EL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA COMO JUEZ GARANTE DE LA PRIVACIDAD EN INTERNET[1]

ARTEMI RALLO LOMBARTE
Catedrático de Derecho Constitucional
Universidad Jaume I

SUMARIO

I. INTRODUCCIÓN

El centenario debate en torno a los perfiles dogmáticos del derecho a la intimidad (*privacy*, en su acepción anglosajona; *vida privada*, en la tradición continental europea) se ha visto en gran medida superado durante las últimas décadas por la emergencia del derecho a la protección de datos. La fuerza expansiva de los perfiles normativos de este novísimo derecho ha evidenciado una capacidad protectora del *right to be alone* frente a las amenazas provenientes de la evolución tecnológica que permite dar por superado el debate anterior para reafirmar que la protección, hoy, de la privacidad tiene sus principales manifestaciones en la garantía efectiva del derecho a la protección de datos frente al fenómeno

1 Este trabajo ha sido elaborado en el marco del proyecto de investigación financiado por el Ministerio de Economía y Competitividad (DER2015-63635-R) sobre «El impacto del nuevo Reglamento Europeo de Protección de Datos: análisis nacional y comparado» del que el autor fue, inicialmente, investigador principal. Una primera versión fue presentada el 23 de septiembre de 2016 en las IX Jornadas italo-hispano-brasileñas de Derecho Constitucional organizadas en el Centro de Estudios Políticos y Constitucionales por el Área de Derecho Constitucional de la Universidad Carlos III bajo la dirección del prof. Aguiar. Por ello, verá la luz, también, en el libro colectivo que recoge las ponencias presentadas a las mencionadas Jornadas.

tecnológico que mayor impacto tiene en los usos sociales: telefonía móvil, Internet y redes sociales[2].

El origen, evolución y consolidación del derecho a la protección de datos personales tiene una inequívoca impronta europea jalonada por cuatro estadios normativos perfectamente identificables:

1. El Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal.
2. La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
3. El art. 8 de la Carta de Derechos Fundamentales de la Unión Europea al que el Tratado de Lisboa otorgó fuerza jurídica a partir de 2009.
4. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en vigor a partir de mayo de 2018).

Sin embargo, el impacto mundial de esta normativa originariamente europea tiene una innegable doble manifestación: por un lado, en la proliferación de regímenes normativos de protección de los datos personales en el resto de los continentes; y, por otro, en la obligada adecuación de los servicios tecnológicos globales —independientemente de su origen geográfico— a la normativa europea de protección de este derecho fundamental y, en concreto, a la jurisdicción garante de su efectividad, esto es, al Tribunal de Justicia de la Unión Europea (TJUE). Por ello, hay que afirmar que el TJUE se ha convertido en un auténtico juez garante de la privacidad ante la evolución tecnológica global.

El siguiente análisis de la jurisprudencia del TJUE evidenciará el impacto allende las fronteras europeas de la normativa europea de protección de datos. La inevitable fuerza expansiva extraterritorial de esta jurisprudencia resultará especialmente evidente en tres renombradas sentencias recientes del TJUE en las que centraremos nuestro estudio: Caso Digital Rights (Directiva conservación de datos), Caso Google (derecho al olvido) y Caso Facebook (Safe Harbour). Estas

2 Resulta relevante reproducir las siguientes afirmaciones contenidas en la STJUE de 8 de abril de 2014 (*Caso 293/12 y 594/12 Digital Rights Ireland y Seitlinger y otros vs, Irish Data Protection Comissioner*) que anuló la Directiva 2006/24/CE sobre conservación de datos de comunicaciones electrónicas: «Para demostrar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada, carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia» (punto 33); «la protección de los datos de carácter personal, que resulta de la obligación expresa establecida en el artículo 8.1 CDFUE, tiene una importancia especial para el derecho al respeto de la vida privada consagrado en el artículo 7 de ésta» (punto 53).

tres recientes sentencias del TJUE marcan un hito en la evolución de la protección de los datos personales frente a la globalización tecnológica por su impacto mundial, esto es, por la expansión de los estándares europeos de protección al resto de latitudes del planeta.

Esta jurisprudencia ilustra sobre los enormes riesgos potenciales para la privacidad del individuo que derivan tanto del uso de servicios y dispositivos tecnológicos (telefonía móvil, Internet y redes sociales) en los que se almacena abundante información personal —que, en la terminología tradicional, no cabría calificar necesariamente como íntima o sensible— sin que el principio de territorialidad estatal pueda satisfacer las garantías necesarias para evitar la lesión en la intimidad individual.

II. ANTECEDENTES

El análisis de los antecedentes jurisprudenciales del TJUE aplicativos de la Directiva 95/46 de protección de datos[3] constituye un acervo indispensable para pergeñar el impacto de dicha normativa sobre los servicios tecnológicos globales y, en particular, sobre Internet.

1. La Directiva de Protección de Datos como marco normativo referencial para la protección de la privacidad en Internet

El *Caso Lindqvist*[4] (C-101/01, 6-11-2003) constituye el caso de referencia en el que el TJUE confirmó la plena aplicabilidad de la Directiva de protección de datos a Internet en los siguientes términos:

3 Una aproximación a los primeros pronunciamientos jurisprudenciales del TJUE en Arenas Ramiro, M.: «El derecho a la protección de datos personales en la jurisprudencia del TJCE», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, vol. 4, 2006, pp. 95 a 119. Más reciente, Rodríguez-Izquierdo Serrano, M.: «El Tribunal de Justicia y los derechos en la sociedad de la información: «Privacidad y protección de datos frente a libertades informativas», *Revista de Derecho Constitucional Europeo*, n.º 24, 1015 (http://www.ugr.es/~redce/REDCE24/articulos/10_RODRIGUEZ_IZQUIERDO.htm).

4 En este asunto se sustancian varias cuestiones prejudiciales sobre la Directiva 95/46 suscitadas en el marco de un proceso penal seguido contra la Sra. Lindqvist, acusada de haber infringido la normativa sueca relativa a la protección de datos personales al publicar en su sitio Internet datos personales de varias personas que, como ella, colaboraban voluntariamente con una parroquia de la Iglesia protestante de Suecia. La Sra. Lindqvist era catequista en la parroquia de Alseda (Suecia) y, tras un curso de informática, creó, desde su domicilio y con su ordenador personal, varias páginas web para que los feligreses de la parroquia obtuvieran fácilmente información sobre la preparación de su confirmación. Dichas páginas web contenían información sobre la Sra. Lindqvist y dieciocho de sus compañeros de parroquia: nombre completo o de pila, comentarios humorísticos, aficiones, situación familiar, número de teléfono, baja por enfermedad en un pie de una compañera, etc. La Sra. Lindqvist fue condenada a una multa (que apeló) por tratamiento automatizado de datos (incluso sensibles) sin autorización, por no comunicarlo previamente a la Autoridad de Protección de datos y por transferencia internacional de datos a países terceros sin autorización.

