InDret
REVISTA PARA EL
ANÁLISIS DEL DERECHO

WWW. INDRET.COM

El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible?

A propósito de la STJUE de 13 de mayo de 2014 (Google Spain, S.L. y Google Inc. / Agencia Española de Protección de Datos [AEPD] y Mario Costeja González, C-131/12, no publicada todavía en el repertorio oficial)

Ricardo Pazos Castro

Facultad de Derecho
Universidad de Santiago de Compostela

BARCELONA, ENERO 2015

Abstract[*]

La aparición de Internet ha hecho aumentar exponencialmente la información al alcance de las personas, y los motores de búsqueda son una de las herramientas que pone en contacto a los usuarios de Internet con esa información. La relación de los motores de búsqueda con los datos personales se manifiesta en dos sentidos. Por un lado, sobre los datos personales de los usuarios que realizan la búsqueda, ya que esta información permite al buscador ser más preciso y las posibilidades de explotación económica de los datos personales por parte de los titulares del motor son enormes. Por otro, porque los motores de búsqueda remiten a páginas web que pueden contener datos personales de terceros, de forma que estos datos pueden ser obtenidos fácilmente por los internautas. En este contexto, se hace preciso establecer normas de protección de datos que pueden condicionar la actividad de los proveedores de los motores de búsqueda. La controversia suscitada en la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 gira en torno al motor de búsqueda como mecanismo mediante el cual el usuario del buscador puede acceder a datos personales de terceros. En esta sentencia se plantean diversas cuestiones relativas al ámbito de aplicación territorial y material de la Directiva 95/46/CE, así como el posible reconocimiento en la misma de un "derecho al olvido".

The appearance of the Internet has exponentially increased the amount of information available to people, and search engines are one of the tools which link the Internet users with that information. The relationship between search engines and personal data shows up in two ways. On the one hand, about personal data of the users searching, since this information makes the Internet browser more accurate and the possibilities of economic exploitation of the personal data by the owner of the search engine are huge. On the other hand, because search engines lead to websites that may contain personal data of third parties, so those data can be obtained easily by Internet users. In this context, it is necessary to establish protection rules that may condition the activity of the search engine providers. The controversy brought up in the judgement of the European Court of Justice of 13 May 2014 revolves around the search engine as a mechanism by which the user of the browser gets access to personal data of third parties. In this judgement, several questions concerning the territorial and material scope of application of Directive 95/46/EC are set out, as well as the possible recognition in it of a "right to be forgotten".

Title: The functioning of Search Engines on the Internet and Policy of Personal Data Protection, an Impossible Relationship?

Keywords: data protection, search engines, processing of personal data, controller, right to be forgotten
Palabras clave: protección de datos, motores de búsqueda, tratamiento de datos personales, responsable del tratamiento, derecho al olvido

[*] Agradezco a los dos revisores anónimos las observaciones realizadas, las cuales han contribuido sin duda a mejorar el presente trabajo. En todo caso, la responsabilidad sobre el resultado final del mismo es exclusivamente mía.

Sumario

1. Introducción

Desde el surgimiento de la denominada "sociedad de la información", concepto cuya aparición algún autor sitúa a principios de los años 70 junto a otras expresiones similares como "revolución de la información" o "era de la información"[1], la sociedad ha avanzado mucho en cuanto a la tecnología disponible y el número de personas que pueden acceder a ella, dando la razón a quienes sostenían que las nuevas tecnologías tendrían un impacto masivo, de modo que acabarían afectando a la estructura y contenido de nuestra cultura[2]. Es evidente que la cantidad de información a la que un individuo puede acceder hoy en día no tiene precedentes en la historia de la humanidad, y ello no sólo porque Internet permite una enorme difusión de información con gran rapidez, sino porque la mayoría de la información comunicada por este medio se almacena, y lo que se transmite en un momento determinado termina quedando a disposición de las personas que naveguen posteriormente por la red.

> WEBSTER señala que la expresión "sociedad de la información" implica mucho más que un avance en el campo puramente tecnológico, debiendo identificarse también el concepto en otras cuatro dimensiones: económica, ocupacional, espacial y cultural. A efectos del presente trabajo, no obstante, el criterio más relevante es precisamente el tecnológico, puesto que como el mismo WEBSTER explica, dicho criterio tiene como idea clave que el avance en cuanto al "procesamiento, almacenado y transmisión de la información" ha conducido a la aplicación de las tecnologías de la información en todos los aspectos de la sociedad[3].

La sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 sirve de base al presente estudio. La controversia que en dicha sentencia se plantea gira en torno a la protección de los individuos contra la disponibilidad de información relativa a cuestiones de su esfera personal cuando ya ha pasado un tiempo desde su aparición. Aunque dicha información pudiera carecer entonces de relevancia, se encuentra, no obstante, a disposición de cualquier persona a través de los motores de búsqueda.

2. La protección de datos personales.

Este trabajo trata diversas cuestiones relacionadas con los "datos personales", por lo que es preciso determinar desde este momento qué debe entenderse por esta expresión. Para ello se recurrirá a las definiciones que proporcionan la Directiva 95/46/CE del Parlamento Europeo y

---

[1] CRAWFORD (1983, p. 380). En este sentido, cabe destacar la referencia que hace la autora (p. 381) a la expresión "industria del conocimiento" aparecida en la obra de MACHLUP *The Production and Distribution of Knowledge in the United States*, Princeton University Press, Nueva Jersey, 1962. Al mismo tiempo expone que en 1970 ya había constancia de la expresión "era de la información". Para WEBSTER (1995, pp. 217 y 219), hablar de "sociedad de la información" no es del todo correcto porque no hay una ruptura o cambio drástico con la sociedad anterior, sino un progreso que se entiende mejor desde una perspectiva continuista de los avances descrita con el término *informatisation*.

[2] CRAWFORD (1983, p. 384).

[3] WEBSTER (1995, pp. 6 y 7).

del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, Directiva sobre protección de datos)[4], y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE nº 298, de 14.12.1999) (en adelante, LOPD), que fue la que transpuso al ordenamiento jurídico español dicha Directiva, fundamentalmente. La sujeción a las definiciones proporcionadas en los textos indicados parece conveniente, porque en la sentencia *Google Spain y Google* el Tribunal de Justicia aclara ciertas dudas existentes en cuanto a la interpretación de la Directiva sobre datos personales, y la sentencia del TJUE influye, como no puede ser de otro modo, sobre las legislaciones nacionales relativas a la protección de datos.

Pues bien, el artículo 2.a) de la Directiva sobre protección de datos define los "datos personales" como "toda información sobre una persona física identificada o identificable", precisando que "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social". El hecho de que los datos permitan identificar a la persona es clave, porque si la recogida, procesamiento o uso de datos no lo permiten, lo cierto es que el derecho del individuo a la intimidad no se ve amenazado, al menos en el mismo grado[5]. Por su parte, el artículo 3.a) de la LOPD se decanta por utilizar la expresión "datos de carácter personal", los cuales son definidos como "cualquier información concerniente a personas físicas identificadas o identificables"[6]. Cuándo un determinado elemento es suficiente para identificar a la persona dependerá de la situación concreta. De hecho, la Directiva de protección de datos habla de una identificación directa o indirecta, es decir, da cobertura a aquellas situaciones en las que los elementos disponibles no permiten conocer la identidad de la persona de cuyos datos se trata, pero que en cambio sí lo harían si se combinasen con otros datos[7]. En mi opinión, resulta adecuado el criterio según el cual son personales los datos que permitan conocer la identidad de una persona utilizando medios razonables[8].

Resulta obligado mencionar el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el

[4] DO L 281, de 23 de noviembre de 1995, p. 31.

[5] DWORK / MULLIGAN (2013, p. 36); LLOYD (2014, p. 50); TENE (2008, p. 1445).

[6] Tanto en la versión en español de la Directiva sobre protección de datos como en la LOPD se hace alusión a la noción de "persona física". Sin embargo, mientras que en la versión en inglés de la Directiva se utiliza el término *natural person*, el artículo 1(1) de la ley británica de protección de datos de 1998 (*Data Protection Act 1998*) establece que los datos personales son datos relativos a una "persona viva" (*living individual*). Así lo pone de manifiesto LLOYD (2014, p. 43), afirmando que es posible defender que el estado de *natural person* no se pierde con la muerte, por lo que la legislación sobre protección de datos podría ser aplicable también a la información relativa a una persona fallecida cuando dicha información afecte de alguna manera a personas vivas. En Derecho español no hay duda de que la LOPD no es aplicable a los datos de personas fallecidas, lo que se desprende del artículo 2.4 del Reglamento que desarrolla la LOPD, si bien, dice este precepto, "las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos".

[7] Sobre esta cuestión puede consultarse el Dictamen 4/2007del Grupo del artículo 29 (pp. 13-23). En relación con la unión de datos que aislados no permiten la identificación de una persona, SOLOVE (2006, pp. 505-515).

[8] DE MIGUEL ASENSIO (2011, pp. 294 y 295); PIÑAR MAÑAS (2010, p. 195).

> Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE nº 17, de 19.1.2008) (en adelante, RPDP). El artículo 5.1.f) del RPDP define datos de carácter personal como "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables". Por su parte, la letra o) del mismo artículo 5.1 del RPDP establece que es una "persona identificable" aquélla "cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social", indicando al mismo tiempo que una persona no es "identificable" cuando la identificación requiere "plazos o actividades desproporcionados".

Obsérvese que a pesar de la relación que existe entre la protección de datos personales y el derecho a la intimidad de las personas, la LOPD no hace distinción en cuanto a datos privados o íntimos y datos públicos, por lo que todos ellos están incluidos en la noción legal de datos personales[9]. Al mismo tiempo hay que decir que la regulación de la LOPD sólo da cobertura, utilizando la terminología empleada por el artículo 2.1 de la propia LOPD y el mismo artículo pero del RPDP, a datos de carácter personal "registrados en soporte físico, que los haga susceptibles de tratamiento". Los datos personales que no estén cubiertos por la LOPD y el RPDP serán susceptibles de protección, pero de acuerdo con otros textos normativos[10].

Una vez que ha quedado fijado a grandes rasgos el concepto de datos personales, procede exponer las razones que justifican la protección de las personas en lo referente a tales datos y hacer ciertas consideraciones al respecto. Las conclusiones del Abogado General en la sentencia *Google Spain y Google* comienzan recordando el famoso artículo publicado en el año 1890 por WARREN y BRANDEIS en el que éstos comentaban que la aparición de nuevos inventos como la fotografía y la prensa permitía invadir la vida privada de los individuos, por lo que, previendo nuevos avances, aludían a la necesidad subsiguiente de proteger a la persona[11]. Dichos autores manifestaron que el derecho a la intimidad formaba parte de un derecho más general a no ser molestado (*to be let alone*), así como que el Derecho debía proteger a las personas en relación con sus asuntos privados sobre los que el resto de la comunidad no tuviese un interés legítimo[12].

> La relación entre la protección de datos personales y el derecho de las personas a mantener vedados a terceros sus asuntos privados parece evidente. Así, el primer principio que legitima el tratamiento de datos personales, o si se prefiere la regla general para que dicho tratamiento sea legítimo, es la necesidad de que exista consentimiento del interesado. No obstante, también hay supuestos en los cuales la ley dispone que el tratamiento de datos podrá realizarse sin obtener tal consentimiento[13]. El principio de consentimiento ha quedado recogido en el artículo 7.a) de la Directiva sobre protección de datos:
>
> "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:
>
> a) El interesado ha dado su consentimiento de forma inequívoca".

---

[9] PIÑAR MAÑAS (2010, p. 185).

[10] PIÑAR MAÑAS (2010, pp. 186 y 187).

[11] WARREN / BRANDEIS (1890).

[12] WARREN / BRANDEIS (1890, pp. 205 y 214).

[13] APARICIO SALOM (2009, pp. 34-39); GUERRERO PICÓ (2006, pp. 257-278); DE MIGUEL ASENSIO (2011, pp. 299-303); TRONCOSO REIGADA (2010, pp. 504-523).

> Una previsión análoga se contiene en el artículo 6.1 de la LOPD:
>
> "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa".

La protección de los datos personales y de la privacidad de las personas es, por tanto, un fin cada vez más difícil de alcanzar, ya que como constata el Abogado General en sus conclusiones en la sentencia *Google Spain y Google*, en la época actual cualquier contenido es susceptible de ser puesto a disposición de terceros a gran escala, de forma instantánea y permanente. Por ello, dice el Abogado General, ha de "establecerse un equilibrio entre diversos derechos fundamentales, como la libertad de expresión, el derecho a la información y la libertad de empresa, por un lado, y la protección de los datos personales y la privacidad de los particulares, por otro"[14].

> HERNÁNDEZ LÓPEZ recoge diferentes posturas sobre el derecho a la protección de datos. Por un lado, la protección de datos puede ser entendida como un derecho autónomo que deriva del artículo 18.4 de la Constitución española, en el que se establece 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". Así lo entiende el propio autor, y las sentencias del Tribunal Constitucional 290/2000 y 292/2000, ambas de 30 de noviembre, se pronuncian en este mismo sentido. De hecho, en el punto 11 de la primera de estas resoluciones, el Tribunal Constitucional afirma que "la LORTAD [Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal], en efecto, ha sido dictada en cumplimiento del mandato contenido en el art. 18.4 que permita garantizar el respeto o el pleno ejercicio de tales derechos".
>
> Por otro lado, el derecho a la protección de datos puede ser concebido como una manifestación del derecho a la dignidad de la persona y al libre desarrollo de la personalidad, contenidos en el artículo 10.1 de la Constitución. El voto particular del magistrado Manuel Jiménez de Parga en la STC 290/2000 ya citada, al que se adhirió Rafael de Mendizábal Allende, menciona el derecho fundamental "a la libertad informática" y entiende que éste procede del derecho a la dignidad, citando la STC 254/1993, de 20 julio.
>
> Una tercera posibilidad que presenta HERNÁNDEZ LÓPEZ es incluir la protección de datos en el derecho al honor, a la intimidad personal y familiar y a la propia imagen, reconocido en el artículo 18.1 de la Constitución. El propio autor reconoce que la protección de datos conecta con estos derechos, pero le otorga a aquélla un carácter autónomo señalando que este derecho puede ser infringido sin que por ello se vea vulnerado el derecho a la intimidad[15]. Si bien es cierto que entre el derecho a la intimidad y la protección de datos existen diferencias, no lo es menos que son nociones que se solapan[16].

Gran parte de la información personal que aparece en Internet forma parte de la esfera pública de los individuos, pero antes de la aparición de los motores de búsqueda esta información disfrutaba de lo que se ha llamado "oscuridad práctica" (*practical obscurity*), esto es, la

---

[14] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, punto 2. Sobre la relación entre protección de datos y libertad de información, véase REED / ANGEL (2007, pp. 463 y 464).

[15] HERNÁNDEZ LÓPEZ (2013, pp. 29-33).

[16] Sobre la relación entre la protección de datos y el derecho a la intimidad (*privacy*) pueden consultarse REED / ANGEL (2007, pp. 461-463) y TRONCOSO REIGADA (2010, pp. 64-78). Haciendo una exposición de las opiniones que entienden el derecho a la intimidad en una vertiente más comunitaria que el tradicional enfoque como un derecho del individuo, véanse SOLOVE (2006, pp. 483-488) y SOLOVE (2007, pp. 760-764).

información permanecía oculta por el elevado coste de obtenerla[17]. Cabe decir que en cierta forma las limitaciones fácticas impedían el desarrollo de los problemas que se plantean respecto a la privacidad de los usuarios de la red.

> Tomando como referencia a SOLOVE, TENE sintetiza estos problemas en agregación (los motores de búsqueda permiten ensamblar informaciones reducidas y elaborar un perfil más o menos completo de una persona), distorsión o inexactitud de la información (que puede llegar a suponer un menoscabo del prestigio o consideración social de una persona), exclusión o incapacidad de una persona para conocer la información recopilada sobre ella, y uso de la información disponible para fines distintos a los que motivaron su recopilación. A todo ello se une el *chilling effect* o desincentivo de ciertas búsquedas en una especie de autocensura, cuando el individuo es consciente de que el sistema registra las búsquedas efectuadas desde cada dirección IP[18].

La oscuridad a la que se ha aludido se ha visto muy reducida, y quizás el caso más claro de ello sea la publicidad comportamental o *behavioral advertising*, esto es, los anuncios que los usuarios reciben de acuerdo con sus intereses. Estos intereses se determinan en función de las búsquedas que los propios usuarios han realizado previamente, de modo que se obtiene un perfil del usuario del equipo informático bastante preciso[19]. Las implicaciones que tiene la *behavioral advertising* en el ámbito económico son enormes, puesto que indudablemente conducen a una mayor eficiencia en el empleo de los recursos, y por eso se ha dicho que los datos personales son verdaderos activos (*assets*) para las entidades que prestan servicios en Internet[20]. Como se señalará posteriormente, uno de los factores que hacen mejor a un motor de búsqueda es la capacidad de mostrar resultados que se adecúen a los intereses de quien realiza la búsqueda. Ello no resulta sencillo, porque los usuarios no utilizan más que unos pocos términos que introducen en el motor de búsqueda, y sin embargo los intereses de dichos usuarios pueden ser muy diferentes entre sí. Por eso, si un motor de búsqueda conoce las preferencias de los usuarios y tiene acceso a datos personales puede prestarles un mejor servicio[21].

