los que necesariamente debe procederse a la eliminación de los datos personales e igualmente, recoge aquellos supuestos en los que no se procederá a la supresión de los mismos, debiendo destacarse, a nuestro juicio, lo dispuesto en el apartado a), que contempla la no supresión de los datos personales cuando ello sea necesario para ejercer el derecho a la libertad de expresión e información. Vemos como nuevamente, y tal y como venía haciendo la jurisprudencia, el legislador nacional prioriza la libertad de expresión e información respecto del derecho a la protección de datos.

Es manifiesta la importancia de este artículo y ello por cuanto nos encontramos por primera vez una regulación específica del derecho al olvido y que además debe implementarse en todos los Estados miembros, de tal manera que gracias a ello se va a lograr establecer un marco normativo uniforme en esta materia.

VII. CRITERIOS PARA EJERCER EL DERECHO AL OLVIDO.

El Grupo de Trabajo del artículo 29 ha aprobado una serie de directrices[66] cuyo objetivo es implementar la Sentencia del Tribunal Superior de Justicia de la Unión Europea de fecha 13 de mayo de 2014. A tal efecto se contienen un total de 13 pautas que deben tenerse en cuenta para ponderar la prosperabilidad del derecho al olvido en relación con los motores de búsqueda, y que son las siguientes:

1) En primer lugar (y, como ya vimos en el apartado IV.3.2. de este trabajo) únicamente pueden ejercer el derecho al olvido las personas físicas, y siempre y cuando aparecen los datos de la misma tras introducir en el buscador su nombre y apellidos, su apodo o pseudónimo. Así, la Agencia Española de Protección de Datos[67] desestimó la solicitud de un particular relativa al ejercicio del derecho de cancelación, por cuanto el nombre introducido en el motor de búsqueda se correspondía con una persona jurídica:

[66] Guidelines on the implementation of the Court of Justice of the European Union Judgment on “Google Spain and Google Inc V. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12.

[67] Resolución de la Agencia Española de Protección de Datos R/01788/2017.

En consecuencia, con lo expuesto, procede desestimar la pretensión del reclamante dado que no se adecúa a lo dictaminado por la citada sentencia del Tribunal de Justicia de la Unión Europea, dado que el elemento de búsqueda no es su nombre sino el de su empresa.

2) En segundo lugar, debe analizarse si el sujeto en cuestión es un personaje público. Debemos tener en cuenta que nos encontramos ante un concepto jurídico indeterminado, si bien la jurisprudencia ha intentado perfilarlo. Así, el Tribunal Supremo en su Sentencia de fecha 15 de octubre de 201568 define el concepto de personaje público en los siguientes términos:

A estos efectos, puede servirnos para conceptuar qué es un personaje público la Resolución 1165, de 1998, de la Asamblea Parlamentaria del Consejo de Europa sobre el derecho a la vida privada, cuando afirma que los personajes públicos son las personas que desempeñan un oficio público y/o utilizan recursos públicos, y, en un sentido más amplio, todos aquellos que desempeñan un papel en la vida pública, ya sea en la política, en la economía, en el arte, en la esfera social, en el deporte y en cualquier otro campo.

Pues bien, el factor del carácter de personaje público o no es muy relevante a estos efectos, por cuanto la jurisprudencia entiende que los tratamientos relativos a las personas que no tienen tal consideración, pierden el interés público con el paso del tiempo, por lo que resulta procedente la cancelación de sus datos. Así se pronuncia el Tribunal Supremo en la Sentencia anteriormente[69] citada:

Pero dicho derecho sí ampara que el afectado, cuando no tenga la consideración de personaje público, pueda oponerse al tratamiento de sus datos personales que permita que una simple consulta en un buscador generalista de Internet, utilizando como palabras clave sus datos

[68] [22] Sentencia del Tribunal Supremo Número 545/2015 de fecha 15 octubre de 2015(RJ 2015\4417).

personales tales como el nombre y apellidos, haga permanentemente presentes y de conocimiento general informaciones gravemente dañosas para su honor o su intimidad sobre hechos ocurridos mucho tiempo atrás, de modo que se distorsione gravemente la percepción que los demás ciudadanos tengan de su persona, provocando un efecto estigmatizador e impidiendo su plena inserción en la sociedad, inserción que se vería obstaculizada por el rechazo que determinadas informaciones pueden causar en sus conciudadanos.