1. hacer referencia en una página web a diversas personas e identificarlas por su nombre o por otros medios, como su número de teléfono, condiciones de trabajo o aficiones, constituye un *tratamiento total o parcialmente automatizado* de datos personales (art. 3.1 de la Directiva 95/46);
2. un tratamiento de datos consistente en difundirlos por Internet haciéndolos accesibles a un grupo indeterminado de personas ni puede considerarse actividad exclusivamente *personal o doméstica* (circunscrita a la vida privada o familiar) ni, en consecuencia, considerarse exceptuada de la aplicación de la Directiva 95/46 por su art. 3.2.

Además, se trata de la primera ocasión en que el TJUE evaluó el impacto extraterritorial —y, en consecuencia. global— de la Directiva europea a los servicios de Internet al negar que nos halláramos en este supuesto ante una *transferencia internacional de datos*[5] —a pesar de que una persona difundiera datos desde una página web de un Estado miembro que fueran almacenados en un servidor del mismo Estado o de otro Estado miembro, y resultando dichos datos accesibles a cualquier persona conectada a Internet aunque se encontrara en países terceros—. El TJUE sostuvo:

1. que, teniendo en cuenta el estado de desarrollo de Internet en el momento de la elaboración de la Directiva 95/46 y la inexistencia de criterios aplicables al uso de Internet en materia de transferencias internacionales, no cabía presumir que la *voluntad del legislador comunitario* fuera incluir en el concepto de «transferencia a un país tercero de datos» la difusión de datos en una página web por parte de un particular —aunque dichos datos resultaran accesibles a personas de países terceros—;
2. que una interpretación contraria implicaría que cada vez que se publicaran datos personales en una página web, los Estados miembros estarían obligados a impedir su difusión en Internet cuando se detectara que un solo país tercero no garantiza un nivel de protección adecuado.

El *Caso Lindqvist* también permitió al TJUE contrastar si la protección de datos personales en Internet podía conculcar otros derechos fundamentales como la libertad de expresión. Para el TJUE,

1. los derechos fundamentales revisten una *importancia especial* por lo que es necesario, ponderar la libertad de expresión y la intimidad de las personas cuyos datos se publican en Internet;

5 Una posición crítica mantuvo POULLET, Y.: «Flujos de datos transfronterizos y extraterritorialidad: la postura europea», *Revista Española de Protección de Datos*, n.º 1, julio-diciembre, 2006, pp. 99 y ss.

2. esta ponderación correspondería a las *autoridades nacionales* al interpretar su Derecho nacional de conformidad con la Directiva 95/46 procurando evitar conflictos con los derechos fundamentales tutelados por el ordenamiento jurídico comunitario o con los otros principios generales del Derecho comunitario como el principio de proporcionalidad;
3. la tutela de la intimidad requiere sanciones eficaces pero que respeten el *principio de proporcionalidad* al ponderar circunstancias como la duración de la infracción o la importancia de los datos difundidos. Esto es, el TJUE negó que la Directiva 95/46 contraviniese la libertad de expresión u otros derechos y libertades y concluyó inequívocamente lo que sigue: «incumbe a las autoridades y a los órganos jurisdiccionales nacionales encargados de aplicar la normativa nacional que adapta el Derecho interno a la Directiva 95/46 garantizar el *justo equilibrio entre los derechos e intereses* en juego, incluidos los derechos fundamentales tutelados por el ordenamiento jurídico comunitario.

Tres *ideas/fuerza* merecen ser destacadas en este precursor pronunciamiento jurisprudencial dictado hace poco más de una década y ya en plena efervescencia de Internet:

1. Toda publicación de datos en Internet constituye un tratamiento automatizado que impacta inevitablemente en el derecho a la protección de datos.
2. Los conflictos que suscite la protección de datos con otras libertades y derechos merecen un ponderado juicio por parte de las autoridades nacionales que intente evitar el sacrificio de cualquiera de ellos y, en todo caso, verifique el principio de proporcionalidad atendiendo a todas las circunstancias concurrentes en el caso concreto.
3. Debe evitarse una irrazonable aplicación de la Directiva (por ejemplo, asimilando la difusión de datos en internet a una transferencia internacional) que, sin más, desnaturalizaría su existencia al imponer una insoportable censura previa sobre sus contenidos que supondría una desproporcionada interpretación de la Directiva.

2. El justo equilibrio en la protección de datos y los derechos de autor en Internet

El *Caso Promusicae* (C-275/06, 29-1-2008)[6] se ocupó centralmente de la protección de datos y del respeto a la intimidad en Internet y sus conflictos con los derechos de autor y a la propiedad intelectual.

6 En el mismo sentido, el *Caso Tele2* (C-557/07), Auto del TJUE de 19 de febrero de 2009 y el *Caso SABAM* (C-70/2010, STJUE de 24 de noviembre de 2011).

El *Caso Promusicae* tiene su origen en la cuestión prejudicial planteada por el Juzgado de lo Mercantil n.º 5 de Madrid en el marco de un litigio entre la asociación gestora de derechos de propiedad intelectual Productores de Música de España (Promusicae) y Telefónica de España por la negativa de ésta a comunicar a Promusicae, datos personales relativos al uso de Internet a través de conexiones suministradas por Telefónica. Promusicae había solicitado que se ordenase a Telefónica revelar la identidad y la dirección de personas a las que ésta prestaba servicio de acceso a Internet y de las que se conocía su dirección IP y la fecha y hora de conexión. Según Promusicae, estas personas utilizaban un programa de intercambio de archivos («peer to peer» o «P2P») —permitiendo el acceso, en una carpeta compartida de su ordenador personal, a contenidos musicales y vulnerando derechos de propiedad intelectual— por lo que solicitaba dicha información para ejercitar acciones civiles. Sin embargo, Telefónica se oponía por entender que la comunicación de dichos datos sólo estaba autorizada para una investigación criminal o por razones de seguridad pública y defensa nacional: no en el marco de un procedimiento civil.

El TJUE entendió: (a) que las Directivas afectadas (2000/31, 2001/29, 2004/48 y 2002/58) *no* establecían *obligación explícita* a los Estados para imponer un deber de comunicar datos para proteger derechos de autor en un procedimiento civil; (b) pero que el Derecho Comunitario *sí* exigía que la adaptación nacional de las Directivas procurase un *justo equilibrio* entre derechos fundamentales; (c) y que las autoridades nacionales debían interpretar su Derecho nacional evitando conflictos con derechos fundamentales o demás principios generales del Derecho comunitario, como el de proporcionalidad.