> Los datos que se ofrecen en el estudio de mercado "Online Targeting of Advertising and Prices" llevado a cabo por la *Office of Fair Trading*, de mayo de 2010, permiten sintetizar los beneficios, en primer lugar, en un ahorro de tiempo para los usuarios, al no requerir tanto esfuerzo en la búsqueda para encontrar lo que interesa y reducir el número de anuncios irrelevantes que el usuario recibe. En segundo lugar, permite a las empresas que se publicitan por Internet ahorrar costes, ya que la información sobre los

[17] TENE (2008, p. 1440). Una idea similar se extrae de BATTELLE (2006, p. 245); HARTZOG / SELINGER (2013, pp. 81, 83 y 84); HERNÁNDEZ LÓPEZ (2013, p. 27); REED / ANGEL (2007, pp. 398 y 399); SIMÓN CASTELLANO (2011, pp. 393 y 394) o SOLOVE (2006, pp. 536-538).

[18] TENE (2008, pp. 1457-1464). En relación con este tema también puede consultarse SOLOVE (2006) y SOLOVE (2007, pp. 765-768).

[19] SLOOT / BORGESIUS (2012, pp. 76-79). También DE MIGUEL ASENSIO (2011, p. 278) y TRONCOSO REIGADA (2010, pp. 270 y 271).

[20] GERADIN / KUSCHEWSKY (2013, p. 4). Los autores remiten en nota a las palabras de Joaquín Almunia el 26 de noviembre de 2012 (SPEECH/12/860), el cual se encuentra disponible en inglés y francés en el enlace http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm (última consulta: 5 de junio de 2014). También BATTELLE (2006, p. 24), que dedica el capítulo 7 de la obra (pp. 197-241) a la relación entre los servicios de búsqueda en internet en general y las posibilidades económicas que ello ofrece. En el mismo sentido, GUERRERO PICÓ (2006, p. 344); DE MIGUEL ASENSIO (2011, p. 280); REED / ANGEL (2007, p. 459); TENE (2008, p. 1452).

[21] BENGHOZI (2008, pp. 95 y 96); GERADIN / KUSCHEWSKY (2013, pp. 2 y 3).

> bienes y servicios llega mucho más fácilmente a las personas a las que se dirige la publicidad. Esto hace a las empresas más competitivas, pudiéndose reflejar esa mayor competitividad en beneficios para el usuario. En tercer lugar, y quizás lo más importante, dado que los servicios de Internet se financian en gran parte gracias a la publicidad, la mayor eficiencia del proceso permite poner a disposición de los usuarios una mayor cantidad de información de manera gratuita[22].

En este contexto, hay que hacer referencia de nuevo a la Directiva sobre protección de datos, cuyos dos objetivos fundamentales se recogen de forma expresa en su artículo 1. En primer lugar, intentar crear el marco para que los Estados miembros den una respuesta similar ante el avance de las tecnologías de la información, las cuales hacen más sencillo tanto el tratamiento como el intercambio de datos personales contribuyendo al progreso económico y social, asegurando al mismo tiempo un alto nivel de protección para los individuos. Esta respuesta conjunta se hace necesaria, ya que el tratamiento de tales datos ha de respetar derechos fundamentales de las personas como el derecho a la vida privada y a la intimidad, y la consecución de este objetivo estaría más alejada si el problema fuese afrontado de manera descoordinada, además de que se generarían desequilibrios entre los ciudadanos de diferentes Estados miembros. El segundo objetivo es garantizar la libre circulación de los datos personales dentro de la Unión Europea. Por otra parte, hay que añadir que la Directiva sobre protección de datos es una directiva de máximos, puesto que pretende una armonización completa de las legislaciones de los estados miembros. Si bien los Estados disponen aun así de cierto margen en situaciones específicas, la propia Directiva acota dicho margen con el fin de garantizar el alto nivel de protección pretendido y, al mismo tiempo, un equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad. Así lo declaró el Tribunal de Justicia de la Unión Europea en su sentencia *Lindqvist*[23].

Como ya se ha indicado, la Directiva sobre protección de datos fue transpuesta al ordenamiento español mediante la LOPD. El artículo 1 de esta ley proclama que la finalidad de la misma es "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar". A su vez, la LOPD fue desarrollada mediante el ya mencionado RPDP.

Al hilo de la Directiva sobre protección de datos, también hay que mencionar el llamado "Grupo del artículo 29". El nombre del mismo viene dado, como es fácilmente deducible, por el artículo 29 de la citada Directiva, el cual creó dicho grupo. A éste se le atribuyó un carácter consultivo e independiente, y sus funciones se encuentran recogidas fundamentalmente en el artículo 30.1 de la propia Directiva, siendo las siguientes:

> "a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;

---

[22] "Online Targeting of Advertising and Prices" (pp. 5, 31 y 33). Este estudio se encuentra disponible en el enlace http://webarchive.nationalarchives.gov.uk/20140402142426/http://www.oft.gov.uk/shared_oft/business_leaflets/659703/OFT1231.pdf (última consulta: 5 de junio de 2014).

[23] Sentencia del TJUE de 6 de noviembre de 2003 (Procedimiento penal entablado contra Bodil Lindqvist, C-101/01, Rec. p. I-12971), apartados 96 y 97.

> b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;
>
> c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adaptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;
>
> d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria".
>
> Las funciones anteriormente indicadas también se ejercerán en el ámbito de las comunicaciones electrónicas, pues así se establece en el artículo 15.3 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[24].

La labor del Grupo del artículo 29 es especialmente destacable por la elaboración de diversos dictámenes en los cuales se tratan diferentes aspectos de la Directiva sobre protección de datos, aclarando conceptos de gran importancia y arrojando algo de luz sobre un tema tan complejo como es el tratamiento de datos personales, sobre todo en Internet[25]. En este sentido, pueden mencionarse los Dictámenes 4/2007, de 20 de junio de 2007, sobre el concepto de datos personales (WP 136); 1/2008, 4 de abril de 2008, sobre cuestiones relativas a los motores de búsqueda (WP 148); 1/2010, de 16 de febrero de 2010, sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento" (WP 169); u 8/2010, de 16 de diciembre de 2010, sobre el Derecho aplicable (WP 179).

Otra directiva que hay que citar en materia de datos personales es la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE[26].

> Por otra parte, la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas había derogado, en virtud de su artículo 19, la Directiva 97/66/EC del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[27].
>
> También hay que mencionar el Reglamento 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Su ámbito de aplicación viene especificado en su artículo 3:

[24] DO L 201, de 31 de julio de 2002, p. 37.

[25] De hecho, en las conclusiones del Abogado General en la sentencia *Google Spain y Google* se encuentran algunas referencias a dictámenes del Grupo del artículo 29.

[26] DO L 105, de 13 de abril de 2006, p. 54.

[27] DO L 24, de 30 de enero de 1998, p. 1.

> "1. Las disposiciones del presente Reglamento se aplicarán al tratamiento de datos personales por parte de todas las instituciones y organismos comunitarios, en la medida en que dicho tratamiento se lleve a cabo para el ejercicio de actividades que pertenecen al ámbito de aplicación del Derecho comunitario.
>
> 2. Las disposiciones del presente Reglamento se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

Teniendo en cuenta que en el momento en que fue dictada la Directiva sobre protección de datos Internet no estaba tan desarrollado como lo está en la actualidad, la sentencia *Google Spain y Google* examina el alcance de la protección conferida por la citada Directiva y sus consecuencias sobre la actividad de los proveedores de servicios de motores de búsqueda en Internet. No obstante, hay que traer la atención sobre una cuestión importante. Normalmente, cuando se habla de protección de datos personales, se está pensando en una relación bilateral en la cual intervienen un usuario de Internet y un prestador de servicios de la sociedad de la información, de manera que los datos personales se refieren a dicho usuario, y es a éste a quien se intenta proteger[28]. Sin embargo, la protección de datos personales engloba también una situación tripartita en la cual la información que contiene datos personales no se refiere al usuario de Internet, sino a un tercero con el que no tiene relación tal usuario, y quizás tampoco el prestador de servicios[29]. Los motores de búsqueda y otras herramientas como las redes sociales no solamente tratan los datos de las personas que utilizan esos medios, sino que son un mecanismo a través del cual los usuarios pueden conocer información sobre terceros, incluyendo datos personales de éstos[30].

> El problema fundamental que generan los motores de búsqueda tiene lugar respecto de informaciones legítimamente publicadas. En los casos en los que la aparición de los datos personales en la red está justificada y el interesado no tiene derecho a impedirla, como sucede en el caso de información recogida de fuentes de acceso público, los motores de búsqueda ayudan a que esa información esté al alcance de cualquiera, lo que podría acarrear el peligro de que la reputación de la persona sobre la que versa la información se viese afectada de manera excesiva o desproporcionada[31].

Tanto la estructura bilateral que puede decirse básica como el escenario tripartito son casos en los que aparece la necesidad de otorgar a las personas protección en cuanto al tratamiento de sus datos personales. Por tanto, las previsiones normativas relativas a dicha protección son aplicables a ambas situaciones. En la sentencia *Google Spain y Google* que se toma como referencia en el

---

[28] APARICIO SALOM (2009, pp. 41-44).

[29] TENE (2008, pp. 1440-1450).

[30] APARICIO SALOM (2009, p. 95); DE MIGUEL ASENSIO (2011, pp. 280 y 281); TRONCOSO REIGADA (2010, pp. 1693 y 1699).

[31] SIMÓN CASTELLANO (2011, p. 403). Véase también el informe elaborado por el Grupo del artículo 29 sobre la sentencia *Google Spain y Google*, con fecha de 26 de noviembre de 2014, titulado *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12* (WP 225) (en adelante, Informe *Guidelines*), punto 7. El informe se encuentra disponible a través del enlace http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf (última consulta: 23 de diciembre de 2014).

presente estudio, los datos personales sobre los que se gira la protección solicitada son los del mismo usuario que utiliza el motor de búsqueda en cuestión, pero esto es así porque el usuario busca información relativa a sí mismo. Más concretamente, el motor de búsqueda en cuestión, utilizado en 2009 introduciendo el nombre del demandante en el litigio principal, arrojaba como resultados de la búsqueda informaciones relativas a dicha persona publicadas en 1998, informaciones que en opinión del demandante ya no tenían ningún valor once años después.

En definitiva, es la estructura que antes fue descrita como tripartita la que ha de tenerse en mente a la hora de examinar la sentencia *Google Spain y Google*, pues como el propio Abogado general manifiesta en sus conclusiones en la sentencia, el problema clave reside en la determinación del "papel de los proveedores de servicios de motores de búsqueda en Internet a la luz de la normativa de la Unión sobre protección de datos existente"[32].

3. Los hechos base del asunto Google Spain y Google

Pese a las limitaciones de la Directiva sobre protección de datos, propias del momento en que fue adoptada, las legislaciones nacionales sí pueden ir respondiendo a las nuevas situaciones, desarrollando la normativa en materia de protección de datos teniendo en cuenta las características de la tecnología y sistemas informáticos actuales. Sin embargo, el hecho de que las legislaciones nacionales evolucionen y afronten nuevos problemas no les libera del deber de mantenerse en el marco fijado por la Directiva, pues sólo así se garantiza que todos los países europeos responden de forma similar a los últimos desafíos. A continuación se presentarán los hechos del litigio principal que dio lugar a la sentencia del TJUE *Google Spain y Google* que sirve de base al presente trabajo. Tales hechos constituyen un claro ejemplo de cómo el paso de los años, lejos de hacer perder protagonismo a la Directiva sobre protección de datos, incrementa la necesidad de interpretarla y determinar qué papel juega ésta, y por consiguiente la normativa nacional que de ella se derive, en una sociedad más interconectada que nunca.

En el año 1998, un periódico español publicó en su edición impresa dos anuncios concernientes a una subasta de inmuebles que se desarrollaba a raíz de la existencia de deudas a la Seguridad Social por parte del demandante en el litigio principal que da lugar a la sentencia objeto del presente comentario. En dichos anuncios se mencionaba el nombre y apellidos del citado deudor. Posteriormente, esta información fue puesta a disposición del público en la versión electrónica del periódico. Once años más tarde, el deudor cuyos inmuebles constaban en el anuncio se dio cuenta de que introduciendo su nombre completo en el motor de búsqueda de Google aparecían como resultados varias páginas del diario en el que aparecían los anuncios de la subasta celebrada años atrás.

En este contexto, el demandante en el litigio principal contactó con la editorial del periódico con la intención de que dichas informaciones desaparecieran de la red, afirmando que las informaciones del año 1998 carecían de relevancia en 2009, puesto que aquellas deudas con la Seguridad Social habían sido pagadas años atrás y en consecuencia el embargo ya se había levantado. La editorial respondió negativamente a la cancelación de sus datos esgrimiendo que la

[32] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, punto 25.

publicación se había realizado por orden del Ministerio de Trabajo y Asuntos Sociales. El demandante en el litigio principal se puso en contacto con Google Spain en febrero de 2010 y solicitó que el motor de búsqueda no arrojase como resultado las informaciones relativas al embargo de años atrás al introducir su nombre y apellidos en dicho motor, alegando que la información disponible en la red carecía de relevancia y, por tanto, que tenía derecho a que los resultados del motor de búsqueda relativos al embargo no apareciesen. Ante esa solicitud, Google Spain remitió al demandante a Google Inc., domiciliada en Estados Unidos, al considerar que esta empresa es quien presta el servicio de búsqueda en Internet[33].

Posteriormente, el demandante en el litigio principal presentó una reclamación ante la Agencia Española de Protección de Datos (AEPD), solicitando a ésta que obligase a la editorial del periódico a eliminar o modificar su publicación para que no apareciesen sus datos, o bien a utilizar los mecanismos de los que disponen los motores de búsqueda para proteger dichas informaciones. Al mismo tiempo, solicitaba que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales, de modo que éstos no apareciesen vinculados al procedimiento de embargo en los resultados de eventuales búsquedas y no se facilitasen enlaces a la edición electrónica del periódico. Su reclamación fue estimada parcialmente con fecha de 30 de julio de 2010[34], instando la AEPD a Google Spain y Google Inc. a tomar las medidas oportunas a fin de que los datos personales del demandante quedasen retirados de la información indexada por el motor de búsqueda y se impidiese así el acceso a la misma a partir de búsquedas efectuadas a través de dicho motor. La AEPD consideró que no había una disposición normativa que impidiese ejercer el derecho de cancelación frente a Google. Por el contrario, la AEPD desestimó la reclamación contra la editorial por considerar que la publicación de los datos en la prensa tenía justificación legal.

> La editorial del diario alegaba que la denegación de la cancelación de datos se debía a que la publicación no era de su responsabilidad, sino que la misma se había realizado "por medio del Ministerio de Trabajo y Asuntos Sociales a través de su Secretaría de Estado de la Seguridad Social, siendo ejecutora la Tesorería General de la Seguridad Social en la Dirección Provincial de Barcelona". En su resolución, la AEPD indica que la aparición de la información en el diario "se motiva legalmente en la publicación de subastas de inmuebles por la Unidad de Recaudación Ejecutiva, en el presente caso la Dirección Provincial de la Tesorería General de la Seguridad Social en Barcelona, cuyo fin pretendido era dar la máxima publicidad a las subastas para conseguir la mayor concurrencia de licitadores". En este sentido, la AEPD se refiere en particular al artículo 117.1 del Real Decreto 1415/2004, de 11 de junio, por el que se aprueba el Reglamento General de Recaudación de la Seguridad Social, el cual establece lo siguiente:
>
> "La subasta se publicará en el tablón de anuncios de la Dirección Provincial, de sus dependencias y de los ayuntamientos, en cuyas demarcaciones se hallen los bienes. Cuando el valor de los bienes supere la cuantía que se fije por resolución del Director General de la Tesorería General de la Seguridad Social, el anuncio de la subasta deberá insertarse, además, en el boletín oficial de la provincia o boletín oficial de la comunidad autónoma correspondiente. Cuando, a juicio del Director Provincial de la Tesorería General de la Seguridad Social, sea conveniente para el fin perseguido y resulte proporcionado con el valor de

[33] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, puntos 19 y 20.
[34] Resolución de la AEPD nº R/01680/2010 (Procedimiento nº TD/00650/2010), la cual se encuentra disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2010/common/pdfs/TD-00650-2010_Resolucion-de-fecha-30-07-2010_Art-ii-culo-16-LOPD_Recurrida.pdf (última consulta: 23 de enero de 2015).

> los bienes, podrá publicarse también el anuncio de la subasta en medios de comunicación de gran difusión o en publicaciones especializadas"[35].

Google Spain y Google Inc. interpusieron sendos recursos ante la decisión de la AEPD solicitando la nulidad de esta decisión, y, al llegar el asunto a la Audiencia Nacional, este órgano decidió suspender el procedimiento y plantear al Tribunal de Justicia de la Unión Europea varias cuestiones prejudiciales clasificadas en tres bloques. Esta clasificación se mantendrá en la exposición de las cuestiones que se llevará a cabo.

De esta forma, el órgano de remisión plantea cuatro cuestiones prejudiciales que se engloban en un primer grupo referido al ámbito de aplicación territorial de la Directiva sobre protección de datos y, por extensión, dada la armonización total que se ha hecho en este punto, de la normativa nacional que la transponga. Además, la Audiencia Nacional plantea otras cuatro cuestiones relativas a la actividad de los buscadores como proveedores de contenidos en relación con la mencionada directiva, es decir, estas cuestiones versan sobre el ámbito de aplicación material de la misma. Y en último lugar se plantea una cuestión prejudicial sobre si de la existencia de los derechos de supresión y bloqueo de los datos y de oposición reconocidos en los artículos 12.b) y 14.a) de la directiva sobre protección de datos, respectivamente, se deriva el reconocimiento también de un "derecho al olvido".