3) En tercer lugar, si nos encontramos ante un menor de edad, resulta procedente el ejercicio del derecho al olvido, y ello tomando como base lo dispuesto en el artículo 24 de la Carta de los Derechos Fundamentales de la Unión Europea que dispone que:

Los niños tienen derecho a la protección y a los cuidados necesarios para su bienestar.

4) En cuarto lugar, nos encontramos con que resulta procedente el derecho al olvido en aquellos casos en los que los datos que se contienen son inexactos. A tal efecto tanto en la Ley Orgánica de Protección de Datos como en el Reglamento que la desarrolla se prevé si los datos de carácter personal registrados son inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados. Por lo tanto, el derecho de cancelación puede ser ejercido en aquellos supuestos en los que no se respeta el principio de calidad de datos, por no corresponderse los mismos con la realidad, es decir, por no ser veraces.

5) La quinta directriz hace referencia a la relevancia de los datos, y ello por cuanto en determinadas ocasiones, aunque los datos sean veraces, los mismos pueden resultar excesivos, bien porque ya no son empelados para la finalidad para la que fueron recabados o bien, porque el paso del tiempo hace que pierdan esa relevancia. Dicha cuestión fue abordada ya por la Audiencia Nacional[70] con carácter

[70] Sentencia de la Audiencia Nacional de fecha 27 de febrero de 2012 (RJCA 2012\321).

previo a que se dictada la Sentencia del Tribunal Superior de Justicia de la Unión Europea de fecha 13 de mayo de 2015, y a tal efecto aquella dispuso que:

> *La determinación del alcance de los derechos de supresión, bloqueo (en derecho español cancelación) y oposición del afectado frente a los buscadores de contenidos en internet, incluyendo el derecho al olvido , resulta relevante para la solución del presente litigio pues, tal y como hemos expuesto a lo largo de esta resolución, el interesado al introducir su nombre y apellidos en el buscador de Google aparecen diversos enlaces que le relacionan con el embargo y anuncio de una subasta (en la que se incluían su nombre y apellidos) de un bien inmueble de su propiedad por deudas a la Seguridad Social y aunque este hecho fue exacto y completo cuando se incluyó, el afectado se opone a su tratamiento por entender que el problema que motivó esta subasta está solucionado y resuelto desde hace años, careciendo de relevancia alguna actualmente, y, sin embargo, la información referida a este hecho sigue apareciendo en el buscador y no desea que sea conocida.*

6) En sexto lugar, se hace referencia a los datos especialmente protegidos, tales como las creencias religiosas, políticas, datos relativos a la salud…

7) En séptimo lugar se hace referencia a la actualización de los datos, ya que puede ocurrir que, con el transcurso del tiempo, datos que inicialmente eran veraces, hayan dejado de serlo.

8 y 9) En las directrices octava y novena se hace referencia a los daños causados, así como a la situación de riesgo en la que se puede poner al titular de los datos. A tal efecto, se matiza en la directriz que no es requisito necesario que concurran tales circunstancias, pero que sin embargo su acreditación contribuye notablemente al reconocimiento del derecho al olvido.

10) Igualmente se hace referencia al contexto en el que dichos datos fueron publicados, en particular se contempla el supuesto de que inicialmente existía el

consentimiento del sujeto en el tratamiento de datos, pero posteriormente el mismo se retira, siendo en ese caso procedente el derecho al olvido del sujeto.

11) se hace referencia a la necesidad de analizar el origen de la información, ya que en determinados casos si la información fue publicada por la prensa puede prevalecer el derecho a la información.

12) Se hace referencia a la obligación legal de publicar determinadas resoluciones, cuestión que como hemos visto ha sido analizada en el apartado V.1 del presente trabajo.