En fin, el *Caso Promusicae* sustanciaba un conflicto entre el derecho a proteger datos personales vinculados al uso de Internet y el derecho a la propiedad intelectual. El TJUE evitó de plano un pronunciamiento que orientase hacia la prevalencia de una lectura del ordenamiento europeo favorable a uno u otro derecho fundamental y remitió a las autoridades nacionales una resolución ponderada y equilibrada que evitara el sacrificio de estos derechos aplicando el principio de proporcionalidad tanto en la transposición de las Directivas como en los actos aplicativos (administrativos o judiciales) del Derecho interno.

3. **El conflicto entre protección de la intimidad y acceso a información digitalizada**

El *Caso Markkinapörssi-Satamedia* (C-73/07, 16-12-2008) entra a resolver un litigio centrado en el conflicto entre el derecho a la protección de datos y el derecho a la información sobre datos personales fiscales difundidos onerosamente mediante mensajes de texto de telefonía móvil.

El *Caso Markkinapörssi-Satamedia* tiene su origen en la cuestión prejudicial planteada a raíz de un litigio existente en Finlandia entre la Comisión de protección de datos y las sociedades Markkinapörssi y Satamedia que recogían datos de

la administración fiscal finlandesa, publicaban extractos anuales en el periódico *Veropörssi* y los difundían, previo pago de dos Euros, mediante mensajes de texto de telefonía móvil.

Para el TJUE, la protección de la intimidad en lo que respecta al tratamiento de datos personales debe conciliarse con la *libertad de expresión* estableciendo los Estados excepciones o restricciones a la protección de datos y a la intimidad «con fines periodísticos o de expresión artística o literaria». Pero la *importancia* de la libertad de expresión en toda sociedad democrática obliga:

a) a interpretar *ampliamente* conceptos como el de 'periodismo';
b) y a establecer a las excepciones y restricciones a la protección de datos los «límites estrictamente necesarios» aplicados no sólo a las empresas de medios de comunicación, sino también a *toda persona que ejerza una actividad periodística*. La publicación de datos con ánimo de lucro no excluiría *a priori* que pudiera considerarse una actividad exclusivamente con fines periodísticos pues toda empresa persigue obtener un beneficio de su actividad y un cierto éxito comercial puede ser incluso la condición *sine qua non* para la subsistencia de un periodismo profesional. La evolución y multiplicación de medios de comunicación y de difusión de información obliga a considerar que el soporte en el que se transmiten los datos —clásico (papel o radio) o electrónico (Internet)— no es determinante para apreciar si estamos ante una actividad «con fines exclusivamente periodísticos».

Por todo ello, en el *Caso Markkinapörssi-Satamedia,* el TJUE entendió que la publicación de datos procedentes de documentos públicos según la legislación nacional, podía considerarse como actividad periodística cuando «su finalidad es divulgar al público información, opiniones o ideas, por cualquier medio de transmisión»; correspondiéndole su apreciación a la jurisdicción nacional competente.

4. **El alcance de la responsabilidad de los buscadores de Internet como «servicios neutros de referenciación»**

En el *Caso Google France vs Louis Vuitton* (C-236/08 y C-238/08, 23-3-2010)[7], el TJUE resolvió las cuestiones prejudiciales presentadas por la Corte de Casación de Francia en relación a los litigios existentes entre Google y Louis Vuitton relativos la presentación por los buscadores de Internet de enlaces promocionales sobre palabras clave correspondientes a marcas.

7 También, las SSTJUE de 8 de julio de 2010 (C-558/08, *Caso Primakabin*), de 12 de julio de 2011 (C-324/09, *Caso L'Oréal*), de 22 de septiembre de 2011 (C-323/09; *Caso Interflora*).

En 2003, Louis Vuitton comprobó, por un lado, que la introducción en el buscador de Google de las marcas de Vuitton daba lugar a la aparición, como «enlaces patrocinados/publicitarios», de enlaces a sitios en los que se comercializaban imitaciones de Vuitton y, por otro, que Google ofrecía la posibilidad de combinar las marcas Vuitton con expresiones como «imitación» y «copia». Vuitton demandó a Google por violar sus derechos de marca.

La Directiva 2000/31 establecía que los prestadores de servicios de la sociedad de la información consistentes en almacenar datos facilitados por el destinatario del servicio no eran responsables de los datos almacenados a petición del destinatario a menos que, tras llegar a su conocimiento la ilicitud, no actuasen con prontitud para retirar los datos o hacer que el acceso a ellos fuera imposible. El TJUE incluyó en el concepto *servicio de referenciación* a los *buscadores de Internet*, definiéndolos como «servicio prestado a distancia, mediante equipos electrónicos de tratamiento y almacenamiento de datos, a petición individual de un destinatario de servicios y normalmente a cambio de una remuneración»; y aplicándoles las exenciones de responsabilidad cuando su actividad tuviera naturaleza «meramente técnica, automática y pasiva», esto es, no tuviera «conocimiento ni control de la información transmitida o almacenada». En consecuencia, sólo si se tratara de una actividad *neutra*, cabría exonerarle de responsabilidad.

En concreto, en el *Caso Google France vs Louis Vuitton*, Google realizó un tratamiento de datos introducidos por los anunciantes que derivaba en la aparición en la pantalla de anuncios en condiciones que Google controlaba al determinar el orden de aparición en función de lo pagado por el anunciante. Sin embargo, para el TJUE la responsabilidad de Google no derivaría ni del carácter remunerado del servicio ni de la concordancia de la palabra clave seleccionada y del término de búsqueda introducido por un internauta; pero sí de la redacción del mensaje comercial que acompañaba al enlace promocional o de la selección de palabras clave.

En definitiva, el TJUE concluyó que la actividad del buscador Google genera responsabilidad cuando desempeñe un *papel activo* que pueda darle conocimiento o control de los datos almacenados. En caso contrario, su responsabilidad por los datos almacenados a petición de un anunciante sólo emergería si, tras tener conocimiento de su ilicitud, no actuara con prontitud para retirar los datos o hacer que el acceso a ellos fuera imposible.

5. **El enjuiciamiento de las lesiones de derechos en webs de Internet en el Estado donde el ciudadano tiene su *centro de intereses***

El *Caso Date Advertising vs. Olivier y Martínez* (C-509/09 y C-161-10, 25-10-2011) resulta de gran interés pues aborda la compleja cuestión de la jurisdicción nacional aplicable en los litigios vinculados a Internet.

Dos hermanos residentes en Alemania fueron condenados en 1993 a cadena perpetua por el asesinato de un actor y en 2008 obtuvieron la libertad condicional.