4. Ámbito de aplicación territorial de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales

Una de las razones por las cuales Internet supone un desafío para el Derecho es la diferente influencia que ejercen las cuestiones geográficas en ambos campos. De una parte, el Derecho tiene un fuerte componente territorial, puesto que las normas jurídicas varían de un lugar a otro en función de las características de cada sociedad, y los individuos se sienten más inseguros ante las normas que no proceden de los órganos de su país. Por el contrario, se puede decir que Internet no conoce fronteras. Si bien es verdad que los operadores en la red se adaptan a las condiciones de cada mercado para obtener el mejor rendimiento, lo cierto es que si por algo se caracteriza Internet es por ser una red global que conecta fácilmente lugares muy distantes y muy diferentes entre sí. En este contexto, los límites de cada Estado en cuanto a su poder de actuación son superados por los servicios prestados en la red, dificultándose así el control de estos servicios, por lo que la existencia normas internacionales y legislaciones coordinadas es especialmente conveniente[36]. Puede decirse que el ámbito de aplicación de la Directiva sobre protección de datos es amplio, puesto que sus efectos no se circunscriben al territorio del Espacio Económico Europeo[37]. Sin embargo, esta circunstancia no evita que surjan dudas sobre la aplicación de la mencionada Directiva, como se verá más adelante.

---

[35] Resolución de la AEPD nº R/01680/2010, de 30 de julio de 2010, hecho probado primero y fundamentos de Derecho sexto y duodécimo.

[36] DE ASÍS ROIG (2002, pp. 208 y 209); GUERRERO PICÓ (2006, pp. 333 y 334).

[37] Dictamen 8/2010 del Grupo del artículo 29 (p. 10).

El ámbito de aplicación territorial de la Directiva sobre protección de datos se recoge en su artículo 4. Así, en primer lugar, el artículo 4.1.a) de la Directiva señala que:

> "Los Estados miembros aplicarán las disposiciones nacionales que haya [sic] aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:
>
> a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable".

Del párrafo reproducido se desprenden dos criterios fundamentales para establecer la aplicación de la directiva en cuestión. Por un lado, que se lleve a cabo un tratamiento de datos personales. Por otro, la existencia de un establecimiento en un Estado miembro en el marco del cual el responsable del tratamiento lleva éste a cabo, no siendo necesario, por consiguiente, que el tratamiento de datos propiamente dicho se realice en el territorio comunitario[38]. Los conceptos de "tratamiento de datos personales" y "responsable del tratamiento" son expuestos en el apartado 5 del presente estudio porque tienen más relevancia a la hora de tratar el ámbito de aplicación material de la Directiva sobre protección de datos, por lo que será en dicho epígrafe donde se comenten. Ahora bien, conviene apuntar desde este momento que si una entidad tiene un "establecimiento" en territorio de la Unión Europea pero dicha entidad no es considerada "responsable del tratamiento" tal y como se define en la Directiva sobre protección de datos, ésta no será de aplicación.

La LOPD no parece seguir exactamente el criterio establecido en la Directiva, ya que para la aplicación de nuestra ley nacional sí es preciso que el tratamiento de datos personales se lleve a cabo de manera efectiva en territorio español, según el tenor literal de la norma. Dice el artículo 2.1.a) de la LOPD:

> "Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:
>
> a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento".

Pese a la dicción del artículo 2.1.a) de la LOPD, lo cierto es que este precepto ha sido interpretado de manera que en la práctica se sigue lo dispuesto en la Directiva sobre protección de datos. De hecho, la redacción del RPDP se aparta de la LOPD y recupera el criterio de la Directiva. Por consiguiente, el tratamiento de datos se someterá a la ley española cuando sea España el lugar donde se encuentre el establecimiento del responsable de dicho tratamiento, aunque éste no trate efectivamente los datos dentro del territorio nacional[39]. En este sentido, dice la letra a) del artículo 3.1 del RPDP:

[38] DE MIGUEL ASENSIO (2011, p. 334).

[39] SANCHO VILLA (2010, pp. 100-105).

> "Se regirá por el presente reglamento todo tratamiento de datos de carácter personal:
>
> a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español".

Ni la LOPD ni el RPDP resuelven la cuestión de qué sucede cuando el responsable del tratamiento está establecido al mismo tiempo en España y en otros Estados miembros. Sin embargo, la resolución de esta duda no parece resultar tan compleja en cuanto al criterio conforme al cual se lleva cabo la determinación de la ley aplicable como en la aplicación práctica de este criterio. Es decir, de acuerdo con el espíritu de la Directiva sobre protección de datos, parece que a cada tratamiento de datos habría de aplicársele la ley del lugar donde se encontrase el establecimiento al que se vinculase dicho tratamiento. Lo problemático es determinar el concreto establecimiento respecto del que se da la vinculación.

El concepto de "establecimiento" genera problemas en el ámbito de la sociedad de la información en relación con los prestadores de servicios en Internet, ya que muchas de las funciones que implican estos servicios se llevan a cabo a distancia y resulta complicado determinar qué parte del proceso se realiza en un lugar determinado. La Directiva sobre protección de datos aclara el concepto en su considerando 19, el cual dice que "el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable". Además, el mismo considerando señala que la forma jurídica empleada es un factor irrelevante a la hora de determinar si existe o no un "establecimiento" a los efectos de la Directiva, lo cual evita controversias en las situaciones en las cuales la actividad comercial, en lugar de llevarse a cabo mediante empresas filiales con personalidad jurídica propia, se desarrolla a través de sucursales o agencias. La Directiva sobre protección de datos se decanta así por una noción de establecimiento en la que prima el aspecto económico sobre elementos formales, el factor relevante es que a partir de dicho establecimiento se lleven a cabo operaciones de tratamiento de datos[40]. A este respecto se ha dicho que el lugar de tratamiento de los datos se encontrará en España no sólo cuando los servidores que recogen los datos se encuentren en nuestro país, sino también cuando el equipo en que se introducen los datos o donde éstos son captados esté situado en España[41].

> En el marco del análisis del concepto de establecimiento parece conveniente hacer referencia a la sentencia nº 1972/2010 de la Sección 4 Penal, del *Tribunale Ordinario di Milano*, dictada con fecha de 24 de febrero de 2010[42]. En esta resolución, que se refiere a servicios prestados por Google (concretamente, el servicio Google Videos), el juez tuvo que decidir si existía o no un establecimiento en Italia en el marco del cual se desarrollaban tales servicios o, de no existir tal establecimiento, si Google efectuaba un recurso a medios situados en el citado país. Todo ello, como se puede deducir, a efectos de determinar la aplicabilidad o no de la ley italiana sobre protección de datos. El juez consideró que sí existía un "establecimiento" en el sentido de la Directiva sobre protección de datos, y para ello tuvo en cuenta las

[40] DE MIGUEL ASENSIO (2011, pp. 333 y 334); SANCHO VILLA (2010, pp. 102 y 103).

[41] DE MIGUEL ASENSIO (2011, p. 334).

[42] Puede accederse a la misma en http://www.giurcost.org/casi_scelti/Google.pdf (última consulta: 5 de junio de 2014).

> actividades desempeñadas por la empresa filial en Italia. Así, la conclusión se basó en que Google Italia tenía que ser considerada una "mano operativa y comercial" de la empresa matriz Google Inc., que actuaba con cierta independencia de la matriz y operando como una unidad propia, y que podía gestionar publicidad mediante el servicio Google AdWords incluyendo enlaces en vídeos. Es decir, aunque los servidores que procesaban los contenidos se encontraban en Estados Unidos y tal procesamiento era llevado a cabo por Google Inc., Google Italia participaba en el proceso respecto de los vídeos subidos en Italia, promoviendo los servicios de Google Videos y gestionando la publicidad relacionada con los mismos[43].
>
> Esta sentencia fue recurrida, y el Tribunal de apelación de Milán (*Corte d'Appello di Milano*) dictó sentencia el 21 de diciembre de 2012. También la resolución de apelación fue recurrida, resolviéndose el recurso en la sentencia del Tribunal Supremo italiano (*Corte Suprema di Cassazione*) de 17 de diciembre de 2013. Sin embargo, en estos recursos fueron discutidas otras cuestiones, diferentes del concepto de establecimiento y la aplicabilidad de la legislación italiana[44].

La noción de establecimiento a efectos de la normativa sobre protección de datos puede compararse con la tomada en otros ámbitos de los servicios de la sociedad de la información. A este respecto, debe mencionarse en primer lugar la letra c) del artículo 2 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)[45]. DE MIGUEL ASENSIO indica que el precepto referido, el cual contiene la definición de "prestador de servicios establecido", recogió la noción de establecimiento que había proporcionado la sentencia del entonces Tribunal de Justicia de las Comunidades Europeas *The Queen / Secretary of State for Transport, ex parte Factortame*[46]. En esta sentencia, el Tribunal de Justicia señaló que el concepto de establecimiento "implica el ejercicio efectivo de una actividad económica por medio de una instalación permanente en otro Estado miembro por una duración indeterminada"[47].

> El concepto de establecimiento que toma la ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE nº 166, de 12.7.2002) (en adelante, LSSI) al transponer la Directiva sobre el comercio electrónico, resulta más preciso que ésta. Así, del apartado primero del artículo 2 de la LSSI se desprende que el establecimiento de un proveedor de servicios es el lugar donde está efectivamente centralizada la gestión administrativa y la dirección de sus negocios. Para el caso de que el prestador de servicios de la sociedad de la información sea residente o tenga su domicilio en otro Estado, la LSSI será aplicable en virtud del apartado segundo de su artículo 2 cuando tal prestador ofrezca sus servicios a través de un establecimiento permanente situado en España, entendiendo por "establecimiento permanente" las instalaciones o lugares de trabajo en los que realice toda o parte de su actividad el prestador de servicios de manera continuada o habitual. A pesar de la mayor precisión del legislador español, lo cierto es que el hecho de que la LSSI se aparte de la Directiva sobre el comercio

[43] SARTOR / VIOLA DE AZEVEDO CUNHA (2010, p. 363).

[44] La sentencia que puso fin al proceso se encuentra disponible en el enlace http://www.cortedicassazione.it/Documenti/2014_5107.pdf (última consulta: 5 de junio de 2014).

[45] DO L 178, de 17 de julio de 2000, p. 1.

[46] Sentencia del TJCE de 25 de julio de 1991 (The Queen / Secretary of State for Transport [Ministro de Transportes] ex parte: Factortame Ltd. y otros, C-221/89, Rec. p. I-3905). Véase DE MIGUEL ASENSIO (2011, p. 145).

[47] Sentencia *The Queen / Secretary of State for Transport, ex parte Factortame*, apartado 20.

> electrónico puede dificultar la coordinación con otras normas españolas, como ha puesto de relieve DE MIGUEL ASENSIO[48].

Si el responsable del tratamiento no se encuentra establecido en el territorio de un Estado miembro, el tratamiento de datos personales entrará en el ámbito de aplicación de la Directiva sobre protección de datos cuando el establecimiento esté situado en un lugar donde la legislación nacional de un Estado miembro sea aplicable en virtud del Derecho internacional público. Así lo dice la letra b) del artículo 4.1 de la citada Directiva. La misma previsión se establece en el Derecho interno español, y más concretamente en la letra b) del artículo 2.1 de la LOPD y en la letra b) del artículo 3.1 del RPDP. De esta forma, si no se cumple la regla general contenida en la letra a) del artículo 2.1 de la LOPD, ya expuesta, el tratamiento de datos se regirá por la ley española cuando nuestras normas internas de Derecho internacional público establezcan que al responsable del tratamiento le es de aplicación la legislación española.

Por otra parte, la letra c) del artículo 4.1 de la Directiva sobre protección de datos prevé otra situación en la cual un tratamiento de datos se regirá por las leyes nacionales aprobadas para la aplicación de tal Directiva pese a que el responsable del tratamiento carezca de un establecimiento en un Estado miembro. Se pretende tener en cuenta la existencia de situaciones en las que, a pesar de no haber un establecimiento, el tratamiento de los datos personales tiene una clara conexión con un Estado que forma parte de la Unión[49].

> "Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea".

En el mismo sentido, la letra c) del artículo 2.1 de la LOPD determina que esta ley es de aplicación:

> "c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito".

Otro concepto sobre el que deben hacerse algunas consideraciones en el presente estudio es el de "recurso a medios". Hay dos elementos que caracterizan estos "medios". El primero es su carácter instrumental, es decir, su función es hacer posible el tratamiento de datos personales. El segundo es su carácter permanente, o lo que es lo mismo, no participan en el proceso de tratamiento de datos de manera puntual. Por supuesto, en la práctica no resulta siempre sencillo diferenciar un medio de lo que no lo es, sobre todo en cuanto al factor de la permanencia. Así, por un lado es complicado establecer la línea que delimita el uso de un medio con fines de mero tránsito de lo que constituye un auténtico recurso permanente. Por otro lado, también puede ser difícil diferenciar un medio permanente de un establecimiento en sí mismo, si bien en este caso la

[48] DE MIGUEL ASENSIO (2011, p. 146).

[49] Dictamen 8/2010 del Grupo del artículo 29 (pp. 21 y 22).

distinción pierde importancia porque la ley nacional en cuestión sería aplicable en ambos casos[50].

> En su Dictamen 8/2010, el Grupo del artículo 29 ha precisado que el "recurso" no supone un control pleno del medio por parte del responsable del tratamiento, sino que éste ejerza a través de él algún tipo de actividad. Por otra parte, el Grupo del artículo 29 constata que la noción de "medios" no se corresponde exactamente con el término *equipment* usado en la versión inglesa de la Directiva, pero que ambas palabras han de recibir el mismo significado de cara a la aplicación de la misma. Además, en el referido dictamen se recuerda que la Directiva no exige que los medios sean automatizados, y que es conveniente hacer un análisis caso por caso para establecer cuándo se trata de un "medio" y cuándo no, reflejando las dudas persistentes sobre si la recogida de datos personales a través de los ordenadores de los usuarios implica la aplicación de la Directiva sobre protección de datos si dichos ordenadores se encuentran en un Estado miembro[51]. Y es que el hecho de que el uso de *cookies* y mecanismos similares se considere un recurso a medios, haciendo aplicable la legislación nacional sobre protección de datos del lugar donde se encuentre el equipo sobre el que actúan dichos mecanismos, es objeto de controversia. Así lo expone DE MIGUEL ASENSIO, quien hace referencia a las opiniones que dicen que este criterio podría conducir una aplicabilidad excesiva de las legislaciones nacionales de los Estados comunitarios[52].
>
> Por otro lado, y como constata el Abogado General en sus conclusiones en la sentencia *Google Spain y Google*, el Grupo del artículo 29 se manifestó al respecto del criterio del "recurso a medios" planteando la posibilidad de que en el futuro este criterio se vea complementado por otro, como es la orientación hacia las personas de las actividades llevadas a cabo por los responsables del tratamiento de datos que no están establecidos en la Unión Europea. De adoptarse esta modificación, la normativa de la Unión Europea en materia de protección de datos resultaría aplicable a responsables del tratamiento establecidos en terceros países cuya actividad de prestación de servicios se dirigiese al territorio comunitario, como ya sucede por ejemplo en el Reglamento (CE) n° 44/2001 del Consejo, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil[53] o en algunas de las legislaciones nacionales que incorporan la Directiva sobre el comercio electrónico[54].

Una vez efectuadas las anteriores consideraciones sobre el ámbito de aplicación territorial de la Directiva sobre protección de datos, procede referirse a la primera de las cuatro cuestiones prejudiciales de la sentencia *Google Spain y Google* que se pueden englobar en un primer grupo

---

[50] Sobre el concepto de "recurso a medios", DE MIGUEL ASENSIO (2011, pp. 335-339) y SANCHO VILLA (2010, pp. 107-113).

[51] Dictamen 8/2010 del Grupo del artículo 29 (pp. 23 y 24).

[52] DE MIGUEL ASENSIO (2011, pp. 336 y 337).

[53] DO L 12, de 16 de enero de 2001, p. 1. Hay que indicar que el Dictamen 8/2010 del Grupo del artículo 29 se refiere específicamente al artículo 15.1.c) del Reglamento 44/2001 (Reglamento Bruselas I). Este Reglamento ha sido derogado en virtud del artículo 80 del Reglamento (UE) 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil, denominado Reglamento Bruselas I bis (DO L 351, de 20 de diciembre de 2012, p. 1). El Reglamento Bruselas I bis entró en vigor el 10 de enero de 2014, siendo aplicables desde esta fecha sus artículos 75 y 76, mientras que los restantes son aplicables desde el 10 de enero de 2015, como se establece en su artículo 81. Por lo tanto, la referencia al artículo 15.1.c) del Reglamento Bruselas I que se hace en el mencionado Dictamen debe entenderse hecha al artículo 17.1.c) del Reglamento Bruselas I bis.