13) Y, finalmente se debe atender también a si los datos se corresponden con la comisión de un ilícito penal, ya que en ese caso se deberá atender a la gravedad del mismo. La regla general suele proceder el reconocimiento del derecho al olvido en aquellos casos en los que se cometió un delito menor hace mucho tiempo, en tanto que en aras del interés público no suele concederse el reconocimiento de tal derecho si los hechos revisten de gravedad. En cualquier caso, ya advierte el Grupo del Artículo 29 que es una cuestión que ha de analizarse caso por caso.

VIII. CONCLUSIONES.

Del análisis de todo lo anteriormente expuesto, podemos obtener las siguientes conclusiones:

1) El derecho al olvido no deja de ser una reformulación de los derechos de cancelación y oposición regulados en el artículo 17 de la Ley Orgánica de Protección de Datos

2) El derecho a la información se ve directamente afectado por el derecho al olvido. Sobre todo, cuando nos encontramos en un entorno periodístico, es necesario ponderar los derechos de los afectados con el interés público que puede tener una determinada información.

3) Hasta el momento, y hasta que no entre en vigor el Reglamento de Protección de Datos Europeo, el derecho al olvido es una figura de creación jurisprudencial.

4) Si bien es cierto que el Reglamento de Protección de Datos Europeo contempla en su artículo 17 el derecho al olvido, la realidad es que, a nuestro juicio, es insuficiente. Debemos tener en cuenta que el derecho al olvido es muy complejo y puede contemplar diversos escenarios, por lo tanto, y puesto que el legislador debe adaptar el contenido del citado Reglamento, podría intentar desarrollar más el contenido de dicho artículo, eso sí, siempre respetando el contenido básico del mismo (incluyendo, por ejemplo, una regulación expresa relativa al derecho al olvido en las redes sociales).

5) Conforme a la Sentencia del Tribunal Superior de Justicia de la Unión Europea de fecha 13 de mayo de 2014 cuando un contenido vulnere el derecho a la protección de datos se puede exigir su retirada al buscador, pero no necesariamente al editor.

6) Igualmente, y gracias a la Sentencia a la que hemos hecho referencia en el párrafo anterior, se reconoce el derecho al olvido únicamente, respecto de las personas físicas, pero no ampara a las personas jurídicas, por lo que en determinadas situaciones pueden encontrarse desamparadas. Por lo tanto, quizás debería darse un paso más allá, y regular el ejercicio al derecho al olvido para las personas jurídicas, ya que cuando hacemos referencia al empresario, si bien puede que la información sea relativa a sus datos cuando actúa en el tráfico mercantil, ello pueda tener una incidencia indirecta en su vida personal, afectando a su intimidad y a su honor.

7) Igualmente, debemos tener en cuenta que el derecho al olvido implica una conducta activa por parte de los afectados, que deben dirigirse a una determinada entidad para solicitar la cancelación de sus datos, con los problemas que ello acarrea, que obligan en muchas ocasiones a los afectados a tener que recurrir a los órganos administrativos o judiciales. Por ello, sería interesante que el legislador arbitrara algún tipo de mecanismos para que dicha

cancelación fuera automática o que al menos facilitara su ejercicio por parte de los ciudadanos.

8) Hasta el momento, conforme a la jurisprudencia civil española, los buscadores (aunque no se encarguen de la gestión y del tratamiento de datos, siendo un mero intermediario que ni conoce ni valora) son considerados como verdaderos responsables del tratamiento, en tanto que, para la jurisprudencia contenciosa, únicamente el que efectúa directamente el tratamiento de datos puede merecer tal consideración. Evidentemente ello genera una gran inseguridad jurídica ya que el mismo órgano jurisdiccional (el Tribunal Supremo) mantiene posturas contradictorias en cuanto a la consideración de un mismo buscador como responsable de datos.