La sociedad eDate Advertising, radicada en Austria, gestionaba un portal de Internet en el que se informaba de sus nombres y del recurso de amparo interpuesto contra la condena ante el Tribunal Constitucional alemán. Uno de los hermanos presentó una demanda de cesación ante los tribunales alemanes contra eDate Advertising para que no informara sobre los hechos cometidos mencionando el nombre completo. La empresa negó la competencia de los tribunales alemanes pero la demanda fue estimada en sucesivas instancias judiciales alemanas.

El *Caso Date Advertising vs. Olivier y Martínez* planteaba el interrogante sobre si resultaba admisible la jurisdicción alemana para dirimir un litigio en el que un residente alemán había solicitado la retirada de informaciones personales de una página web de una empresa austríaca y, en su caso, si resultaba aplicable el Derecho alemán o el Derecho austriaco.

El art. 5.3 del Reglamento 44/2001 sobre competencia judicial y reconocimiento y ejecución de resoluciones judiciales en materia civil y mercantil establecía que la jurisdicción aplicable cuando se vindicase una lesión de los derechos de la personalidad producida por contenidos publicados en Internet sería el *lugar donde se hubiere producido o pudiere producirse el hecho dañoso*. Esta competencia especial, como excepción al principio de competencia judicial según el domicilio del demandado, se basaría en la estrecha conexión entre la controversia y el órgano jurisdiccional del lugar de los daños y buscaría una buena administración de la justicia y una sustanciación adecuada del proceso. En el *Caso Shevill* (C-68/93, STJUE de 7 de marzo de 1995) el TJUE había establecido que la difamación a través de un artículo de prensa difundido en varios Estados habilitaba a la víctima a entablar contra el editor una acción de reparación (1) bien ante los órganos judiciales del Estado del lugar de establecimiento del editor (2) bien ante los órganos judiciales de cada Estado en que la publicación hubiera sido difundida y en que la víctima alegare haber sufrido un ataque contra su reputación. Ahora bien, la dificultad de aplicación en el ámbito de Internet del criterio del lugar del daño utilizado en el *Caso Shevill* resultaba evidente: la publicación de contenidos en un sitio de Internet (a diferencia de un medio impreso) persigue la ubicuidad de contenidos que pueden ser consultados instantáneamente por un número indefinido de usuarios de Internet en todo el mundo. En consecuencia, el criterio de competencia según la difusión resultaba poco útil en Internet ya que el alcance de la difusión «es, en principio, universal».

De ahí que el TJUE juzgara necesario adaptar el criterio de competencia judicial partiendo de dos premisas:

a) el enorme impacto de los contenidos publicados en Internet sobre los *derechos de la personalidad* podría ser apreciado mejor por «el órgano jurisdiccional del lugar en el que la supuesta víctima tuviera su *centro de intereses*» —a fin de garantizar una buena administración de la justicia y la previsibilidad de las normas de competencia por parte de quien emite contenido lesivos en Internet—;
b) y, en general, los individuos tienen su *centro de intereses* en su *residencia habitual*.

En definitiva, atendiendo a la interpretación más favorable a los derechos del justiciable, el TJUE concluyó que la persona lesionada podría recurrir:

1. Ante los órganos judiciales del Estado del lugar de establecimiento del emisor de esos contenidos;
2. Ante los órganos judiciales del Estado donde esté su «centro de intereses»;
3. O ante los tribunales de cada Estado en cuyo territorio el contenido publicado en Internet hubiera sido accesible[8].

6. La justiciabilidad de la publicidad fraudulenta en los buscadores de Internet

El *Caso Wintersteiger* (C-523/10, 19-4-2012) se ocupó de un conflicto sobre competencia judicial en el litigio entre la empresa austriaca Wintersteiger y la alemana Products 4U Sondermaschinenbau en el que la primera pretendía que se prohibiese a la segunda utilizar la marca austriaca Wintersteiger como palabra clave en el buscador de Internet.

Si bien en el *Caso Date Advertising vs. Olivier y Martínez* el TJUE entendió que, cuando se alega una lesión de los derechos de la personalidad, el perjudicado por contenidos publicados en un sitio de Internet puede recurrir ante los órganos judiciales del Estado donde se halla su *centro de intereses*, en el *Caso Wintersteiger* el TJUE entendió que este criterio no servía para determinar la competencia judicial sobre vulneración de derechos de propiedad industrial siguiendo los siguientes argumentos:

1. Si bien la lesión de los derechos de la personalidad se extendería a todos los Estados miembros, la protección derivada del registro de una marca nacional se limita al territorio del Estado de registro y son los órganos judiciales del Estado de registro los que están en mejores condiciones para evaluar si se vulnera la marca nacional protegida —por ello, el TJUE entiende que a éstos corresponderá resolver el litigio causado por el uso por un anunciante de una palabra clave idéntica a otra marca en *el sitio de Internet de un motor de búsqueda que opera bajo un dominio nacional* de otro Estado—.
2. Tratándose de un lugar cierto e identificable, tanto para el demandante como para el demandado, facilitando en consecuencia la administración de la prueba y la sustanciación del procedimiento, el lugar de

8 El *Caso Date Advertising vs. Olivier y Martínez* sirvió al TJUE para resolver el interrogante sobre si resultaba aplicable al caso la legislación material alemana o la austriaca, esto es, la del lugar de residencia del recurrente o la del lugar del establecimiento de Internet concluyendo que no se garantizaría plenamente la libre circulación de esos servicios de comercio electrónico si los prestadores debieran cumplir, en el Estado miembro de acogida, requisitos más estrictos que los que les son exigibles en su Estado de *establecimiento*.

establecimiento del anunciante es el lugar donde se decide el desencadenamiento del proceso de exhibición del anuncio.

Por todo lo anterior, el TJUE concluyó que este tipo de litigios —en los que un anunciante usa una palabra clave idéntica a una marca en un buscador de Internet dominio nacional de primer nivel de otro Estado— podrán dirimirse tanto ante los órganos judiciales del Estado de registro de la marca como en los del Estado en los que esté establecido el anunciante.

III. CASO DIGITAL RIGHTS IRELAND — SEITLINGER Y OTROS (C-293/12 Y C-594/12, 8-4-14): LA ILICITUD DE LA DIRECTIVA 2006/24/CE DE CONSERVACIÓN DE DATOS DE COMUNICACIONES ELECTRÓNICAS

La STJUE de 8 de abril de 2014 (*Caso 293/12 y 594/12 Digital Rights Ireland y Seitlinger y otros vs, Irish Data Protection Comissioner*), siguiento las Conclusiones contenidas en el Dictamen del Abogado General, Cruz Villalón, anuló la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre conservación de datos de tráfico y localización de comunicaciones electrónicas que perseguía garantizar la disponibilidad de esos datos con fines de prevención, investigación, detección y enjuiciamiento de delitos graves —la delincuencia organizada y el terrorismo— y, a tal fin, obligaba a las compañías proveedoras de estos servicios a conservar los datos de tráfico y de localización y los necesarios para identificar al abonado o al usuario —pero no amparaba, sin embargo, la conservación del contenido de las comunicaciones—.