[54] Dictamen 8/2010 del Grupo del artículo 29 (WP 179), p. 28; conclusiones del Abogado General en la sentencia *Google Spain y Google*, punto 56.

que versa sobre el ámbito de aplicación territorial de la Directiva sobre protección de datos y de la normativa nacional que la transpone. En este sentido, se plantea si existe un "establecimiento" en el sentido del artículo 4.1.a) de la directiva cuando concurren uno o varios supuestos que se citan seguidamente. El primero de estos supuestos es la creación por parte de la empresa proveedora del motor de búsqueda de una oficina o filial en un Estado miembro destinada a la promoción y venta de los espacios publicitarios del buscador en un Estado miembro, dirigiéndose la actividad publicitaria a los habitantes del Estado en cuestión. El segundo de los supuestos se refiere a la empresa matriz que designa como su representante a una filial ubicada en un Estado miembro, otorgándole la responsabilidad del tratamiento de los ficheros relativos a los datos de los clientes que contrataron publicidad con dicha empresa. Y la última de las situaciones propuestas se produce cuando la oficina o filial establecida en un Estado miembro traslada a la empresa matriz las solicitudes y requerimientos relativos a la protección de datos que le plantean los afectados o las autoridades nacionales competentes.

El Tribunal de Justicia de la Unión Europea no tuvo muchas dudas a la hora de dar una respuesta positiva. Tras recordar que el considerando 19 de la Directiva sobre protección de datos vincula la existencia de un establecimiento al ejercicio "efectivo y real de una actividad mediante una instalación estable", constata que Google Spain cumple con esta descripción[55]. El Tribunal también señala que Google Spain goza de personalidad jurídica propia y que es una filial de Google Inc., pero lo cierto es que estos hechos no son importantes a la hora de considerar si hay o no un establecimiento, como dice el propio considerando mencionado.

Para que la Directiva sobre protección de datos sea aplicable se requiere además que el tratamiento de datos se efectúe en el marco de las actividades del establecimiento del responsable del tratamiento en el territorio del Estado miembro, estimando el Tribunal de Justicia que este requisito también se cumple. El TJUE tiene en cuenta el hecho de que Google Spain es la entidad a través de la cual la empresa matriz Google Inc. lleva a cabo la promoción y venta en España "de los espacios publicitarios del motor de búsqueda", lo cual permite que el servicio del motor de búsqueda resulte rentable. Por ello, resulta imposible establecer una separación entre la actividad de ambas empresas, teniendo en cuenta que entre los resultados que arroja el motor de búsqueda se encuentran ofertas publicitarias que el gestor del motor pretende que respondan a los intereses y preferencias del usuario del servicio. Así las cosas, se concluye que se cumplen los criterios contenidos en el artículo 4.1.a) de la Directiva sobre protección de datos, y por tanto ésta es aplicable "cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro"[56].

> El Tribunal de Justicia coincide en este aspecto con el Abogado General, para quien también es preciso examinar el modelo de negocio del proveedor del servicio del motor de búsqueda en cuestión. La publicidad a partir de los términos de búsqueda es esencial, ya que constituye "la razón de ser económica para proveer una herramienta de localización de información gratuita en forma de motor de búsqueda". Para poder aprovechar las posibilidades económicas del servicio que ofrece, el proveedor

[55] Sentencia *Google Spain y Google*, apartados 48 y 49.

[56] Sentencia *Google Spain y Google*, apartados 55 a 60. Véase también MUÑOZ (2014, pp. 4 y 5).

referido necesita tener implantación en los diferentes Estados miembros a través de "establecimientos" en el sentido de la Directiva sobre protección de datos. El establecimiento constituye un nexo entre el servicio ofrecido en el mercado y la fuente de ingresos que lo hacen rentable, por lo que es innegable que el tratamiento de datos personales que se efectúa en el caso de la sentencia *Google Spain y Google* tiene lugar en el marco de las actividades del establecimiento que gestiona el mercado publicitario, y por tanto la Directiva sobre protección de datos es de aplicación[57]. El razonamiento del Tribunal y del Abogado General es similar al que hizo el *Tribunale Ordinario di Milano* en el caso que ha sido mencionado en un momento anterior en este artículo.

El resto de cuestiones del bloque relativo al ámbito de aplicación territorial de la Directiva no serán objeto de una exposición detallada, puesto que al haber resuelto la primera de manera afirmativa, el Tribunal de Justicia consideró que no era preciso valorar las demás.

La segunda de las cuestiones de este primer grupo versaba sobre el artículo 4.1.c) de la Directiva sobre protección de datos, y, más concretamente, si tal artículo debía interpretarse en el sentido de que existía un "recurso a medios situados en el territorio de dicho Estado miembro" cuando un buscador utilizase arañas o robots para localizar e indexar la información contenida en páginas web ubicadas en servidores de ese Estado miembro o cuando utilizase un nombre de dominio propio de un Estado miembro y dirigiese las búsquedas y los resultados en función del idioma de ese Estado miembro. La tercera de las cuestiones sobre el ámbito de aplicación territorial de la Directiva sobre protección de datos también incidía en el concepto de "recurso a medios" y en el artículo 4.1.c) de la misma, consistiendo la cuestión en si estaba incluido en esta noción el almacenamiento temporal de la información indexada por los buscadores en Internet, y en caso afirmativo, si podía entenderse que este criterio de conexión concurre en el caso en el cual la empresa aduce motivos de carácter competitivo para negarse a revelar el lugar donde almacena los índices utilizados por los motores de búsqueda.

Mediante la última cuestión del primer grupo, la cual se planteaba con independencia de las respuestas a las demás, el órgano de remisión quería conocer si la normativa que transpone la Directiva sobre protección de datos ha de aplicarse, a la luz del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea[58], en el país miembro donde la controversia tenga su centro de gravedad, haciendo posible una tutela más eficaz de los derechos de los ciudadanos de la Unión Europea. El artículo 8 de la Carta, que se refiere a la protección de datos de carácter personal, dice en su apartado primero que "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan". En su apartado segundo, el artículo 8 de la Carta dispone que "estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación". Y en el apartado tercero del artículo 8 de la Carta se establece que "el respeto de estas normas quedará sujeto al control de una autoridad independiente".

Al respecto de esta última cuestión puede precisarse que el Abogado General daba una respuesta negativa en sus conclusiones, esto es, el centro de gravedad de la controversia no podía servir como un criterio a tomar en consideración para determinar la aplicación de las normas sobre protección de datos. El Abogado General sostenía que el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea debía tenerse en cuenta al interpretar los conceptos empleados en el artículo 4.1 de la Directiva

[57] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, puntos 64 a 68. Sobre la relación existente entre Google Inc. y sus filiales radicadas en los diferentes Estados miembros a efectos de la aplicabilidad de la Directiva sobre protección de datos, puede consultarse el análisis que se hace, centrándose en la normativa italiana en materia de protección de datos, en SARTOR / VIOLA DE AZEVEDO CUNHA (2010, pp. 363 y 364).

[58] DO C 83, de 30 de marzo de 2010, p. 389.

> sobre protección de datos, pero que ello no significaba que los criterios de conexión establecidos por el legislador comunitario pudiesen extenderse, ya que la armonización del ámbito territorial de aplicación de la normativa en materia de protección de datos es total. A continuación, el Abogado General se remitía a lo dicho por el Grupo del artículo 29 en su Dictamen 8/2010 sobre el Derecho aplicable, y determinaba que el ámbito de aplicación territorial de la Directiva sobre protección de datos y, por consiguiente, de las normas nacionales que la desarrollen, dependían de criterios como la ubicación del establecimiento del responsable del tratamiento, o bien la ubicación de los medios o del equipo que se esté utilizando cuando el responsable del tratamiento esté establecido fuera del Espacio Económico Europeo. Por el contrario, la nacionalidad o la residencia habitual de la persona cuyos datos personales son tratados no son criterios decisivos en este sentido, así como tampoco lo es la ubicación física de tales datos[59].

5. Ámbito de aplicación material de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales

La Directiva sobre protección de datos establece en su artículo 3.1 que sus disposiciones son aplicables al "tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero", indicando el artículo 3.2 una serie de excepciones a la regla anterior, casos en los que dicha Directiva no se aplicará:

> "Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:
>
> - efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;
>
> - efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas".

Por otra parte, el artículo 2.b) de la Directiva sobre protección de datos contiene el concepto de "tratamiento de datos". Dice este artículo:

> "A efectos de la presente Directiva, se entenderá por: b) «tratamiento de datos personales» («tratamiento»): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción".

La LOPD sigue una sistemática similar. En cuanto a su ámbito de aplicación material, el artículo 2.1 de la LOPD señala que esta ley es aplicable "a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de

[59] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, puntos 54, 55 y 58; y Dictamen 8/2010 del Grupo del artículo 29 sobre el Derecho aplicable, pp. 9 y 10. Véase también BOTANA GARCÍA / OVEJERO PUENTE (2014, p. 9).

estos datos por los sectores público y privado". De igual forma que en la Directiva sobre protección de datos, en nuestra ley nacional también se establecen excepciones a la regla general. En el apartado segundo del propio artículo 2 de la LOPD se establece:

> "El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:
>
> a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
>
> b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
>
> c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos".
>
> Por su parte, el apartado tercero del artículo 2 de la LOPD prevé que el tratamiento de datos efectuado en ciertos ámbitos se regirá por las leyes especiales correspondientes, siendo la LOPD de aplicación supletoria a dichas leyes más específicas:
>
> "Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:
>
> a) Los ficheros regulados por la legislación de régimen electoral.
>
> b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
>
> c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
>
> d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
>
> e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia."

Puede concluirse que tanto la Directiva sobre protección de datos como la LOPD requieren para su aplicación dos elementos fundamentales. En primer lugar, la existencia de una serie de datos personales, es decir, información sobre una persona física que la identifica o que puede identificarla por sí sola o en conjunción con otros datos, según la noción que quedó apuntada en el epígrafe 2 del presente trabajo. Y en segundo lugar, se requiere la existencia de un "fichero" o soporte duradero que permita contener dichos datos personales y tratarlos, esto es, realizar con ellos operaciones de recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, atendiendo a la definición de "tratamiento de datos" que se contiene en el artículo 3.c) de la LOPD[60].

> El artículo 2.c) de la Directiva define "fichero de datos personales" como "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o

[60] DE ASÍS ROIG (2002, pp. 204 y 205).

repartido de forma funcional o geográfica". Por su parte, el artículo 3.b) de la LOPD dispone que a los efectos de la ley se considerará un fichero "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

En la sentencia *Google Spain y Google*, el segundo bloque de cuestiones prejudiciales se encuentra compuesto por cuatro cuestiones que parten de la actividad de los buscadores en Internet y de la posición jurídica que ostenta el proveedor de servicios del motor de búsqueda, en relación con los supuestos de hecho previstos por la Directiva sobre protección de datos que determinan su ámbito de aplicación material. Al enunciar la cuestión prejudicial se explica que la actividad de Google consiste en "localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia". Antes de proseguir la exposición hay que analizar, al menos en líneas generales, el funcionamiento de los motores de búsqueda, puesto que como es lógico, si no se establece primero en qué consiste la actividad del buscador de Google no puede darse una respuesta a si tal actividad puede englobarse en las conductas recogidas en la Directiva sobre protección de datos.

Siguiendo la explicación de BATTELLE, la estructura de un motor de búsqueda consta de tres partes, que son el rastreo, el índice y el procesador o servidor de consultas[61]. En primer lugar, el motor de búsqueda utiliza un programa rastreador que le permite consultar todas las páginas web. El motor de búsqueda realiza estas consultas de manera constante, recoge las páginas que encuentra y las reenvía al índice para su catalogación, obteniendo en el proceso nuevas direcciones en las que realizar esa misma tarea. En este primer momento, por tanto, el motor de búsqueda es un recipiente de información dada por terceros, información que se va recopilando a partir de un rastreo permanente en Internet[62]. Dice el Abogado General en sus conclusiones en la sentencia *Google Spain y Google* que el motor de búsqueda solicita a las páginas que le envíen una copia de las mismas y registra estas copias en su memoria oculta, registrando también al mismo tiempo las palabras clave presentes en las páginas analizadas. Al recoger la información que se encuentra disponible en páginas web de terceros, el motor de búsqueda recopilará datos personales si las páginas web rastreadas contienen este tipo de datos[63].

Toda la información que recibe el rastreador, incluyendo no sólo el contenido de las páginas web en sentido estricto, sino también archivos de diferentes tipos e información sobre las propias páginas web, es remitida a un índice, que ha sido definido como una "base de datos masiva", a fin de que esa información pueda ser utilizada posteriormente[64]. El índice del motor de búsqueda se compone en primer término de la combinación de las palabras clave con las direcciones URL[65]

[61] BATTELLE (2006, p. 34). También se encuentra una breve descripción del proceso de búsqueda a través de Google en la Resolución de la AEPD nº R/01680/2010, de 30 de julio de 2010, hecho probado tercero y fundamento de Derecho séptimo, apartado V.

[62] APARICIO SALOM (2009, p. 94); BATTELLE (2006, p. 35); BENGHOZI (2008, pp. 84 y 85); DE MIGUEL ASENSIO (2011, p. 320).

[63] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, puntos 34 y 73.

[64] BATTELLE (2006, p. 36); BENGHOZI (2008, p. 85).

[65] Siglas de *Uniform Resource Locator*, "Localizador Uniforme de Recursos".

que identifican un recurso en la red y permiten su posterior localización en la misma[66]. La parte del índice que no ha sido procesada todavía organiza lo recopilado de manera que de cada dirección URL se pueden precisar las palabras, los enlaces y el texto de los enlaces que se contienen en ella. Es decir, sabiendo una dirección URL pueden conocerse las palabras clave asociadas a la misma. Pero los motores de búsqueda actuales van más allá. Mediante algoritmos, es decir, conjuntos de operaciones preestablecidas que permiten obtener la solución de un problema, el motor de búsqueda determina la relevancia de cada página en relación con una consulta concreta.

> Aunque no es el único algoritmo utilizado por el motor de búsqueda de Google, el algoritmo más conocido es el denominado *PageRank*, que fue el primero utilizado por dicho motor. Al respecto de este algoritmo, BATTELLE señala: "[el algoritmo] examina los enlaces de una página, el texto de enlace que se encuentra entre las etiquetas de un enlace y la popularidad de las páginas que enlazan con otra página y los analiza en su conjunto para determinar la importancia final de una página en particular relación a su consulta"[67].

Los índices, además, contienen también etiquetas o clasificaciones de las páginas webs según un criterio determinado, como el idioma o la temática del contenido, lo cual resulta imprescindible para que los resultados arrojados por el motor de búsqueda se correspondan con lo que el internauta quiere. La información recopilada en el rastreo, ya analizada y clasificada, se recoge en una base de datos que proporcionará al internauta los resultados de su búsqueda y que se denomina índice de tiempo de ejecución[68]. Los usuarios realizan la búsqueda dentro del índice del motor que utilicen, esto es, el servidor de consultas de dicho motor conecta la búsqueda con el índice para después realizar la conexión en sentido inverso, mostrando al usuario la información contenida en dicho índice. En su búsqueda en el índice el servidor de consultas se sirve de las etiquetas y catalogaciones efectuadas, utiliza palabras clave, descarta expresiones o términos generales, e incluso puede servirse de la información sobre las anteriores búsquedas efectuadas desde el mismo equipo. Con esto se pretende minimizar los efectos de la poca precisión de la inmensa mayoría de las búsquedas efectuadas a través de los motores, llevadas a cabo introduciendo muy pocos términos que además pueden mostrar intereses muy dispares. De esta forma, entre los resultados que se ofrecen no se encuentran páginas que, si bien responden a las palabras introducidas, no se corresponden con el interés de la consulta, o al menos se reduce el número de estos resultados insatisfactorios[69].

> Los motores de búsqueda desarrollan un "servicio de intermediación", tal y como se define en la letra b) del Anexo de la LSSI:
>
> "b) «Servicio de intermediación»: servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información. Son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios

---

[66] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, punto 73.
[67] BATTELLE (2006, p. 37).
[68] BATTELLE (2006, pp. 36 y 37).
[69] BATTELLE (2006, pp. 38-41). En el mismo sentido, APARICIO SALOM (2009, pp. 94 y 95); TENE (2008, pp. 1450 y 1451).

> suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet".

Un motor de búsqueda será mejor cuanto mejor realice los tres bloques de actividades que se han descrito. En este sentido, se ha afirmado que el valor de un motor de búsqueda depende del volumen y actualidad de la información indexada, de la calidad de la indexación, y de la adecuación de la respuesta a la búsqueda efectuada[70].

La primera cuestión prejudicial del bloque relativo al ámbito de aplicación material de la Directiva 95/46/CE en la sentencia *Google Spain y Google* consiste en determinar si la actividad expuesta llevada a cabo por el motor de búsqueda está comprendida en el concepto de "tratamiento de datos" contenido en el artículo 2.b) de la misma, el cual ha sido reproducido al comienzo del presente apartado. El Tribunal de Justicia y el Abogado General coinciden en este punto, ya que ambos consideran que no hay duda de que la actividad del motor de búsqueda de Google lleva a cabo un tratamiento de datos personales en el sentido de la Directiva. En el litigio no se discute que entre los datos que el motor de búsqueda encuentra, indexa, almacena y pone a disposición del usuario del motor se encuentran datos de carácter personal. En este contexto, los amplios términos en los que se redacta el artículo 2.b) de la Directiva sobre protección de datos hacen que se incluya en el precepto una actividad como la del motor de búsqueda, que "recoge", "extrae", "registra", "organiza" y "conserva" datos personales, para posteriormente comunicarlos y facilitar el acceso a los mismos. No altera esta conclusión el hecho de que el motor de búsqueda no modifique los datos y que éstos hayan sido publicados por terceros en algún medio de comunicación[71].