   Derivado de lo anterior, y puesto que es lógico que en principio cada una de las Salas mantenga esa postura, lo más adecuado sería que interviniera el legislador y fijara las pautas para delimitar los supuestos en los que un motor de búsqueda puede considerarse responsable de un determinado tratamiento de datos.

9) No solo en la jurisprudencia nos encontramos con situaciones paradójicas, lo mismo ocurre con la normativa que regula la publicación de las Sentencias, y ello por cuanto si las mismas son publicadas en los Boletines Oficiales no es necesario proceder a la disociación de los datos personales, en cambio cuando son publicadas en el Centro de Documentación Judicial sí que lo es. Ello da lugar a situaciones en las que nos encontramos con que la publicación de una determinada resolución judicial tiene dos versiones: una con los datos personales sin disociar y otra con los datos personales disociados, lo que de alguna manera impide el ejercicio del derecho a la protección de datos. Evidentemente, debería lograrse cierta consistencia en la anonimización de datos, por lo que quizás sería adecuado que se introdujera alguna modificación tendente a asegurarla, por ejemplo, que se estableciera una excepción al carácter de fuente accesible al público de los boletines respecto de las resoluciones que son publicadas en el Centro de Documentación Judicial.

10) Sin duda alguna, la entrada en vigor del Reglamento de Protección de Datos Europeo plantea la duda de cómo va a convivir con la normativa existente, esto es la Ley Orgánica de Protección de Datos y el Reglamento que la desarrolla. A priori, parece que la misma podrá seguir siendo aplicable, si bien es obvio será necesaria una labor de revisión con el objetivo de adaptar las previsiones existentes en la normativa española al contenido armonizador del Reglamento Europeo.

    Quizás sería un buen momento para que el legislador intentara solventar las cuestiones que hemos ido apuntando en los párrafos anteriores, tales como los límites del derecho al olvido por las personas físicas cuando actúan como empresarios, la instrumentalización de mecanismos que faciliten el ejercicio del mismo, la delimitación de los supuestos en los que puede considerarse a un motor de búsqueda responsable del tratamiento de datos así como la coordinación de la anonimización de las resoluciones cuando son publicadas paralelamente en Boletines Oficiales y por el Centro de Documentación Judicial, ya que todo ello conllevaría a proporcionar a los afectados una mayor seguridad jurídica a la par que a incrementar sus derechos y garantías constitucionales.

11) A modo de conclusión final, simplemente poner de manifiesto que a día de hoy parece imposible que se pueda implantar en internet un derecho a la protección de datos absoluto, y ello por las dificultades que existen a día de hoy tanto a nivel técnico, como legislativo, como jurisprudencia. Sin embargo, es deseable que se continúe la senda que se está siguiendo tanto por los Tribunales, como por el legislador como por las autoridades en materia de protección de datos que están en constante desarrollo de diversos mecanismos para salvaguardar los derechos de los ciudadanos.

IX. BIBLIOGRAFÍA.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2013). “Memoria anual 2013”. (Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/memorias/memoria2013/Memoria_AEPD_2013.pdf; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2008). “Memoria anual del año 2008”, página 43.
(Disponible en: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2008/AEPD_memoria_2008.pdf; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2009). “Memoria anual del año 2009”, página 56.
(Disponible en: http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2009/AEPD_memoria_2009.pdf; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. “Memoria anual del año 2010”, página 55.
(Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2010/AEPD_Memoria_2010.pdf; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2011). “Memoria anual del año 2011”, página 89.
(Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2011/Memoria_2011.pdf; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2011). “Memoria anual del año 2012”, página 73.
(Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2012/Memoria_2012.pdf; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2013). “Memoria anual del año 2013”, página 85.
(Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2013/Memoria_2013.pdf; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2014). “Memoria anual del año 2014”, página 111.
(Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2014/Memoria_2014.pdf; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2015). “Memoria anual del año 2015”, página 119.
(Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2015/Memoria_2015.pdf; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2015). “Memoria anual del año 2016”, página 73.
(Disponible en: https://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/common/memorias/2016/Memoria_2016.pdf; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. “Derecho de Oposición”. (Disponible en:

http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derechos/oposicion-ides-idphp.php; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. “Derecho de Cancelación”. Disponible en: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derechos/cancelacion-ides-idphp.php; fecha última consulta 17-09-2017).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. “Eliminar fotos y vídeos de internet”.
(Disponible en: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/eliminar_fotos_videos/index-ides-idphp.php; fecha última consulta 17-09-2017).