Para el TJUE, estos datos, considerados en su conjunto, podían proporcionar indicaciones muy precisas sobre la vida privada de las personas cuyos datos se conservasen, como los hábitos de la vida cotidiana, los lugares de residencia permanente o temporal, los desplazamientos diarios u otros, las actividades realizadas, las relaciones sociales y los medios sociales frecuentados. Por ello, el TJUE concluyó que la Directiva se inmiscuía de manera especialmente grave en los derechos fundamentales al respeto a la privacidad y a la protección de datos de carácter personal y podía generar en las personas afectadas el sentimiento de que su vida privada era objeto de una vigilancia constante.

El Tribunal Superior de Irlanda (a instancias de Digital Rights) y el Tribunal Constitucional de Austria (en el litigio promovido por los Seitlinger y otros) interpusieron sendas cuestiones prejudiciales ante el TJUE para examinar la adecuación de sus respectivas legislaciones nacionales que trasponían dicha Directiva y, a su vez, la de ésta a los derechos fundamentales a la privacidad y a la protección de datos consagrados en la Carta de los Derechos Fundamentales de la Unión Europea.

La Directiva 2006/24/CE fue la respuesta jurídica de las instituciones europeas a los atentados terroristas de Madrid (2004)[9] y Londres (2005): «Dado que la conservación de datos se ha acreditado como una herramienta de investigación necesaria y eficaz para aplicar la ley en diferentes Estados miembros, en particular en asuntos de gravedad como la delincuencia organizada y el terrorismo, es necesario garantizar que los datos conservados se pongan a disposición de las fuerzas y cuerpos de seguridad durante un determinado período de tiempo» (Considerando 9).

En síntesis, la Directiva 2006/24/CE disponía lo que sigue:

1. los proveedores de servicios de comunicaciones electrónicas estarían obligados a conservar,
2. por un período de tiempo no inferior a seis meses ni superior a dos años,
3. los datos de tráfico, localización e identificación de personas físicas y jurídicas,
4. proporcionada por el uso de la telefonía fija y móvil e Internet,
5. no el contenido de las comunicaciones,
6. con fines de investigación, detección y enjuiciamiento de delitos graves,
7. según los defina cada Estado[10].

9 Sendos análisis de la normativa española de transposición de esta Directiva en Rallo Lombarte, A.: «El terrorismo internacional y sus conflictos: Seguridad vs. privacidad», *Inteligencia y seguridad. Revista de análisis y prospectiva*, n.º 3, 2007-2008, pp. 113 a 131 y Cubero Marcos, J.I. y Aberasturi Gorriño, U.: «Protección de los datos personales en las comunicaciones electrónicas: especial referencia a la Ley 25/2007 sobre conservación de datos», *Revista Española de Protección de Datos*, n.º 83, 2008, pp. 175 a 197. Una visión más recinte en Serra Cristóbal, R.: «Los derechos fundamentales en la encrucijada de la lucha contra el terrorismo yihadista. Lo que el constitucionalismo y el Derecho de la Unión Europea pueden ofrecer en común», *XIV Congreso Asociación de Constitucionalistas de España*, 2016 (http://congresoace.deusto.es/wp-content/uploads/2016/01/ComunicacionMesa1RosarioSerra.pdf).

10 Una correcta comprensión del impacto de la Directiva 2006/24 lo ofrece el amplio catálogo de datos cuya conservación prescribe su art. 5: a) datos necesarios para rastrear e identificar el origen de una comunicación: 1) telefonía de red fija y a la telefonía móvil: i) el número de teléfono de llamada, ii) el nombre y la dirección del abonado o usuario registrado; 2) acceso a Internet, correo electrónico por Internet y telefonía por Internet: i) la identificación de usuario asignada, ii) la identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía, iii) el nombre y la dirección del abonado o del usuario registrado al que se le ha asignado una dirección de Protocolo Internet (IP), una identificación de usuario o un número de teléfono; b) datos necesarios para identificar el destino de una comunicación: 1) telefonía de red fija y a la telefonía móvil: i) números marcados de destino y el número al que se transfieren las llamadas, ii) nombres y las direcciones de los abonados o usuarios registrados; 2) correo electrónico por Internet y telefonía por Internet: i) identificación de usuario o número de teléfono del destinatario de una llamada telefónica por Internet, ii) nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación; c) datos necesarios para identificar fecha, hora y duración de una comunicación: 1) telefonía de red fija y telefonía móvil: fecha y hora del comienzo y fin de la comunicación, 2) acceso a Internet, correo electrónico por Internet y telefonía por Internet i) fecha y hora de la conexión y desconexión del servicio de acceso a Internet, basadas en un determinado huso horario, y la dirección del Protocolo Internet, ya sea dinámica o estática, y la identificación de usuario del abonado o del usuario registrado, ii) fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario; d) datos necesarios para identificar el tipo de comunicación: 1) telefonía de red fija y telefonía móvil: el servicio telefónico utilizado, 2) correo electrónico por Internet y telefonía por Internet: el servicio de Internet utilizado; e) datos necesarios para identificar el

1. Una *injerencia especialmente grave* en la privacidad

No es de extrañar, por lo tanto, que el TJUE empezase llamando la atención sobre la enorme trascendencia personal de la tipología de información que se conservaba al amparo de esta Directiva: «Estos datos, considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan» (punto 27).

De hecho, el TJUE advirtió que, aunque la Directiva 2006/24 prohibía conservar el contenido de las comunicaciones telefónicas o la información consultada a través de comunicaciones electrónicas, estas previsiones legales podrían «tener una incidencia en el uso por los abonados o usuarios registrados de los medios de comunicación a que se refiere esta Directiva y, en consecuencia, en el ejercicio por parte de éstos de su libertad de expresión, garantizada en el artículo 11 de la CDFUE» (punto 28).

En definitiva, la conservación de estos datos podría condicionar el ejercicio de la libertad de expresión y posibilitar una extraordinaria intromisión en la privacidad y, en consecuencia, la Directiva supondría *una injerencia especialmente grave* en los derechos fundamentales a la vida privada y a la protección de datos de carácter personal: «la injerencia resulta de gran magnitud y debe considerarse especialmente grave. Además, la circunstancia de que la conservación de los datos y su posterior utilización se efectúen sin que el abonado o el usuario registrado hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de *una vigilancia constante*» (punto 37).