Creo que en este caso el Tribunal de Justicia acierta en su conclusión. El argumento con el que Google Spain y Google Inc. sostienen que no se produce un tratamiento es que los motores operan con la información disponible en la red sin distinguir entre lo que constituyen datos personales y las informaciones que no lo son, pero no considero que este elemento sea relevante a la hora de determinar si se produce un tratamiento de datos personales o no, tal y como aparece redactado el artículo 2.b) de la Directiva sobre protección de datos. En este artículo se describen diversas operaciones que constituirán un tratamiento de datos personales siempre que tales operaciones como la recogida, el registro, la organización, la conservación, la elaboración, la modificación, la extracción o la consulta, sean "aplicadas a datos personales". Por tanto, la clave reside en cómo interpretar la expresión entrecomillada. Si se entiende, como hacen Google Spain y Google Inc., que las conductas descritas en el artículo han de aplicarse únicamente a datos personales o al menos siendo consciente de que se está actuando sobre este tipo de datos, entonces el motor de búsqueda en cuestión no realizaría un tratamiento de datos personales. Si por el contrario se interpreta que la Directiva requiere simplemente que las operaciones enumeradas en el precepto se realicen de manera efectiva, sin importar la consciencia o no al llevarlas a cabo, entonces Google sí trata datos personales, porque el motor de búsqueda procesa datos en general y los datos personales forman parte de éstos. El Tribunal de Justicia y el

[70] BENGHOZI (2008, p. 86).

[71] Sentencia *Google Spain y Google*, apartados 27 a 31; conclusiones del Abogado General en la sentencia *Google Spain y Google*, punto 71 y 72.

Abogado General optan por esta segunda interpretación.

En mi opinión, la conclusión a la que llegan el Tribunal y el Abogado General es correcta, porque la propia definición del artículo 2.b) contempla la posibilidad de que las actividades descritas en el mismo puedan llevarse a cabo mediante "procedimientos automatizados", lo cual presupone una no discriminación entre los datos personales y el resto de la información. Cuestión diferente es que la definición de la Directiva sea acertada o no, aspecto que sin duda podría ser objeto de debate.

Para el caso de que el Tribunal de Justicia estimase que la actividad del motor de búsqueda constituye un tratamiento de datos, como finalmente ha sucedido, se solicita al Tribunal que responda si el proveedor del motor búsqueda es "responsable del tratamiento" de los datos personales que se contienen en las páginas que indexa, tal y como se define el concepto en el artículo 2.d) de la Directiva sobre protección de datos. En virtud del artículo citado:

> "A efectos de la presente Directiva, se entenderá por: d) «responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario"[72].

La cuestión de la responsabilidad del intermediario es un tema que ha despertado el interés de la doctrina desde siempre, por ser una cuestión ciertamente compleja. En este contexto, se ha planteado hasta qué punto ha de ser responsable un intermediario por la información contenida en las páginas web fuente a las que dicho intermediario remite, ya que éste, aun cuando almacena en sus servidores la información que recoge de las fuentes, normalmente lo hace de manera automática y sin pretender conocer los contenidos de lo almacenado y transmitido[73]. Los motores de búsqueda desafían esta concepción, la cual no responde exactamente a ellos, pero tampoco les es del todo ajena. Los más modernos motores de búsqueda sí quieren conocer el contenido de las páginas web fuente. Por supuesto, los motores no pretenden saberlo todo sobre este contenido y tomar una visión de conjunto, como un investigador que examina varios artículos jurídicos sobre un tema con el ánimo de extraer ideas, analizarlas, formarse una opinión general y defender una postura que pueda plasmar en un trabajo propio. Sin embargo, debe recordarse que uno de los factores de los que depende la calidad de un motor de búsqueda es la adecuación entre la búsqueda del usuario y las respuestas que le son ofrecidas, y tal adecuación es más fácil de conseguir si el motor de búsqueda "conoce", en cierta forma, el contenido de la información que recoge. Este conocimiento, no obstante, no parece que se refiera al carácter personal o no de la información. Lo que desde luego no admite duda es que la actividad del motor de búsqueda se realiza de forma automática.

> Al negar su responsabilidad sobre los contenidos recopilados, Google suele alegar que el servicio que

[72] LLOYD (2014, p. 57) indica que el elemento clave para concluir que nos encontramos ante un responsable del tratamiento es la capacidad de quien procesa una información para determinar "la naturaleza y la extensión" de dicho procesamiento.

[73] REED / ANGEL (2007, pp. 239 y 240).

presta es de almacenamiento de datos o *hosting*, el cual es tratado en el ámbito del artículo 14 de la Directiva sobre el comercio electrónico[74]. Este precepto ordena a los Estados miembros garantizar que "cuando se preste un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio, el prestador de servicios no pueda ser considerado responsable de los datos almacenados a petición del destinatario", si se cumplen dos condiciones. La primera de ellas es que el prestador de servicios no conozca la ilicitud de la actividad o información, así como que en lo que se refiere a una acción por daños y perjuicios, no tenga conocimiento de hechos o circunstancias que revelen el carácter ilícito de dicha actividad o información. La segunda es que el prestador de servicios actúe rápidamente para eliminar los datos o impedir el acceso a los mismos tan pronto como sepa de la ilicitud referida anteriormente. Por tanto, Google considera que no se le puede hacer responsable de lo publicado por terceros, si no conoce de manera efectiva la información que recopila[75].

La atribución de responsabilidad a los intermediarios y la persecución de éstos en lugar de la web fuente cuentan a su favor con ciertas razones, como por ejemplo la mayor capacidad económica del intermediario, dar solución a los casos en los que la situación geográfica del infractor dificulta la acción contra él, y la mayor eficacia que tiene actuar sobre el intermediario ante ciertos tipos de pretensiones, como impedir el acceso futuro a una determinada información[76].

A este respecto, y en el ámbito del Derecho español, es importante mencionar el artículo 11 de la LSSI, en el cual se recoge el deber de colaboración de los prestadores de servicios de intermediación. En el apartado primero de dicho artículo 11 se establece que cuando un órgano competente hubiese ordenado la interrupción "de la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España", el mismo órgano puede ordenar a los intermediarios que suspendan los servicios utilizados "para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados", si la colaboración del intermediario es necesaria para que esta última orden se cumpla. La misma previsión se contiene en el apartado segundo del artículo 11 de la LSSI, para el caso en el que se haya acordado "la interrupción de la prestación de un servicio o la retirada de contenidos procedentes de un prestador establecido en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo", si es preciso impedir el acceso desde España a dichos contenidos y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación establecidos en España.

En cualquier caso, no parece que esté cerca de su fin el debate recogido por algunos autores sobre si los motores de búsqueda son meros recipientes de datos y su actividad se circunscribe al almacenaje de los mismos o si por el contrario son en sí mismos proveedores de contenidos. En el mismo sentido, queda mucho camino por recorrer en el terreno de la responsabilidad de los intermediarios[77]. Quizás en este debate entren en juego dos factores. Por un lado, el hecho de que si bien los motores de búsqueda parecen meras herramientas de intermediación entre el internauta y las páginas web fuente, lo cierto es que las empresas que gestionan dichos motores se relacionan cada vez más con los titulares de las páginas webs que publican la información que luego se indexa[78]. Por otro, que los propios titulares de

[74] SARTOR / VIOLA DE AZEVEDO CUNHA (2010, p. 369).

[75] Esto es especialmente importante para el caso de publicación por terceros de contenidos difamatorios, como señalan REED / ANGEL (2007, pp. 243, 255-265). Sobre esta cuestión puede consultarse también LLOYD (2014, pp. 509-519).

[76] REED / ANGEL (2007, p. 240).

[77] REED / ANGEL (2007, pp. 278-279); SARTOR / VIOLA DE AZEVEDO CUNHA (2010, pp. 369-371).

[78] BENGHOZI (2008, p. 88).

> los motores de búsqueda prestan otro tipo de servicios electrónicos, utilizando sus propios motores de búsqueda para dar la mayor difusión posible a sus servicios[79]. En tal caso, la actividad de almacenamiento de datos y la puesta de éstos a disposición de los usuarios daría paso a una conducta mucho más activa, pudiendo alcanzar el grado de generación de contenidos[80].
>
> En este sentido, es necesario hacer referencia a las conclusiones del Abogado General en la sentencia *Google Spain y Google*. En dichas conclusiones, el Abogado General dice que aunque el rastreo de las páginas web se hace de manera continuada, puede resultar que desde el indexado de la información se hayan producido cambios en la página web rastreada o ésta haya sido eliminada, por lo que la página mostrada por el motor de búsqueda podría no coincidir con la página fuente, ofreciendo información que ya no se encuentra disponible en ésta[81]. Al mismo tiempo se constata que con el fin de que el usuario maneje más fácilmente los resultados que el motor de búsqueda le ofrece, éste no sólo muestra en enlace a las páginas web fuente, sino que incluye "extractos de texto, contenido audiovisual o incluso instantáneas de las páginas web fuente". Y lo cierto es que a veces esta información adicional puede recuperarse "a partir de los dispositivos del proveedor de servicios de motor de búsqueda en Internet, y no instantáneamente desde la página web original", por lo que se concluye que el proveedor del servicio de búsqueda posee de manera efectiva la información adicional[82].

En la sentencia *Google Spain y Google*, el Tribunal de Justicia considera que el proveedor de un motor de búsqueda es responsable del tratamiento, a diferencia de la opinión del Abogado General. El Tribunal incide en la definición de "responsable del tratamiento" proporcionada por el artículo 2.d) de la Directiva sobre protección de datos, y considera que el gestor del motor de búsqueda determina los fines y los medios del tratamiento de datos personales que lleva a cabo, por lo que adquiere la condición de responsable. El TJUE aplica además un criterio teleológico, al decir que la Directiva pretende otorgar a los interesados una protección eficaz y completa, y que ello podría verse comprometido si la ausencia de control sobre los datos personales fuese un factor suficiente para no considerar responsable del tratamiento al gestor de un motor de búsqueda. El Tribunal de Justicia también pone de manifiesto que introducir el nombre de una persona en un buscador permite obtener un perfil de esta persona, ya estructurado y más o menos completo, lo que sin duda puede afectar a la vida privada de los particulares y a la protección de sus datos personales en mayor medida de lo que lo pueden hacer las páginas web fuente[83]. Por tanto, el gestor del motor de búsqueda debe garantizar "en el marco de sus responsabilidades, de sus competencias y de sus posibilidades" que sus servicios cumplen con las exigencias de la Directiva sobre protección de datos, y ello debe ir más allá de actuar de la no indexación de los contenidos que los editores de las páginas web quieran vedar al buscador

[79] SARTOR / VIOLA DE AZEVEDO CUNHA (2010, p. 370).

[80] Al respecto de la aplicabilidad de la Directiva sobre protección de datos a diferentes servicios prestados por Google, así como la competencia judicial internacional en este mismo ámbito, véase SLOOT / BORGESIUS (2012, pp. 81-91).

[81] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, puntos 73 y 74. También DE MIGUEL ASENSIO (2011, p. 321).

[82] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, punto 35.

[83] En este sentido puede consultarse el Informe *Guidelines*, punto 4.

mediante el empleo de protocolos de exclusión y códigos[84].

Mi opinión al respecto difiere de la del Tribunal y coincide con la del Abogado General, sobre la base precisamente de que el sistema automatizado del motor de búsqueda no discrimina entre datos personales y datos no personales. Si bien en cuanto a la noción de "tratamiento" esta circunstancia no parece ser relevante habida cuenta de los términos en los que se define el concepto en la Directiva, sí lo es en cuanto a la noción de "responsable del tratamiento". Como indica con acierto en sus conclusiones el Abogado General, el criterio clave para calificar a una persona como "responsable del tratamiento" es que dicha persona determine "los fines y los medios del tratamiento de datos *personales*" (cursiva en el original), es decir, una persona sólo es responsable del tratamiento cuando sea "consciente de la existencia de una categoría determinada de información que contiene datos personales" y trate estos datos "con una intención relacionada con su tratamiento *como* datos personales" (cursiva en el original)[85].

El Abogado General considera que la Directiva sobre protección de datos parte de la premisa de que el responsable del tratamiento "sabe lo que está haciendo en relación con los datos personales de que se trata, en el sentido de que es consciente de qué tipo de datos personales está tratando y por qué". El proveedor de servicios del motor de búsqueda carece de esta consciencia, ya que en la operación que lleva a cabo el motor de búsqueda los datos personales no aparecen claramente diferenciados del resto. El Abogado General alude a lo establecido por el Grupo del artículo 29 en su dictamen 1/2008 sobre cuestiones relativas a los motores de búsqueda. En este dictamen se afirma que el "principio de proporcionalidad requiere que, en la medida en que un proveedor de un motor de búsqueda actúe exclusivamente como intermediario, no debe considerarse como responsable principal del tratamiento de datos personales efectuado". El Abogado General constata que el proveedor del buscador en Internet no tiene relación con el contenido de páginas web fuente, sobre el que carece de control alguno. Por ello, en opinión del Abogado General el proveedor de servicios de búsqueda en Internet "no puede ni jurídicamente ni de hecho cumplir las obligaciones del responsable del tratamiento"[86].

> En este sentido, coincido con BOTANA GARCÍA cuando afirma que el funcionamiento del motor de búsqueda es "exclusivamente tecnológico", automático, que el buscador es "una herramienta de localización de información que no ejerce ningún control sobre los datos personales incluidos en las páginas web de terceros", por lo que "su intervención se limita a indexar y mostrar la información publicada en webs"[87].
>
> Sin embargo, VILASAU SOLANA comparte la respuesta del Tribunal de Justicia y considera que Google es un responsable del tratamiento, basando su posición en que "los buscadores permiten una visualización, inmediatez y ubicuidad de la información que sin estos no sería posible", por lo que considera que se "realiza algo más que una mera localización de información". En realidad, la posición de VILASAU SOLANA se justifica fundamentalmente en razones de tipo práctico, puesto que a su juicio es poco

[84] Sentencia *Google Spain y Google*, apartados 32 a 40. Véase también MUÑOZ (2014, pp. 2 y 3).

[85] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, puntos 80 a 82.

[86] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, puntos 83 a 89.

[87] BOTANA GARCÍA (2014, p. 16).

> conveniente no considerar responsable del tratamiento al gestor del motor de búsqueda, "teniendo en cuenta el protagonismo de los motores de búsqueda en el actual marco de la sociedad de la información"[88]. En esta misma línea, DE MIGUEL ASENSIO ha puesto de manifiesto que la consideración de los gestores de los buscadores como responsables del tratamiento se ve favorecida por la gran importancia de los mismos para el acceso de las personas a la información, mencionando también que la posición de dominio que ostenta Google "puede implicar ciertas cargas que en un contexto (estructura de mercado) diferente no se producirían"[89].
>
> Por otro lado, BOTANA GARCÍA y OVEJERO PUENTE plantean que es posible sostener que el motor de búsqueda determina los fines del tratamiento de datos cuando los resultados que ofrece están acompañados de contenidos publicitarios, pero no cuando la búsqueda carece de vinculación con la actividad comercial, puesto que en este caso el buscador no muestra los resultados para sus propios fines[90]. Adoptando este criterio tampoco se requeriría que el motor de búsqueda fuese consciente de que los datos que trata constituyen datos personales y que el tratamiento de los mismos se realizase en cuanto tales.

Resulta sorprende que el Tribunal de Justicia no haya hecho alusión al punto 90 de las conclusiones del Abogado General en la sentencia *Google Spain y Google*, puesto que una respuesta al argumento contenido en dicho punto 90 resultaba esencial, en mi opinión, para que la postura del Tribunal fuese defendible. El Abogado General hizo notar el resultado absurdo al que se llegaría si se considerase que el gestor de un motor de búsqueda es responsable del tratamiento. Así, el Abogado General indicó que los motores de búsqueda en Internet serían incompatibles con el Derecho comunitario si en alguna de las páginas web de terceros constasen los datos personales a los que se refiere el artículo 8.1 de la Directiva sobre protección de datos. Estos datos personales son aquellos que revelan el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, o se tratase de datos relativos a la salud o a la sexualidad. El mencionado artículo 8.1 obliga a los Estados miembros a prohibir el tratamiento de este tipo de datos salvo cuando se cumplen con estrictos requisitos, y el Abogado General afirma con acierto que "la actividad del proveedor de servicios de motor de búsqueda en Internet sería automáticamente ilegal" si no se cumpliese con estas condiciones[91].

> Una de estas circunstancias que legitimarían el tratamiento de datos personales relativos a las cuestiones señaladas en el artículo 8.1 de la Directiva sobre protección de datos es que "el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado". Por tanto, si el proveedor del servicio de búsqueda es considerado responsable de tratamiento, sería ilegal la indexación de cualquier página que contenga datos personales sobre el origen racial o étnico de una persona, sus opiniones políticas, sus convicciones religiosas o filosóficas, su pertenencia a sindicatos, sus condiciones de salud o su sexualidad, siempre que la persona sobre la que se refieran los datos no haya dado su consentimiento expreso para que el motor de búsqueda haga tal indexación.

[88] VILASAU SOLANA (2014, p. 22).

[89] DE MIGUEL ASENSIO (2014, pp. 8-10).

[90] BOTANA GARCÍA / OVEJERO PUENTE (2014, pp. 10 y 11).

[91] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, punto 90.