BLÁZQUEZ AGUADO, Eva María (2017). “La implantación de un protocolo de videovigilancia en el centro de trabajo”. *Revista Aranzadi de Derecho y Nuevas Tecnologías núm. 43/2017.*

DAVARA RODRÍGUEZ, Miguel Ángel. (1998). “La relación entre los artículos 28.1 CE y 18.4 CE desde la óptica de la llamada protección de datos personales". *Editorial Aranzadi, S.A.U., Cizur Menor.*

DAVARA RODRÍGUEZ, MIGUEL ÁNGEL (2013). “El derecho al olvido en Internet”, Madrid, *La Ley.*

GIRALDO, Valentina (2015). “Los motores de Búsqueda y la utilidad que tienen.” (Disponible en: de https://marketingdecontenidos.com/motores-de-busqueda/; fecha última consulta 17-09-2017).

GUDÍN RODRÍGUEZ-MAGARIÑOS, Faustino. (2015). “Réquiem por el derecho a la intimidad en los smartphone: análisis de la última Jurisprudencia del TC contrastada con la del TDEH”. Barcelona (España). *Revista Aranzadi Doctrinal núm. 9/2014.*

GUICHOT, Emilio (2012). “La publicidad de datos personales en Internet por parte de las Administraciones Públicas y el Derecho al olvido”, Pamplona, *Aranzadi*.

MARTÍNEZ OTERO, Juan María (2015). “El derecho al olvido en internet”. Madrid, *Revista de Derecho Político de la UNED.*

DE MIGUEL ASENSIO, Pedro (2016) “Las recientes sentencias del Tribunal Supremo sobre Google Spain SL y Google Inc. desde la perspectiva del Derecho internacional privado”. (Disponible en: http://pedrodemiguelasensio.blogspot.com.es/2016/04/las-recientes-sentencias-del-tribunal.html; fecha última consulta 17-09-2017).

MUÑOZ, Joaquín (2014). “El llamado "derecho al olvido" y la responsabilidad de los buscadores”, Madrid, *La Ley.*

MURILLO DE LA CUEVA, Pablo Lucas. *(2010). “*Comentario a la ley Orgánica de Protección de Datos de Carácter Personal”. *Editorial Aranzadi, S.A.U.*

RALLO, Artemi (2014). “El derecho al olvido en Internet. Google versus España”. Madrid, *Centro de Estudios Políticos y Constitucional.*

SANCHO LÓPEZ, Marina (2016). “Consideraciones procesales del ejercicio del derecho al olvido: examen de jurisprudencia reciente y nuevo marco legal”. *Revista Aranzadi de Derecho y Nuevas Tecnologías núm. 41/2016.*

SIMÓN CASTELLANO, Pere (2012). *El régimen constitucional del derecho al olvido digital,* Madrid, Tirant lo Blanch.

SIMÓN CASTELLANO, Pere (2015). *El reconocimiento del Derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014,* Barcelona, Bosch.

VILLAVERDE, Beatriz (2015). “Historia del derecho al olvido”, Madrid. *Creativa legal.* (Disponible en: http://www.creativalegal.com/2015/02/10/la-historia-del-derecho-al-olvido/; fecha de la última consulta 17-09-2017).

X. FUENTES JURÍDICAS.

X.1 Referencias Normativas.