2. Una *vigilancia constante*, indiscriminada y desproporcionada

En particular, el TJUE concluyó que esta injerencia en los derechos fundamentales estaba justificada (en razones de interés general como la lucha contra la

equipo de comunicación de los usuarios: 1) telefonía de red fija: números de teléfono de origen y destino, 2) telefonía móvil: i) números de teléfono de origen y destino, ii) identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada, iii) la identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada, iv) la IMSI de la parte que recibe la llamada, v) la IMEI de la parte que recibe la llamada, vi) en el caso de los servicios anónimos de pago por adelantado, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio; 3) acceso a Internet, correo electrónico por Internet y telefonía por Internet: i) número de teléfono de origen en caso de acceso mediante marcado de números, ii) línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación; f) datos necesarios para identificar la localización del equipo de comunicación móvil: 1) etiqueta de localización (identificador de celda) al comienzo de la comunicación, 2) datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

delincuencia grave y la seguridad pública) pero vulneraba el principio de proporcionalidad al tratarse de una injerencia en los derechos fundamentales no limitada a «lo estrictamente necesario» sino «de gran magnitud y especialmente grave» (punto 37).

a) La Directiva afectaba a toda la población —«aunque las personas cuyos datos se conservan no se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales … se aplica incluso a personas respecto de las que no existen indicios que sugieran que su comportamiento puede guardar relación, incluso indirecta o remota, con delitos graves …no establece ninguna excepción, por lo que se aplica también a personas cuyas comunicaciones están sujetas al secreto profesional» (punto 58)—, medios de comunicación electrónica y datos sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves;
b) La Directiva no establecía criterios objetivos —ni condiciones materiales o procesales— que garanticen el acceso a los datos sólo para perseguir delitos especialmente graves dejando a cada Estado la concreción del término «delitos graves» definidos por cada Estado miembro en su ordenamiento jurídico interno (punto 60).
c) La Directiva prescribía un período mínimo de conservación de seis meses y máximo de veinticuatro sin precisar criterios objetivos que diferencien ente categorías de datos (puntos 63 y 64). Además, la Directiva no garantizaba ni que los datos se conservasen en el territorio de la Unión Europea ni el control por una autoridad independiente (punto 68).

IV. CASO GOOGLE VERSUS AEPD (C-131/12, 13-5-14): EL DERECHO AL OLVIDO EN INTERNET

La STJUE de 13 de mayo de 2014 (*C-131/12, Caso Google vs AEPD*) admitió el derecho al olvido frente a los buscadores de Internet. La historia de Internet tuvo, tras esta Sentencia, un antes y un después pues su impacto no sólo alcanza a la garantía de los derechos fundamentales de los usuarios (en particular, su privacidad y la protección de sus datos personales) sino, incluso, al obligado rediseño de los más exitosos servicios de Internet (buscadores, redes sociales, etc.).

Para el TJUE, los buscadores de Internet son responsables y deben eliminar los enlaces de su lista de resultados aunque el nombre o la información personal no se borren previa o simultáneamente de las páginas web y aunque la publicación en dichas páginas sea lícita. Cualquier internauta que realice una búsqueda a partir del nombre de una persona física puede obtener, a través de la lista de resultados, una visión estructurada de la información relativa a esa persona que circula en Internet. Los internautas pueden establecer así un perfil más o menos

detallado de las personas buscadas. Concluye el TJUE que el efecto de esta injerencia en los derechos de la persona se multiplica a causa del importante papel que desempeñan en la sociedad moderna Internet y los motores de búsqueda por conferir ubicuidad a la información contenida en las listas de resultados. Finalmente, el TJUE proclama que, con el tiempo, un tratamiento inicialmente lícito de datos exactos puede llegar a ser incompatible con la Directiva cuando esos datos se revelen inadecuados, no pertinentes o excesivos atendiendo a los fines para los que fueron tratados y al tiempo transcurrido. Los enlaces a páginas web que contienen esa información deberían suprimirse salvo que el papel de esa persona en la vida pública justifique la prevalencia del interés del público del acceso a esa información[11].

1. El TJUE como juez garante de un derecho fundamental *constitucionalizado*

El Tribunal de Luxemburgo, en el *Caso Google vs AEPD*, ha sido, ante todo, un juez garante de derechos que ha confirmado la alta condición jurídica que ya venía atribuyéndose al derecho a la protección de datos personales tanto en su jurisprudencia como en el marco legal y «constitucional» europeo.

El TJUE alude el *alto nivel de protección*[12] otorgado al derecho de protección de datos, por la Directiva 95/46, el artículo 8 CEDH y los principios generales del Derecho comunitario. Sin embargo, no limita su alcance al de un derecho meramente legalizado por la Directiva 95/46 —como afirmaba el Abogado General en sus Conclusiones— sino que le reconoce el alcance «constitucional» derivado de la consagración en los arts. 7 y 8 CDFUE del respeto de la vida privada y el derecho a la protección de los datos personales —donde se impone que los 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, que toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación y que el respeto de estas normas

11 Un análisis monográfico de esta STJUE puede encontrarse en Rallo Lombarte, A.: *El derecho al olvido en Internet. Google vs. España,* CEPC, Madrid, 2014. También, Vilasau, M.: «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)», *Revista de Internet, Derecho* y Política, n.º 18, 2014; Azurmendi, A.: «Por un derecho al olvido para los europeos: Aportaciones jurisprudenciales de la Sentencia del Tribunal Europeo del Caso Google Spain», *Revista de Derecho Político,* n. 92, enero-abril 2015; Martínez, J.M.: «El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja», *Revista de Derecho Político, n.º* 93, mayo-agosto 2015, pp. 119 y ss.; Martínez, R.: «Aplicar el derecho al olvido», *Revista Aranzadi de derecho y nuevas tecnologías*, n.º 36, 2014; Boix Palop, A.: «El equilibrio entre los derechos del art. 18 de la Constitución, el derecho al olvido y las libertades informativas tras la Sentencia Google», *Revista General de Derecho Administrativo*, n.º 98, 2015; Simón, P.: *El reconocimiento del derecho al olvido digital en España y en la UE,* Bosch, 2015, Barcelona.

12 Considerando 10.

estará sujeto al control de una autoridad independiente—. Esto es, el TJUE no limita su interpretación a un mero juicio de legalidad comunitaria enjuiciando la vigencia de la Directiva sino que recurre al marco constitucional europeo preservando el valor jurídico de la CDFUE y garantizando la vigencia del derecho a la protección de datos en ella consagrado.

2. El *significado* de la privacidad en la sociedad digital

El TJUE toma partido por una determinada comprensión de los efectos de Internet en la sociedad contemporánea: obviando los evidentes efectos benéficos, relevancia social y económica de Internet, el TJUE acotó su valoración a la singular función de los motores de búsqueda. Sus efectos en la protección de datos le permitieron partir de una *conclusión* incuestionable: «la organización y la agregación de la información publicada en Internet efectuada por los motores de búsqueda para facilitar a sus usuarios el acceso a ella puede conducir, cuando la búsqueda de los usuarios se lleva a cabo a partir del nombre de una persona física, a que éstos obtengan mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet que les permita establecer un perfil más o menos detallado del interesado» (punto 37).