> No obstante, el Abogado General señaló que hay ciertos casos en los cuales el proveedor de un servicio de motor de búsqueda sí puede ser considerado "responsable del tratamiento". Y es que si bien el proveedor del servicio del motor de búsqueda no controla el contenido de las páginas web fuente, sí controla la estructura el índice y puede bloquear algunos resultados, al igual que puede elegir respetar o no los códigos de exclusión utilizados por la fuente y optar por no actualizar una web aunque el responsable de ésta se lo solicite. En estos casos, a modo de excepción, el Abogado General entiende que el proveedor sí es responsable del tratamiento de datos personales[92].
>
> Por su parte, VILASAU SOLANA reconoce que aplicando de forma estricta las normas sobre protección de datos la situación de los buscadores sería "completamente ilegal", pero precisa que "no es una solución adecuada negar el carácter de responsable al buscador por el hecho de que las consecuencias de esta interpretación no se consideren adecuadas o deseables"[93].

Para el caso de que Google fuese considerado responsable del tratamiento, se plantea una tercera pregunta al Tribunal de Justicia de la Unión Europea consistente en determinar si la autoridad nacional de control de datos puede exigir a la empresa que gestiona el buscador la retirada de sus índices de una información publicada por terceros, sin habérselo exigido previamente o hacerlo en el mismo momento al titular de la página web que recoge la información indexada por el motor de búsqueda. Finalmente, si la pregunta anterior también recibe una respuesta afirmativa deberá afrontarse otra cuestión, cual es si el deber de tutelar los derechos de protección de datos personales que tienen los servicios de búsqueda en Internet resulta excluido cuando los datos personales se encuentran contenidos en una información publicada lícitamente por terceros y se mantienen disponibles en la página web de origen.

En la medida en que se hace responsable del tratamiento al proveedor del servicio del motor de búsqueda en Internet y se predica el deber de dicho proveedor de garantizar que el tratamiento de datos que realiza cumple con los requisitos de la Directiva sobre protección de datos, se produce la contraposición entre los derechos de las personas sobre las que versa la información en internet y los derechos de los usuarios del motor de búsqueda. Por una parte, en virtud del artículo 12.b) de la Directiva sobre protección de datos el interesado puede ejercer frente al responsable del tratamiento los derechos de rectificación, supresión y bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva. Por otra, con base en el artículo 14.a) de la Directiva el interesado podrá ejercer un derecho de oposición, también frente al responsable del tratamiento. El contenido de estos derechos será objeto de una exposición más extensa en el apartado 6 del presente estudio. En el otro lado de la balanza se encuentra la libertad de información de los internautas, en relación también con el derecho de los proveedores de motores de búsqueda a ofrecer en el mercado un producto de estas características. Los derechos que aparecen enfrentados se encuentran recogidos en la Carta de los Derechos Fundamentales de la Unión Europea, más concretamente en los artículos 7, 8 y 11:

> "Artículo 7. Respeto de la vida privada y familiar.
>
> Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

[92] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, puntos 91 a 93.

[93] VILASAU SOLANA (2014, p. 22).

> Artículo 8. Protección de datos de carácter personal.
>
> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le 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 le conciernan y a obtener su rectificación.
>
> 3. El respeto de estas normas estará sujeto al control de una autoridad independiente
>
> Artículo 11. Libertad de expresión y de información.
>
> 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o 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".

Sin embargo, en este punto el Tribunal de Justicia de la Unión Europea no lleva a cabo una verdadera ponderación entre los diferentes intereses y derechos en juego, sino que la misma resulta muy breve y a mi juicio insuficiente. Al resolver las cuestiones relativas al ámbito de aplicación material de la Directiva sobre protección de datos, el Tribunal de Justicia realiza más bien, a mi modo de ver, un alegato en favor únicamente de los derechos de las personas cuyos datos se encuentran en Internet, no prestando especial consideración a la libertad de información.

El Tribunal de Justicia recuerda que el objetivo de la Directiva es garantizar un elevado nivel de protección a las personas físicas en cuanto al tratamiento de sus datos personales, en relación con la protección de su vida privada. Asimismo, se refiere a los ya reproducidos artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, y proclama las obligaciones que la Directiva sobre protección de datos impone al responsable del tratamiento con el fin de garantizar la efectividad de estos derechos. Así, el responsable del tratamiento está obligado a adoptar todas las medidas que sean razonables para que los datos sean suprimidos o rectificados cuando tales datos no sean tratados de manera leal y lícita, cuando sean recogidos con fines determinados, explícitos y legítimos pero posteriormente sean objeto de un tratamiento incompatible con estos fines, cuando no sean adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben, cuando no sean exactos o no estén actualizados, y cuando sean conservados en una forma que permita la identificación de los interesados más allá del período necesario para los fines para los que fueron recogidos. De igual forma, el interesado tiene derecho a negarse a que sus datos sean tratados, salvo que la legislación nacional disponga otra cosa[94].

Sentado lo anterior, el Tribunal de Justicia determina que el interesado puede ejercitar sus derechos frente al responsable del tratamiento, y cuando éste no atienda al requerimiento del interesado, la autoridad nacional en materia de protección de datos y los tribunales deben actuar. El TJUE toma en consideración que la mayor accesibilidad a la información que proporcionan los motores de búsqueda puede afectar a la vida privada de las personas, reitera la idea de que los buscadores facilitan el hacer perfiles de una persona al introducir su nombre en los mismos, y

[94] Sentencia *Google Spain y Google*, apartados 66 a 76.

concluye que el interés económico del gestor del motor de búsqueda no es un argumento con la suficiente entidad como para contrarrestar estos peligros. El Tribunal tampoco considera suficiente argumento el hecho de que la supresión de algunos resultados de la lista arrojada por el buscador afecta al interés legítimo de los internautas en cuanto a su derecho a obtener información. Por eso, dice el TJUE, el equilibrio de intereses en casos como el del litigio principal ordena hacer prevalecer el de la persona cuyos datos figuran en internet. En otros casos, no obstante, la naturaleza de la información de que se trate y el grado de afectación de dicha información a la vida privada de la persona afectada, así como la existencia de un interés público en obtener la información, por ejemplo por la relevancia pública que una persona pueda tener, son factores que deberán ser considerados en la ponderación de intereses[95].

Por otra parte, hay que tener en cuenta que la eficacia de la protección que la Directiva sobre protección de datos pretende garantizar sería menor si sólo se pudiese actuar contra el gestor del motor de búsqueda cuando al mismo tiempo se obtuviese la eliminación de la información en la página web fuente. También es relevante el hecho de que los intereses de los gestores de los motores de búsqueda y de los editores de las páginas web fuente son distintos, lo que puede alterar el resultado de la ponderación de intereses que se haga. En este contexto, resulta adecuado en opinión del Tribunal que tanto la autoridad nacional en materia de protección de datos como los tribunales puedan ordenar al gestor del motor de búsqueda que elimine de la lista de resultados algunos vínculos, incluso cuando no se requiera de manera previa o simultánea a la página web fuente la eliminación de esa misma información[96].

> El Tribunal de Justicia no ha seguido la opinión del Abogado General. Para éste, el gestor del motor de búsqueda no es responsable del tratamiento salvo en casos muy puntuales, y por consiguiente frente a él no cabe ejercer los derechos de rectificación, supresión y bloqueo de datos y de oposición al tratamiento. Pero incluso en aquellas situaciones en las que el Abogado General considera que el gestor del motor de búsqueda es un responsable del tratamiento, entiende que sólo podría ordenársele la retirada de información de su índice cuando el proveedor de servicios no ha respetado los códigos de exclusión o no ha atendido una solicitud de actualización de la página web fuente hecha por el editor de la misma. Y eso porque, como afirma el Abogado General, un responsable del tratamiento debe cumplir los requisitos establecidos en el artículo 6 de la Directiva sobre protección de datos, esto es, los datos personales que trate deben ser adecuados, relevantes y no excesivos en relación con los fines para los que han sido recogidos, así como estar actualizados. Por consiguiente, el Abogado General dice que "en la medida en que el enlace es adecuado, en el sentido de que los datos correspondientes al término de búsqueda aparecen realmente o han aparecido en las páginas web enlazadas, a mi juicio el índice cumple los criterios de adecuación, relevancia, proporcionalidad, exactitud y completitud, establecidos en el artículo 6, letras c) y d), de la Directiva"[97]. En mi opinión, tanto la solución propuesta por el Abogado General como la argumentación en la que se basa son impecables.

[95] Sentencia *Google Spain y Google*, apartados 77 a 81.

[96] Sentencia *Google Spain y Google*, apartados 82 a 88.

[97] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, puntos 94 a 98.

6. El derecho al olvido

La razón por la cual se plantea la existencia de un derecho al olvido es análoga a la razón por la cual la protección de datos ha crecido en importancia en los últimos en tiempos. Las nuevas tecnologías permiten almacenar muy fácilmente información que quedará a disposición de otras personas en el futuro, de modo que el paso del tiempo ya no supone la pérdida de la información, con las ventajas que ello implica. Pero esto también tiene sus riesgos, puesto que preservar la información sobre una persona puede no ser lo que ésta desearía, e incluso podría llegar a causarle perjuicios[98].

De esta forma, lo que subyace tras la intención de alguien de que "se le olvide" es la mera voluntad de permanecer en el anonimato en la medida de lo posible, en lugar de ser esclavo a lo largo del tiempo de lo que se pudo conocer sobre él en el pasado. De manera análoga al derecho general a no ser molestado (*to be let alone*) del que hablaban WARREN y BRANDEIS, y al que ya se hizo referencia en su momento, el derecho al olvido permitiría colmar las aspiraciones del individuo que no quiere verse importunado en el futuro por informaciones aparecidas tiempo atrás[99]. Un derecho a ser olvidado de carácter pleno iría más allá que el derecho a la intimidad, pues abarcaría también informaciones públicas que no están cubiertas por la obligación de respeto por la vida privada de las personas[100]. En este contexto, un genuino derecho al olvido permitiría a la persona que ha publicado por sí misma una opinión en una página web que dicha opinión desapareciese. De esta forma, el derecho al olvido vendría a responder al hecho de que, como ha puesto de manifiesto algún autor, "las personas cambian, evolucionan, maduran e incluso se contradicen a lo largo de su trayectoria vital"[101]. Bajo el derecho al olvido pleno al que se está aludiendo también quedarían amparadas las aspiraciones de quien se ha convertido en un personaje público en el pasado pero desea perder tal carácter llegado un momento determinado, interesándole al mismo tiempo que desaparezcan declaraciones que hizo cuando participaba en la vida pública de la sociedad y existía un interés general en conocerlas[102].

Para el caso de que la información accesible en Internet haya sido compartida o publicada por el propio individuo, como sucede con las opiniones manifestadas en blogs o la participación en redes sociales, el debate sobre derecho al olvido podría tomar en consideración las nociones de

[98] HERNÁNDEZ LÓPEZ (2013, p. 116); ROSEN (2012, pp. 88 y 89).

[99] En este sentido, LETTERON (1996, pp. 388-390) dice que quien desea ser olvidado aspira "a ser dejado en paz" (*à être laissé en paix*).

[100] LETTERON (1996, p. 413).

[101] SIMÓN CASTELLANO (2011, p. 394).

[102] LETTERON (1996, pp. 417 y 418).

confidencialidad, revelación e incremento de la accesibilidad de la información[103]. Tomando como referencia a SOLOVE, puede decirse que la confidencialidad protege a quien comparte una información con terceros y tiene expectativas en que dicha información permanezca en ese círculo en base a una relación de confianza. La revelación de la información puede ser perjudicial para el individuo porque afecte a su reputación o, simplemente, porque se le hace esclavo de su pasado. Y el riesgo generado por el aumento de la accesibilidad de la información es que informaciones públicas sobre las personas que antes permanecían desconocidas para gran parte de la sociedad, hoy están al alcance de cualquiera[104].

> Estas tres nociones pueden relacionarse con el derecho al olvido. En primer lugar, quien ha publicado una información sobre sí mismo puede pretender confidencialidad, en el sentido de que sólo accedan a dicha información el círculo de personas que acudan directamente a la página web fuente, y no quien lo haga tras utilizar un buscador. En segundo lugar, el interesado puede querer que no se revele información sobre él cuando se haya accedido a ella por cualquier motivo. Esto es especialmente importante en materia de motores de búsqueda, ya que el interesado puede querer que el motor no revele a los usuarios del mismo una información que se ha obtenido al rastrear las páginas web fuente. Y por último, porque el peligro que suponen los motores de búsqueda para la intimidad de la personas viene, precisamente, por hacer más fácil el acceso a la información e incrementar el riesgo de revelación de información sobre terceros.

En definitiva, el establecimiento de un auténtico derecho al olvido debería implicar no sólo la desaparición de información comprometida en el momento actual para una persona, sino también de información que a la larga pueda suponerle algún perjuicio de cualquier tipo[105]. Pero no se detendría ahí, sino que alcanzaría a toda aquella información que careciese de este potencial efecto dañino. La razón para ello sería que el individuo en cuestión simplemente no quiere que se conozcan detalles sobre él, aunque en el pasado su voluntad fuese diferente[106].

> Cuando se alude al sacrificio que los poderes públicos imponen a los ciudadanos en cuanto a su derecho a la intimidad por razones de seguridad, tal sacrificio es aceptado por muchos ciudadanos con el argumento de que si no hay nada que esconder no hay por qué rechazar la pérdida de intimidad a cambio de una mayor seguridad. SOLOVE ha tratado la cuestión de la recopilación de información por parte de los servicios de seguridad estatales y se ha mostrado contrario a este argumento, poniendo de relevancia que la noción de intimidad engloba muchas situaciones diferentes entre sí, y desde luego mucho más que la mera posibilidad de esconder una mala acción[107]. Tomando en consideración esta noción de intimidad, según la cual el individuo también debe estar protegido frente a situaciones que no

[103] Sobre el quebrantamiento de la confidencialidad, si bien en relación con la cesión a terceros de los datos de los usuarios de los motores de búsqueda por parte de los titulares de éstos, pueden consultarse SOLOVE (2006, pp. 524-527) y TENE (2008, pp. 1486-1490).

[104] SOLOVE (2006, pp. 525-538).

[105] En este sentido pueden verse SOLOVE (2006, p. 487) y SOLOVE (2007, p. 769). El autor sostiene que uno de los problemas que plantea la intimidad no se manifiesta en un daño efectivo a la reputación de una persona, sino en la creación del riesgo de que ese daño pueda producirse en el futuro.

[106] Sin embargo, BOTANA GARCÍA / OVEJERO PUENTE (2014, p. 13) vinculan el derecho al olvido con la reputación, el honor y la propia imagen, indicando que este derecho sólo puede ser protegido cuando la información perjudicial o no pertinente supone además una vulneración del "derecho a la intimidad y propia imagen en términos constitucionales".

[107] SOLOVE (2007, p. 764).

> le son humillantes, vergonzosas o que afectan a su reputación, puede defenderse un derecho al olvido con un gran alcance: es irrelevante que la información que alguien quiere que sea olvidada le perjudique o no, lo fundamental es que la persona sobre la que trata la información tiene interés en que ésta desaparezca.

El último bloque de cuestiones prejudiciales en la sentencia *Google Spain y Google* está integrado por una única cuestión. En ésta se plantea la existencia de un derecho al olvido a partir de los derechos de supresión y bloqueo de los datos, reconocido en el artículo 12.b) de la Directiva sobre protección de datos, y de oposición, recogido en el 14.a) de la misma Directiva. El órgano de remisión de la cuestión prejudicial pregunta si estos dos artículos comportan el derecho del interesado a requerir de los buscadores que no se indexe la información referida a su persona aparecida en páginas web de terceros de manera lícita, si su voluntad es que dicha información "no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada". Para un correcto análisis de la cuestión conviene exponer previamente en qué consisten los derechos de supresión y bloqueo de los datos y de oposición y cómo los contemplan la Directiva sobre protección de datos y la normativa española correspondiente.

En primer lugar, y al respecto del derecho de supresión y bloqueo de datos, dice el artículo 12.b) de la citada Directiva:

> "Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos".

Al transponer el artículo 12.b) reproducido, el legislador español optó por la denominación de "derecho de rectificación y cancelación", que se recoge en el artículo 16 de la LOPD. Pese a la terminología empleada por el legislador español, debe quedar claro que se trata de dos derechos diferentes y alternativos[108]. Estos derechos de rectificación y cancelación se reconocen para el caso de que el titular de los datos detecte que sus datos contenidos en un fichero son inexactos, incompletos, inadecuados o excesivos, por lo que es preciso que previamente el interesado haya tenido acceso a los datos[109]. Por ello, algún autor ha expuesto estos derechos como derivados del derecho de acceso, es decir, de conocer la información que sobre uno mismo tiene un tercero[110].

Como se desprende del artículo 31 del RPDP, mediante el derecho de rectificación el interesado pretende que sus datos inexactos o incompletos se corrijan a fin de que se correspondan con la realidad. Por ello, al interesado no le basta con solicitar la rectificación, sino que también debe demostrar la exactitud de los nuevos datos que constarán[111]. En este sentido, considero que no sólo debe reputarse inexacta cualquier información que sea falsa, sino también la que induzca a error[112]. Por su parte, quien ejerce su derecho de cancelación busca la eliminación de sus datos

[108] GUERRERO PICÓ (2006, p. 298); SERRANO PÉREZ (2010, p. 1223).

[109] GUERRERO PICÓ (2006, p. 298); HERNÁNDEZ LÓPEZ (2013, pp. 75 y 76); TRONCOSO REIGADA (2010, p. 559).

[110] LLOYD (2014, pp. 129-131).

[111] APARICIO SALOM (2009, p. 255); TRONCOSO REIGADA (2010, p. 559). Véase también el artículo 32.1 del RPDP.