Constitución Española, 1978:

Art. 10
Art. 18.4
Art. 120

Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente:

Art. 10

Instrumento de Ratificación de España del Pacto Internacional de Derechos Civiles y Políticos, hecho en Nueva York el 19 de diciembre de 1966:

Art. 19.2

Carta de los Derechos Fundamentales de la Unión Europea, hecha en Estrasburgo de 12 de diciembre de 2007:

Art. 8
Art. 11

Reglamento 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:

Art. 13
Art. 14
Art. 17
Art. 18.1
Art. 20
Art. 25
Art. 37
Art. 39
Art. 78

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial:

Art. 235
Art. 266.1
Art. 560.1.10º

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

Art. 2.1
Art. 3
Art. 4.1
Art. 4.2
Art. 4.3
Art. 6.1
Art. 6.2
Art. 6.4
Art. 15

Art. 16.2
Art. 17
Art. 30.4

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

Art. 17
Art. 8.1

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

Art. 5.f)
Art. 7
Art. 24.3

Acuerdo de 15 de septiembre de 2005, del Pleno del Consejo General del Poder Judicial, por el que se aprueba el Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales:

Art. 7.

X.2 Referencias Jurisprudenciales.

1985

STC 53/1985 de fecha 11 de abril de 1985 (RTC 1985\53)

1990

STC 171/1990 de fecha 12 noviembre (RTC 1990\171)

1993

STC 254/1993 de fecha 20 de julio de 1993. (RTC 1993\254).

1995

STS de fecha 3 de marzo de 1995 (RJ 1995\2292)

2000

STC 292/2000 de fecha 20 de noviembre de 2000. (RTC 2000\292).

2008

STSJ Madrid 186/2008 de fecha 31 de enero de 2008 (JUR 2009\164175).

SJPI 8 de Barcelona de fecha 14 de noviembre de 2011 (JUR 2015\296352)

2010

STS de fecha 1 de febrero de 2010 (RJ 2010\1370)

SAP de Madrid 95 /2010 de fecha 19 de febrero de 2010 (JUR 2010\133011)

2011

STS de fecha 28 de octubre de 2011 (RJ 2012\1691)

2012

SAN de fecha 27 de febrero de 2012 (RJCA 2012\321)

SJPI 4 de Barcelona de fecha 3 de septiembre de 2012 (JUR 2013\366988)

SJPI 21 de Barcelona de fecha de 4 octubre 2012 (JUR 2014\4375).

2013

STC 17/2013 de fecha 13 de enero de 2013 (RTC 2013\17).

SAP de Barcelona 86/2013 de fecha 8 de febrero de 2013 (JUR 2013\111097)

STS 144/2013 de fecha 4 de marzo de 2013 (RJ 2013\338).

SAP de Barcelona 486/2013 de fecha 11 octubre de 2013 (AC 2013\1921)

2014

STJUE de 13 de mayo de 2014 (TJCE 2014\85)

SAP de Barcelona 364/2014 de fecha 17 de julio de 2014 (AC 2014\1661)

Auto TS de fecha 9 septiembre 2014 (JUR 2014\246001)

SAN de fecha 29 de diciembre de 2014 (RJCA 2015\183)

2015

Auto TS de fecha 9 de septiembre de 2015 (JUR 2015\216224)

STS 545/2015 de fecha 15 octubre de 2015 (RJ 2015\4417)

2016

STC 39/2016 de fecha 3 marzo de 2016. (RTC 2016\39).

STS 574/2016 de fecha 14 marzo de 2016 (RJ 2016\1071).

STS 210/2016 de fecha 5 de abril de 2016 (RJ 2016\1006)

SAN 251/2016 de fecha 4 de mayo de 2016 (JUR 2016\134261).

X.3 Referencias Administrativas.

2008

Resolución AEPD R/00320/2008 de fecha 4 de abril de 2018.

Resolución AEPD R/01239/2007 de fecha 24 de abril de 2008.

2010

Resolución AEPD R/02694/2009 de fecha 19 de enero de 2010.

Resolución AEPD R/01553/2010 de fecha 8 de julio de 2010.

2015

Resolución AEPD R/02681/2015

2016

Resolución AEPD R/02767/2016 de fecha 4 de noviembre de 2016 (JUR 2017\419).

2017

Resolución AEPD E/03240/2016 de fecha 28 de marzo de 2017.

Resolución AEPD R/01788/2017.