Esta actividad descrita por la STJUE impacta en los derechos fundamentales de los ciudadanos y obliga a su protección conforme al vigente marco comunitario: «en la medida en que la actividad de un motor de búsqueda puede afectar, significativamente y de modo adicional a la de los editores de sitios de Internet, a los derechos fundamentales de respeto de la vida privada y de protección de datos personales, el gestor de este motor, como persona que determina los fines y los medios de esta actividad, debe garantizar, en el marco de sus responsabilidades, de sus competencias y de sus posibilidades, que dicha actividad satisface las exigencias de la Directiva 95/46 para que las garantías establecidas en ella puedan tener pleno efecto y pueda llevarse a cabo una protección eficaz y completa de los interesados, en particular, de su derecho al respeto de la vida privada» (punto 38).

3. El *automatismo* de los buscadores de Internet no exonera de responsabilidad

Google negó que los motores de búsqueda «tratasen» datos personales amparándose en el automatismo del rastreo de datos indistintamente personales o no. Pero, el TJUE, siguiendo su propia doctrina inaugurada en el *Caso Lindqvist*, afirmó la vigencia y aplicación del art. 2 b) de la Directiva 95/46: «al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda 'recoge' tales datos que 'extrae', 'registra' y 'organiza' posteriormente en el marco de sus programas de indexación,

'conserva' en sus servidores y, en su caso, 'comunica' y 'facilita el acceso' a sus usuarios en forma de listas de resultados de sus búsquedas. Ya que estas operaciones están recogidas de forma explícita e incondicional en el artículo 2, letra b), de la Directiva 95/46, deben calificarse de 'tratamiento'» (punto 28).

Así las cosas, el TJUE negó que el automatismo de los buscadores los convirtiera en intermediarios neutrales ajenos a las obligaciones derivas del tratamiento de datos:

1. «sin que sea relevante que el gestor del motor de búsqueda también realice las mismas operaciones con otros tipos de información y no distinga entre éstos y los datos personales» (punto 28);
2. «tampoco contradice la apreciación anterior el hecho de que estos datos hayan sido ya objeto de publicación en Internet y dicho motor de búsqueda no los modifique» (punto 29); «aunque la modificación de datos personales constituye, ciertamente, un tratamiento, en el sentido de ésta, en cambio el resto de operaciones que se mencionan en el art. 2 b) de la Directiva 95/46 no precisan en modo alguno de que estos datos se modifiquen» (punto 31).

La STJUE no admite matices al atribuir al buscador de Internet la condición de responsable del tratamiento de datos pues «determina los fines y los medios de esta actividad» en el sentido del art. 2 d) de la Directiva 95/46[13]: «sería contrario, no sólo al claro tenor de esta disposición sino también a su objetivo, consistente en garantizar, mediante una definición amplia del concepto de 'responsable', una protección eficaz y completa de los interesados, excluir de esta disposición al gestor de un motor de búsqueda debido a que no ejerce control sobre los datos personales publicados en las páginas web de terceros»[14].

¿En qué posición queda la responsabilidad de los webmasters? La STJUE establece unas impecables pautas delimitadoras:

1. El tratamiento de datos efectuado por los buscadores es distinto al de los editores de sitios de Internet (punto 35).
2. El impacto de los buscadores sobredimensiona el tratamiento de datos en las webs de origen (punto 36).
3. La falta de utilización por los editores de sitios de Internet de protocolos de exclusión como «robot.txt» y de códigos como «noindex» o «noarchive» no libera «al gestor de un motor de búsqueda de su responsabilidad» (punto

13 Por el contrario, para el Abogado General, «en la medida en que los motores de búsqueda sirven de simples intermediarios, las empresas que los gestionan no pueden considerarse 'responsables', salvo en los casos en los que almacenan datos en una 'memoria intermedia' o una 'memoria oculta' por un período de tiempo que supere lo técnicamente necesario» (punto 24).

14 Punto 34.

39) puesto que el art. 2 d) de la Directiva 95/46 prevé expresamente que la determinación de fines y medios del tratamiento puede realizarse «sólo o conjuntamente con otros».

4. Dada la facilidad con que la información publicada en una web de Internet puede ser copiada en otras, no resultaría una protección eficaz de los interesados que se les exigiera, con carácter previo o en paralelo a la solicitud de cancelación de resultados de búsquedas, obtener su eliminación de los webmasters (punto 84).

Por lo tanto, independientemente del ejercicio de derechos que efectúen los ciudadanos ante los webmasters, los buscadores de Internet deberán atender idénticas pretensiones cuando se les dirijan directamente por su indudable impacto: *la búsqueda por el nombre de una persona puede constituir una injerencia mayor en el derecho fundamental al respeto de la vida privada que la publicación en una página web* (punto 87).

4. La *ingeniería empresarial* y *los legítimos intereses económicos* no pueden debilitar la protección del derecho fundamental

La STJUE atribuyó a la filial española de Google idéntica responsabilidad a pesar de la aparente división de funciones

Frente a la afirmación exculpatoria de que el tratamiento de datos lo efectúaba exclusivamente Google Inc. como gestor de Google Search, sin que Google Spain tuviera intervención alguna —limitándose a promocionar la actividad publicitaria de Google—, el TJUE estimó que la protección eficaz y completa perseguida por la Directiva 95/46 obligaba a *prescindir de una interpretación restrictiva* (puntos 52 y 53). Esto es, vistos los Considerandos 18 a 20 y el artículo 4 de la Directiva 95/46 «el legislador de la Unión pretendió evitar que una persona se viera excluida de la protección garantizada por ella y que se eludiera esta protección, estableciendo un ámbito de aplicación territorial particularmente extenso» (punto 54).

La STJUE confirmó que la filial para venta publicitaria de Google en España (Google Spain) era un «establecimiento» —en los términos del art. 4.1 a) de la Directiva 95/46—. El Tribunal concluyó que el tratamiento de datos se efectúa «en el marco de las actividades» del establecimiento «si éste está destinado a la promoción y venta en dicho Estado miembro de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio propuesto por el motor. En efecto, en tales circunstancias, las actividades del gestor del motor de búsqueda y las de su establecimiento situado en el Estado miembro de que se trate están indisociablemente ligadas, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable y dado que este motor es, al mismo tiempo, el medio que permite realizar las mencionadas actividades» (puntos 55 y 56).