[112] LLOYD (2014, pp. 107, 108 y 130).

que sean inadecuados o excesivos o, si se prefiere, la supresión y bloqueo de datos innecesarios o no pertinentes[113]. En virtud del artículo 16.3 de la LOPD, la eliminación de los datos da lugar al bloqueo de los mismos, si bien se encontrarán a disposición de las administraciones públicas, jueces y tribunales para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas, pasado el cual se suprimirán definitivamente. Además, el artículo 16.4 de la LOPD extiende el deber de rectificación y cancelación a los terceros a quienes el responsable del tratamiento haya comunicado los datos objeto de rectificación o cancelación.

Diferente del derecho de supresión y bloqueo de datos es el derecho de oposición, el cual consiste en la negativa de una persona a que sus datos de carácter personal sean tratados o a dicho tratamiento se mantenga, cuando se viniese produciendo con anterioridad. Al respecto del derecho de oposición, el artículo 14.a) de la Directiva establece:

> "Los Estados miembros reconocerán al interesado el derecho a:
>
> a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos".
>
> Hay que señalar que el artículo 7 de la Directiva sobre protección de datos contempla una serie de condiciones para que el tratamiento de datos personales pueda tener lugar. Las letras e) y f) a las que se hace mención en el precepto anteriormente reproducido contemplan, respectivamente, los casos en los que el tratamiento de datos personales "es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos", y cuando "es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva".

En nuestro Derecho hay que referirse a los artículos 6.4 de la LOPD y 34 del RPDP.

> El artículo 6.4 de la LOPD dice:
>
> "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".
>
> Por su parte, en el artículo 34 del RPDP se define el derecho de oposición recogiendo además el carácter dual del mismo. Por un lado, se trata del derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal, y por otro, el derecho a que cese un tratamiento que se viene produciendo. El mismo artículo 34 del RPDP precisa los supuestos en los cuales nos encontramos ante el derecho de oposición:
>
> "a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

---

[113] SERRANO PÉREZ (2010, p. 1226).

> b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.
>
> c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento".

Debe resaltarse que el derecho de oposición, tal y como se configura en la normativa española, se reconoce para los casos en los cuales el tratamiento de datos no precisa consentimiento previo por parte del individuo al que se refieren los datos. Como bien expone algún autor, cabe plantearse si el derecho de oposición sólo entra en juego cuando el tratamiento de datos personales no es ilícito, esto es, cuando la falta de consentimiento previo no convierte en ilegal dicho tratamiento[114]. La interpretación de la ley española que se obtiene siguiendo un criterio gramatical se puede observar también en la STC 292/2000, de 30 de noviembre, ya mencionada anteriormente. En esta sentencia, el Tribunal Constitucional se refirió a la "libertad informática" y mantuvo que ésta comprende "entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".

No obstante, el legislador español debía cumplir con el mandato del artículo 18.4 de la Constitución española y limitar 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". La LOPD y el RPDP son parte de los instrumentos normativos de los que el legislador se sirvió para dar cumplimiento a ese mandato constitucional, optando en dicha labor por otorgar al derecho de oposición un contenido determinado, al preverlo como un mecanismo de defensa contra el uso legítimo de los datos personales sin consentimiento previo del interesado. Por tanto, a los efectos de la ley y del reglamento, el derecho de oposición se da sólo ante usos legítimos de los datos personales, bien impidiendo los usos que podrían tener lugar en el futuro, bien interrumpiendo los usos que se viniesen produciendo ya. Cuestión distinta es que al derecho de oposición considerado en abstracto pueda dársele un alcance mucho más amplio y vincularlo al poder de disposición y control sobre los propios datos personales, de modo que el derecho a oponerse englobe también el derecho a no consentir el uso de los datos en aquellos casos en los cuales el consentimiento es imprescindible para que el tratamiento de datos sea legítimo[115].

Como puede deducirse de la exposición realizada, el derecho al olvido comparte ciertas características con los derechos de cancelación y oposición. Quien pretende "ser olvidado" busca un resultado similar al que pretende quien quiere que sus datos sean eliminados o que no puedan ser tratados. De hecho, el artículo 17 de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), de 25 de enero de 2012[116], se recoge un "derecho al olvido y a la supresión"

[114] VILLAVERDE MENÉNDEZ (2010, p. 495).

[115] VILLAVERDE MENÉNDEZ (2010, pp. 497-500).

[116] COM (2012) 11 final.

que consiste, según se establece en el apartado primero de dicho precepto, en que "el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión". Este derecho no constituye un genuino derecho al olvido, puesto que sólo se otorga al interesado, de acuerdo con el propio artículo 17.1 de la Propuesta de Reglamento, cuando se produce alguna de las circunstancias siguientes:

> "a) los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados;
>
> b) el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el artículo 6, apartado 1, letra a), o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos;
>
> c) el interesado se opone al tratamiento de datos personales con arreglo a lo dispuesto en el artículo 19;
>
> d) el tratamiento de datos no es conforme con el presente Reglamento por otros motivos".
>
> Hay que decir que en la Resolución legislativa del Parlamento Europeo sobre la citada Propuesta de Reglamento, de 12 de marzo de 2014[117], se han eliminado las referencias al derecho al olvido. De esta forma, por ejemplo, mientras que el considerando 53 de la Propuesta de Reglamento comenzaba diciendo que "toda persona debe tener derecho a que se rectifiquen los datos personales que le conciernen y «derecho al olvido»", en el texto de 2014 se dice que "toda persona debe tener derecho a que se rectifiquen los datos personales que le conciernen y «derecho a la supresión»". Y la rúbrica del artículo 17 de la Propuesta, "derecho al olvido y a la supresión", ha quedado reducida a "derecho a la supresión". Así, el artículo 17.1 queda redactado del siguiente modo en la Resolución legislativa del Parlamento Europeo:
>
> "1. El interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión y, en relación con terceros, a que estos supriman todos los enlaces a los datos personales, copias o reproducciones de los mismos, cuando concurra alguna de las circunstancias siguientes:
>
> a) los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados;
>
> b) el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el artículo 6, apartado 1, letra a), o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos;
>
> c) el interesado se opone al tratamiento de datos personales con arreglo a lo dispuesto en el artículo 19;
>
> c bis) un tribunal o una autoridad reguladora con sede en la Unión ha dictaminado de forma definitiva e irrevocable que han de suprimirse los datos de que se trate;
>
> d) los datos han sido tratados ilícitamente"[118].

De esta forma, el derecho al olvido puede definirse como la facultad del individuo para exigir que otros no puedan acceder a información sobre él, un "derecho a retirarse del sistema y

---

[117] P7_TA(2014)0212.

[118] Sobre la Propuesta de Reglamento de 2012 y el texto aprobado por el Parlamento Europeo en 2014, véase VILASAU SOLANA (2014, pp. 28-31).

eliminar la información personal que la red contiene"[119]. Sin embargo, la pretensión en abstracto de una persona de que se le olvide no tendría por qué partir en todo caso de una situación en la cual la información fuese incorrecta, excesiva o perjudicial de alguna manera para el sujeto del que se trate, que son los presupuestos que dan lugar a los derechos de cancelación y oposición. El contenido del derecho al olvido que se plantea en la cuestión prejudicial correspondiente en la sentencia *Google Spain y Google* tiene un alcance mucho más limitado que el de un derecho al olvido puro. Dicha cuestión prejudicial es planteada de la siguiente manera:

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

Por un lado, y dado que la Directiva sobre protección de datos sólo se refiere a datos personales, la respuesta del Tribunal de Justicia sobre el derecho al olvido sólo se proyecta sobre este tipo de datos, y no a cualquier información disponible sobre una persona que ésta quiera que se elimine. Por otro, en la cuestión prejudicial no se hace referencia a una desaparición total de Internet de los datos personales, ya que no se discute la posibilidad de que una página web pueda contener información personal si ha sido lícitamente publicada, sino simplemente si puede ordenarse que tal información personal no sea indexada por los motores de búsqueda. Ciertamente, en la cuestión prejudicial se alude expresamente a que el fin de esta pretensión de olvido es que la información no sea conocida por los internautas sobre la base de la desaparición de la finalidad para la que tales datos habían sido recabados o divulgados. Sin embargo, el Tribunal de Justicia de la Unión Europea no se enfrenta a la eliminación de la información en las páginas web fuente, sino que sólo evalúa la facultad de una persona para dificultar el conocimiento de la información que le concierne. Los internautas seguirán pudiendo acceder a la información personal sobre la persona acudiendo al origen de la información, por lo que el derecho al olvido que busca el demandante en el litigio principal puede decirse que es, en realidad, un derecho a censurar determinados contenidos en el motor de búsqueda con el fin de que la información personal se vea afectada por los obstáculos que existían con anterioridad a la aparición de las nuevas tecnologías y, en particular, de los buscadores[120].

No obstante, por otra parte, la cuestión prejudicial no limita el hipotético derecho al olvido a los casos en los cuales la información sobre una persona pueda perjudicarle. En mi opinión, la formulación de la cuestión prejudicial diferencia dos supuestos. El primero de ellos consiste en la voluntad del interesado de que los internautas no puedan acceder a la información sobre él cuando crea que ese acceso le podría perjudicar. La segunda, cuando el individuo quiere que esa información se pierda con el paso del tiempo, sin más.

El Tribunal de Justicia comienza indicando que el derecho de supresión reconocido en el artículo

[119] SIMÓN CASTELLANO (2011, p. 395).

[120] De hecho, en el Informe *Guidelines* no se hace referencia en ningún momento a la noción de "olvido", sino que se opta por hablar de "remoción de una lista" o *de-listing*.

12.b) de la Directiva sobre protección de datos no entra en juego únicamente cuando los datos sean inexactos, sino también cuando son inadecuados, no pertinentes, excesivos en relación a los fines del tratamiento, cuando no están actualizados o cuando se conservan por más tiempo del debido. El paso del tiempo juega un importante papel en cuanto a la licitud del tratamiento de datos, ya que dicho carácter lícito puede estar presente al inicio del tratamiento y perderse tiempo después. El Tribunal proclama que el tratamiento de datos personales ha de ser legítimo en todo momento, y por eso cuando la información que aparece en los resultados de un motor de búsqueda es inadecuada, no pertinente o excesiva en relación con los fines para los que el motor de búsqueda la obtiene, los resultados que contienen esa información no pueden ser ofrecidos al usuario del motor de búsqueda. Y ello con independencia de si la información que aparece en los resultados causa un perjuicio o no al interesado[121].

El Tribunal establece que el derecho a la eliminación de la lista de resultados de los enlaces que contengan datos personales inadecuados, no pertinentes o excesivos prevalece como regla general tanto sobre el interés económico del gestor del motor de búsqueda como sobre la libertad de información de los usuarios del motor y su consiguiente derecho a recibir información de acuerdo con el artículo 11 de la Carta de los Derechos Fundamentales de la Unión Europea. Por el contrario, prevalecerían estos últimos derechos sobre los de la persona a la que se refiere la información en cuestión si se apreciase la existencia de un interés público en conocer tal información, habida cuenta del papel que el individuo en cuestión desempeña en la vida pública. El Tribunal de Justicia indica que las circunstancias del litigio principal no parecen justificar una desviación de la regla general expuesta, refiriéndose al carácter sensible de la información de la que se trata y a los años que han pasado desde la publicación de la información, afirmando además que no parece que deba apreciarse un interés público en que dicha información esté a disposición de cualquier usuario de un motor de búsqueda. No obstante, la conclusión sobre este punto le corresponde al órgano jurisdiccional nacional que debe resolver el litigio principal[122].

> Resulta conveniente mencionar en este momento el informe 214/2010 de la AEPD[123], en el cual esta agencia manifiesta que el problema que surge en el supuesto que se le plantea viene dado por la concurrencia de dos hechos: la publicación de la notificación en la edición electrónica de un Diario Oficial y su indexación por el servicio de búsqueda en Internet. En este contexto, la AEPD reproduce su Resolución de Tutela TD/01589/2008 y determina que cabe ejercer un derecho de oposición contra el propietario del motor de búsqueda, el cual debe adoptar "las medidas necesarias para retirar los datos de su índice e imposibilitar el acceso posterior a los mismos". Al hilo de la anterior resolución de la AEPD, SIMÓN CASTELLANO ponía de manifiesto que cuando la información publicada en la red es ilegítima y no ha de ampararse en la libertad de información, el afectado tiene a su disposición los derechos de acceso, cancelación y rectificación "frente al titular o responsable de la web que lo publicó". Pero cuando la información es legítima y no puede solicitar la desaparición de la misma, el interesado dispone de un derecho de oposición contra el titular del motor de búsqueda si la información carece de

[121] Sentencia *Google Spain y Google*, apartados 92 a 96.

[122] Sentencia *Google Spain y Google*, apartados 96 a 99.

[123] Este informe puede consultarse a través del enlace http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/derecho_acceso_rectificacion_cancelacion_oposicion/common/pdfs/2010-0214_Publicaci-oo-n-en-Diarios-Oficiales-de-las-notificaciones-y-su-indexaci-oo-n-en-los-motores-de-b-uu-squeda-en-Internet.pdf (última consulta: 5 de junio de 2014).

> "relevancia pública actual"[124]. En este sentido, SIMÓN CASTELLANO constataba la cercanía entre el derecho al olvido y el derecho fundamental a la protección de datos personales, con quien compartiría sus principios inspiradores: el principio de consentimiento y el principio de finalidad. Por un lado, el interesado revoca su consentimiento sobre el acceso a lo que él mismo ha publicado o no lo presta al tercero que ha publicado información sobre él sin su permiso previo. Por otro, el mismo interesado se opone a que se continúe tratando una información que carece de relevancia en el presente, habiendo desaparecido el fin para el cual fue puesta a disposición de la sociedad[125].

Sin embargo, el Abogado General no está de acuerdo con la conclusión del Tribunal de Justicia sobre el derecho al olvido. Según aquél, los derechos de rectificación, supresión y bloqueo de datos reconocidos en la Directiva sobre protección de datos se refieren a datos personales que no cumplen con los requisitos que la Directiva impone para su tratamiento, en particular por el carácter incompleto o inexacto de los mismos. Al mismo tiempo, constata que la información que aparece en la página web fuente que el motor de búsqueda incluye entre sus resultados no es ni incompleta ni inexacta. También dice el Abogado General que en la ponderación de intereses en juego que imponen los derechos mencionados no han de tenerse en cuenta las preferencias subjetivas del interesado, concluyendo que los derechos de rectificación, supresión y bloqueo de datos que reconoce la Directiva sobre protección de datos no incluyen un derecho al olvido[126].

De igual modo, el Abogado General examina si cabe reconocer un derecho al olvido a partir del derecho al respeto de la vida privada y familiar reconocido en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea, siendo en este caso su conclusión igualmente negativa. A este respecto, el Abogado General dice que la búsqueda en Internet a través de los motores es una de las formas más importantes que tienen las personas de ejercer su derecho a recibir información, en la que debe incluirse la información relacionada con la condición personal de un tercero aunque pertenezca a su vida privada. Si los motores de búsqueda se viesen obligados a omitir resultados de búsqueda, los usuarios del motor no recibirían información veraz y al mismo tiempo se atacaría la libertad de expresión de los editores de las páginas web fuente[127]. De esta forma, los proveedores de motores de búsqueda pueden cumplir una función importante cuando los órganos nacionales competentes ordenen bloquear el acceso a una página web cuyos contenidos son ilegales, pero ni de la Directiva sobre protección de datos ni de la Carta de los Derechos Fundamentales de la Unión Europea se desprende un derecho generalizado al olvido[128]. Mi opinión personal coincide con la expresada por el Abogado General

---

[124] SIMÓN CASTELLANO (2011, pp. 403-406).

[125] SIMÓN CASTELLANO (2011, pp. 398-400).

[126] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, puntos 104 a 111.

[127] Para ROSEN (2012, p. 88), el derecho al olvido representa la mayor amenaza que tendrá la libertad de expresión en la próxima década. La amenaza se proyecta en mayor sentido, quizás, sobre el derecho a la información, en la medida en que a las personas se les ofrecerá una versión sesgada de la realidad, desprovista de las cuestiones negativas que afecten a una persona. Por eso, posiblemente el derecho al olvido que se reconoce en la sentencia *Google Spain y Google* pueda describirse de forma más precisa como un "derecho a ser editado". En este sentido, véanse también BOTANA GARCÍA / OVEJERO PUENTE (2014, pp. 12, 18 y 19), quienes aluden a un "derecho a no ser buscado" y exponen los problemas que este derecho presenta para la credibilidad de los buscadores, y BOTANA GARCÍA (2014, p. 19), que comenta que algunas personas podrán "acomodar" las informaciones que sobre ellas están disponibles en Internet.

[128] Conclusiones del Abogado General en la sentencia *Google Spain y Google*, puntos 126 a 137.

en sus conclusiones en la sentencia *Google Spain y Google*.

Tras un primer momento en el que Google mostró su desacuerdo con la sentencia del Tribunal de Justicia, la reacción del gestor del motor de búsqueda ha sido crear un formulario a través del cual los internautas pueden ejercitar los derechos reconocidos por el Tribunal de Justicia en la sentencia *Google Spain y Google*, solicitando que el buscador no ofrezca un determinado enlace entre los resultados de la búsqueda[129]. El internauta que desee cumplimentar el formulario debe proporcionar la URL de cada enlace que se solicita que se retire, así como explicar los motivos por los que la página web fuente ha publicado la información en cuestión y las razones por las que el solicitante considera que la información aparecida en los resultados de búsqueda es irrelevante, obsoleta o inadecuada. Otro elemento que debe aportar es una copia de un documento que permita verificar la identidad del solicitante o, si el solicitante actúa en nombre de otra persona, la autorización correspondiente y el documento de identidad con una foto del representado. Se permite la ocultación de ciertos datos del documento siempre que no imposibilite la identificación referida. Asimismo, Google indica en el formulario que la información aportada sólo se utilizará para comprobar la autenticidad de la solicitud, y que borrará la copia del documento de identificación en el plazo de un mes desde que la solicitud de retirada quede cerrada.

Lógicamente, la puesta a disposición de los internautas de un formulario no significa que todas las solicitudes vayan a ser aceptadas, por lo que con relación a dicho formulario se suscitan ciertas dudas. Así, cabe preguntarse si Google tiene capacidad efectiva para evaluar con la exhaustividad adecuada cada una de las solicitudes que reciba. En este sentido, hay que tener en cuenta que el artículo 32.2 del RPDP prevé que el responsable del fichero debe resolver sobre la solicitud de rectificación o cancelación de datos en el plazo máximo de diez días a contar desde la recepción de la solicitud. De no hacerlo, el interesado podrá reclamar ante la AEPD. Tampoco son conocidos los criterios que seguirá el gestor del motor de búsqueda para ponderar los derechos de las personas identificadas en las páginas web fuente y el derecho a conocer y distribuir información, o cómo determinará Google si la información contenida en la web fuente es obsoleta o inadecuada[130]. Otra cuestión que podría plantearse es qué sucederá si el motor de búsqueda arroja un enlace que alguien pretende que se elimine, el cual es al mismo tiempo favorable para otra persona. Esta persona podría esgrimir que la supresión de un enlace en los motores de búsqueda impide que el resto de la sociedad conozca información favorable relativa a él, mientras que Google podría tener este hecho en cuenta en la ponderación de intereses que realice.

Por otra parte, del formulario *online* dispuesto por Google resulta que, de aceptar una solicitud

---

[129] Puede accederse al formulario mencionado a través del siguiente enlace: https://support.google.com/legal/contact/lr_eudpa?product=websearch (última consulta: 5 de junio de 2014). En dicho formulario se indica: "Google evaluará cada solicitud de forma individual e intentará buscar un equilibrio entre los derechos de privacidad de los usuarios y el derecho del público a conocer y distribuir información. Al evaluar tu solicitud, Google examinará si los resultados incluyen información obsoleta sobre ti, así como si existe interés público por esa información".

[130] Hay que mencionar la posibilidad indicada por ROSEN (2012, pp. 90 y 91), a la que también se alude en el punto 133 de las conclusiones del Abogado General en la sentencia *Google Spain y Google*, de que en los casos ambiguos el gestor de un motor de búsqueda opte por borrar los datos, lo cual podría suponer la eliminación de mucha información sin haber motivo suficiente para ello.

> presentada, el enlace en cuestión no se mostrará en ningún momento en el buscador, sean cuales sean los términos de búsqueda utilizados. Esto es más importante de lo que a primera vista pudiera parecer, porque el Tribunal de Justicia se refiere en diversas ocasiones en la sentencia *Google Spain y Google* a las búsquedas efectuadas mediante la introducción en el motor de búsqueda del nombre de una persona física[131], lo cual podría ser utilizado por los gestores de dichos motores para limitar el alcance de la sentencia a aquellos casos en los cuales los resultados aparecen sólo cuando entre los términos de búsqueda figura el nombre completo de una persona. Dicho de otro modo, las sucesivas alusiones al nombre de la persona que hace el Tribunal de Justicia de la Unión Europea podrían ser empleadas por los gestores de los motores de búsqueda para sostener que no están obligados a eliminar ninguno de los resultados arrojados por el motor cuando éstos se muestren en una búsqueda en la cual entre los términos introducidos en el motor sólo figure el nombre de pila de la persona o uno de los apellidos en combinación con otras palabras. A este respecto, el Grupo del artículo 29 ha puesto de manifiesto que, no habiendo precisado el Tribunal de Justicia qué debe entenderse por "nombre", el derecho reconocido en la sentencia *Google Spain y Google* se aplica también en el caso de búsquedas efectuadas introduciendo diferentes versiones del mismo o los apellidos, pero, además, indica que las autoridades nacionales en materia de protección de datos considerarán "términos de búsqueda relevantes" los pseudónimos y apodos, siempre que el interesado pueda establecer que éstos se encuentran ligados a su identidad[132].

En cualquier caso, en mi opinión, la mejor ponderación de los derechos en juego en los casos en los que la publicación de la información se hace de manera lícita es la que se desprende del comportamiento de los propios internautas, debido a la naturaleza de Internet y a sus efectos en la sociedad. Y es que Internet es una de las mejores herramientas para apreciar la existencia o no de un interés público sobre una información y, aunque pueda sonar paradójico, para garantizar el olvido de informaciones que verdaderamente sean obsoletas o irrelevantes. Cuando se alude a que Internet es un mecanismo clave para conservar información a lo largo del tiempo, se obvian diversos efectos consustanciales a este aumento de capacidad de preservar información. La capacidad del ser humano para retener información es limitada y de hecho se ve superada con mucha amplitud por el volumen de información al que se accede. Por primera vez en la Historia, el ser humano dispone de más información de la que necesita y, probablemente, de la que puede absorber. Es decir, las personas sólo retienen una mínima parte de la información que en algún momento llegan a conocer, siendo esta proporción incluso menor si se compara con el volumen de información con el que han tenido contacto. No cabe duda de que los individuos del siglo XXI se enfrentan a un problema de sobrecarga de información (*overload*) que les obliga a seleccionar tanto la información que van a manejar como la que conservarán.

Al mismo tiempo, hoy en día las personas se molestan menos en retener la información, porque el coste de recuperarla cuando sea necesaria es muy reducido, siendo Internet clave en este proceso. Las personas necesitan conservar fácilmente accesibles menos datos, pues esto ya viene dado por Internet. Cuando precisen una determinada información la buscarán, y, una vez utilizada, la borrarán de su memoria hasta la próxima ocasión en la que la necesiten, salvo que el uso de dicha información sea tan continuado que les sea más eficiente recordarla. Por tanto, considero que Internet y los buscadores son una fuente magnífica de conservación de información, pero el empleo de la misma y la consciencia sobre ella tienen lugar sobre todo a

[131] Sentencia *Google Spain y Google*, apartados 36, 37, 62, 80, 82, 87, 88, 89, 94, 96, 97, 98 y 99.

[132] Informe *Guidelines*, punto 21 y p. 13, criterio 1.

corto plazo y en cuanto a datos que no es necesario utilizar repetidamente en la vida cotidiana.

> Por ejemplo, hace no muchos años, ante la necesidad de tener que dar el número de teléfono de una persona a un tercero, podía recordarse el número de memoria y decirlo al momento, o acudir a una agenda telefónica en papel. Como no existían los teléfonos móviles, la cantidad de números de teléfono a los que se recurría era mucho menor que ahora, y por tanto el coste de memorizar los números compensaba el esfuerzo de buscar en la agenda cada vez que se necesitaba. Hoy en día tenemos contacto con muchísimas más personas, de las cuales casi todas tienen un número de teléfono personal, si no varios. El coste de obtener el número de contacto de alguien es muy reducido porque tanto nuestro propio teléfono móvil como en ciertos casos Internet nos lo facilitan. Así, los incentivos para recordar un número de teléfono son mucho menores hoy de lo que lo eran antes. Sin perjuicio de que existan ciertos números que puedan recordarse de memoria, como pueden ser los de los familiares más cercanos, en la mayoría de casos se incorpora el número a la agenda del teléfono móvil, se olvida y se consulta cuando sea preciso, olvidándolo nuevamente hasta que vuelva a ser necesario obtener el número en cuestión.

La sentencia *Google Spain y Google* ha recibido, como es lógico, bastante atención en los medios de comunicación. El nombre de la persona que inició el litigio ha sido mencionado y su imagen ha aparecido en muchos de ellos, de modo que los ciudadanos han tenido contacto con ambas fuentes de información. Sin embargo, cabe preguntarse cuántas personas de las que han escuchado o leído el nombre y visto la imagen del demandante en el litigio principal los recordarán dentro de unos meses. En mi opinión, serán muy pocas. En definitiva, creo que una vez que los datos aparecen publicados en una página web de manera lícita, el hecho de que un motor de búsqueda ofrezca esa página web entre sus resultados sólo es relevante si el usuario del motor tiene un verdadero interés en conocer dicha información, mientras que si la utilidad que el usuario del motor obtiene de la información no llega a niveles elevados tal información caerá en el olvido.

En conclusión, en situaciones como las del litigio principal del que deriva la sentencia *Google Spain y Google*, la propia naturaleza de Internet, la sobrecarga de información que caracteriza a la sociedad de nuestro tiempo y la limitada capacidad de atención y memoria del ser humano hacen que cuando una persona retiene una información comprometedora para otra se deba a que su interés en ello es alto, hasta el punto de que ese interés probablemente supere el de la persona a la que se refiere la información. Si el interés de la sociedad es realmente bajo, no hace falta proclamar la prevalencia de los derechos de la persona identificada por los datos personales, ya que la propia sociedad olvidará la información con su desinterés por acceder a ella. Un razonamiento como éste podría ser utilizado por Google para denegar un número amplio de las solicitudes que recibe a través del formulario online, pero también por los órganos nacionales con capacidad para ordenar la retirada de los resultados de los motores de búsqueda. De esta manera, dichos órganos nacionales tenderían a no imponer la eliminación del buscador de los enlaces controvertidos más que en un número reducido de casos, lo cual sería una solución mucho más respetuosa con la libertad de información que a la que aparentemente conduce la sentencia del Tribunal de Justicia de la Unión Europea que se toma como referencia en el presente trabajo.

7. Tabla de jurisprudencia citada

Sentencias del Tribunal de Justicia de la Unión Europea

Sala y Fecha	*Asunto*	*Referencia Aranzadi*	*Partes*
Gran Sala, 13.5.2014	C-131/12	TJCE 2014, 85	*Google Spain, S.L. y Google Inc. c. Agencia Española de Protección de Datos [AEPD] y Mario Costeja González*
Sala Pleno (TJCE), 6.11.2003	C-101/01	TJCE 2003, 368	*Procedimiento penal entablado contra Bodil Lindqvist*
Sala Pleno (TJCE), 25.7.1991	C-221/89	TJCE 1991, 244	*The Queen c. Secretary of State for Transport [Ministro de Transportes] ex parte: Factortame Ltd. y otros*

Sentencias del Tribunal Constitucional español

Sala y Fecha	*Referencia Aranzadi*	*Magistrado Ponente*
Sala Pleno, 30.11.2000	RTC 2000, 292	*Julio Diego González Campos*
Sala Pleno, 30.11.2000	RTC 2000, 290	*Julio Diego González Campos*
Sala 1ª, 20.7.1993	RTC 1993, 254	*Fernando García-Mon y González-Regueral*

8. Bibliografía

Javier Aparicio SALOM (2009), *Estudio sobre la Ley orgánica de protección de datos de carácter personal*, 3ª edición, Aranzadi, Cizur Menor.

Agustín E. DE ASÍS ROIG (2002), "Protección de datos y derecho de las telecomunicaciones", en Javier CREMADES (Dir.), *Régimen jurídico de Internet*, La Ley, Las Rozas (Madrid), pp. 201-228.

John BATTELLE (2006), *Buscar. Cómo Google y sus rivales han revolucionado los mercados y transformado nuestra cultura*, Ediciones Urano, Barcelona.

Pierre-Jean BENGHOZI (2008), "Les moteurs de recherche: trou noir de la régulation?", en Alain STROWEL / Jean-Paul TRIAILLE (Dir.), *Google et les nouveaux services en ligne. Impact sur l'économie du contenu et questions de propriété intellectuelle*, Larcier, Bruselas, pp. 83-101.

Gema Alejandra BOTANA GARCÍA (2014), "Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea a propósito de la cuestión prejudicial planteada por la Audiencia Nacional en el Caso Google", *Práctica de Derecho de Daños*, nº 120, Sección Informe de Jurisprudencia, Tercer trimestre de 2014, Editorial La Ley (La Ley 3941/2014).

Gema Alejandra BOTANA GARCÍA / Ana Mª OVEJERO PUENTE (2014), "Claves de la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 en la cuestión prejudicial planteada en el caso Google", *Actualidad Civil,* 9 de junio de 2014, Editorial La Ley (La Ley 3951/2014).

Susan CRAWFORD (1983), "The Origin and Development of a Concept: The Information Society", *Bulletin of the Medical Library Association*, Vol. 71, nº 4, pp. 380-385.

Cynthia DWORK / Deirdre K. MULLIGAN (2013), "It's Not Privacy, and It's Not Fair", *Stanford Law Review Online*, Vol. 66, Symposium Issue, pp. 35-40.

Damien GERADIN / Monika KUSCHEWSKY (2013), "Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue", 12 de febrero de 2013 (http://ssrn.com/abstract=2216088).

María del Carmen GUERRERO PICÓ (2006), *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*, Thomson-Civitas, Cizur Menor.

Woodrow HARTZOG / Evan SELINGER (2013), "Big Data in Small Hands", *Stanford Law Review Online*, Vol. 66, Symposium Issue, pp. 81-88.

José Miguel HERNÁNDEZ LÓPEZ (2013), *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*, Aranzadi, Cizur Menor.

Rosalie LETTERON (1996), "Le droit à l'oubli", *Revue du Droit Public et de la Science Politique en France et à L'Étranger*, nº 2, 1996, pp. 385-424.

Ian J. LLOYD (2014), *Information Technology Law*, 7ª edición, Oxford University Press, Oxford.

Pedro Alberto DE MIGUEL ASENSIO (2014), "El tratamiento de datos personales por buscadores de Internet tras la sentencia Google Spain del Tribunal de Justicia", *La Ley Unión Europea*, nº 17, pp. 5-10.

--- (2011), *Derecho privado de Internet*, 4ª edición, Aranzadi, Cizur Menor.

Joaquín MUÑOZ (2014), "El llamado «derecho al olvido» y la responsabilidad de los buscadores. Comentario a la sentencia del TJUE de 13 de mayo 2014", *La Ley*, nº 8317, 23 de mayo de 2014.

José Luis PIÑAR MAÑAS (2010), "Comentario al artículo 3", en Antonio TRONCOSO REIGADA (Dir.), *Comentario a la ley Orgánica de Protección de datos de carácter personal*, Civitas, Cizur Menor, pp. 184-213.

Chris REED / John ANGEL (Eds.) (2007), *Computer Law. The Law and Regulation of Information Technology*, 6ª edición, Oxford University Press, Oxford.

Jeffrey ROSEN (2012), "The Right to Be Forgotten", *Stanford Law Review Online*, Vol. 64, Symposium Issue, pp. 88-92.

Diana SANCHO VILLA (2010), "Comentario al artículo 2.1", en Antonio TRONCOSO REIGADA (Dir.), *Comentario a la ley Orgánica de Protección de datos de carácter personal*, Civitas, Cizur Menor, pp. 98-115.

Giovanni SARTOR / Mario VIOLA DE AZEVEDO CUNHA (2010), "The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents", *International Journal of Law and Information Technology*, Vol. 18, nº 4, pp. 356-378.

María Mercedes SERRANO PÉREZ (2010), "Comentario a los artículos 16 y 17", en Antonio TRONCOSO REIGADA (Dir.), *Comentario a la ley Orgánica de Protección de datos de carácter personal*, Civitas, Cizur Menor, pp. 1219-1240.

Pere SIMÓN CASTELLANO (2011), "El régimen constitucional del derecho al olvido en Internet", en Agustí CERRILLO-I-MARTÍNEZ *et al*. (Coords.), *Net Neutrality and other challenges for the future of the Internet*, UOC-Huygens, Barcelona, pp. 391-406.

Bart VAN DER SLOOT / Frederik Zuiderveen BORGESIUS (2012), "Google and Personal Data Protection", en Aurelio LÓPEZ-TARRUELLA (Ed.), *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, Asser Press, La Haya, pp. 75-111.

Daniel J. SOLOVE (2007) "«I've Got Nothing to Hide» and Other Misunderstandings of Privacy", *San Diego Law Review*, Vol. 44, pp. 745-772.

--- (2006), "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, Vol. 154, nº 3, pp. 477-560.

Omer TENE (2008), "What Google Knows: Privacy and Internet Search Engines", *Utah Law Review*, Vol. 2008, nº 4, pp. 1433-1492.

Antonio TRONCOSO REIGADA (2010), *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, Valencia.

Mònica VILASAU SOLANA (2014), "El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido (análisis de la STJUE de 13 de mayo de 2014)", *IDP. Revista de Internet, Derecho y Política*, nº 18, pp. 16-32.

Ignacio VILLAVERDE MENÉNDEZ (2010), "Comentario al artículo 6", en Antonio TRONCOSO REIGADA (Dir.), *Comentario a la ley Orgánica de Protección de datos de carácter personal*, Civitas, Cizur Menor, pp. 494-502.

Samuel D. WARREN / Louis D. BRANDEIS (1890), "The Right to Privacy", *Harvard Law Review*, Vol. IV, nº 5, 15 de diciembre de 1890, pp. 193-220.

Frank WEBSTER (1995), *Theories of the information socie*ty, Routledge, Londres.