Además, aunque el art. 7 f) de la Directiva 95/46 permite *a priori* el tratamiento de datos por un motor de búsqueda para la satisfacción de un interés empresarial y económico legítimo, éste no prevalecerá sobre la protección de los datos personales. Para el TJUE, *el buscador no ostenta otro título de legitimación para el tratamiento de datos personales que «el mero interés económico»* (punto 81) y su actividad ni está avalada por el derecho fundamental a la información ni puede atribuírsele la condición de «medio de comunicación».

El TJUE admite que, en ocasiones, una web podrá hacer valer *la excepción periodística* para, a tenor del art. 9 de la Directiva 95/46, eludir su aplicación cuando la publicación de información se realice «con fines exclusivamente periodísticos». Pero «ese no es el caso en el tratamiento que lleva a cabo el gestor de un motor de búsqueda» (punto 85), es decir, ni se trata de un medio de comunicación ni su actividad se ampara en el derecho a la información (como sí puede ocurrir, en ocasiones, con las webs de Internet).

La degradación del valor jurídico de la actividad de los buscadores a los justos términos referidos va a tener una extraordinaria relevancia en los ejercicios de ponderación: los ciudadanos obtendrán la prevalencia de sus derechos fundamentales frente a otros intereses —legítimos y apreciables sin duda— pero que el ordenamiento jurídico ubica en un escalón inferior al que sin duda ostentan los derechos fundamentales consagrados en los arts. 7 y 8 CDFUE.

5. El derecho a la información sobre los datos de *personajes públicos* es el único límite al derecho al olvido

La STJUE no reconoce *a priori* un «derecho a la información de los internautas» que les permita oponerse a la cancelación de datos de los buscadores. El TJUE entiende que «la supresión de vínculos de la lista de resultados podría, en función de la información de que se trate, tener repercusiones en el interés legítimo de los internautas potencialmente interesados en tener acceso a la información» (punto 81). Resulta indispensable un ejercicio de ponderación que alcance «un justo equilibrio, en particular entre este interés y los derechos fundamentales de la persona afectada con arreglo a los artículos 7 y 8 de la Carta» (punto 81).

Ahora bien, esta STJUE acota este ejercicio de ponderación sobre *dos extremos* que restringen extraordinariamente la relevancia del interés legítimo de los internautas sobre los datos personales de terceros indexados por los buscadores:

1. Los derechos del titular de los datos prevalecen, con carácter general, sobre el interés de los internautas.
2. En supuestos específicos, *el interés del público* prevalecerá en virtud de la naturaleza de la información y del carácter sensible para la intimidad de la persona afectada —como ocurrirá atendiendo a la función «que esta persona desempeñe en la vida pública» (punto 81)—.

En conclusión, para el TJUE el interés del público internauta únicamente será objeto de valoración y ponderación en el caso concreto cuando los datos personales que pretenden borrarse de los índices de búsqueda afecten a un personaje público o a una información de interés público; aunque, en todo caso, deberán evaluarse tanto la naturaleza de la información como su sensibilidad e impacto en la intimidad de la persona afectada.

La STJUE ofrece diversos pronunciamientos de interés sobre las limitaciones con que se encuentra el derecho al olvido cuando es pretendido por personajes públicos, afectan a informaciones de interés público o son objeto de actividad periodística.

El tratamiento de datos «con fines exclusivamente periodísticos» se beneficia de la exención prevista en el art. 9 de la Directiva 95/46 y limita la aplicación de la normativa de protección de datos tanto si lo realizan prototípicamente *medios de comunicación online* como otros editores de páginas web de Internet sobre informaciones de interés para el público. En estos casos, la STJUE niega la posibilidad de ejercer el derecho al olvido ante el webmaster.

Todo lo contrario cabe afirmar de los motores de búsqueda de Internet que, para el TJUE, ni son medios de comunicación ni actúan al amparo de la excepción periodística ni ejercen el derecho a informar. Por lo tanto, si bien el interesado tiene vedado el ejercicio del derecho al olvido ante las webs «con fines periodísticos», sí podrá solicitarlo del gestor del motor de búsqueda en determinadas circunstancias ejerciendo los derechos de cancelación y oposición previstos en los arts. 12 b) y 14.1 a) de la Directiva 95/46 (punto 85). Y eso es así por cuanto el buscador realiza un tratamiento de datos previsto en el art. 2 b) de la Directiva 95/46 aunque esté referido únicamente a información ya publicada en medios de comunicación.

En consecuencia, la fuerza expansiva del derecho al olvido ante los buscadores resulta extraordinaria y no conoce más límite que el que derive de la ponderación de muy específicos intereses o derechos: ni el mero interés económico de los buscadores ni los intereses del público internauta constituyen elementos suficientes para debilitar el derecho al olvido ante los buscadores salvo en supuestos específicos, dependiendo de la naturaleza de la información y de su carácter sensible para la intimidad de los afectados y siempre en función del papel que estos desempeñen en la *vida pública* (punto 81).

Habrá que valorar el interés público de las informaciones personales y ponderarlo con la afectación de su intimidad para concluir si debe prevalecer el interés de la publicación de los datos o su borrado/olvido en los índices del motor de búsqueda: el interesado no podrá solicitar que la información sea eliminada de la lista de resultados si resulta «por razones concretas, como el papel desempeñado por el mencionado interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate» (punto 97).

6. La *eternidad* de la información en Internet y sus efectos en la privacidad: el «paso del tiempo» como legitimación del derecho al olvido

El derecho de oposición consagrado en el art. 14.1 a) de la Directiva 95/46 será, para el TJUE, el instrumento jurídico idóneo para garantizar un derecho al olvido ponderado y equilibrado, aplicado al caso concreto, y motivado y justificado sobre la situación individual de los solicitantes. El derecho de oposición permite al interesado oponerse, 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 o existan intereses, derechos y libertades que pudieran prevalecer.

La STJUE resume magníficamente cómo el tratamiento de datos personales por los buscadores puede afectar *significativamente* a los derechos fundamentales a la intimidad y a la protección de datos: la búsqueda realizada sirviéndose de ese motor de búsqueda a partir del nombre de una persona física «permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no se habrían interconectado o sólo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o menos detallado de la persona de que se trate … el efecto de la injerencia en dichos derechos del interesado se multiplica debido al importante papel que desempeñan Internet y los motores de búsqueda en la sociedad moderna, que confieren a la información contenida en tal lista de resultados carácter ubicuo» (punto 80).

La *gravedad potencial de esta injerencia* (punto 81) resulta suficiente, a los ojos del TJUE, para fundamentar el ejercicio individual del derecho de oposición y obliga a los motores de búsqueda a eliminar de las listas de resultados obtenidos rastreando el nombre de una persona en páginas web, publicadas por terceros aunque no se borren previa o simultáneamente de dichas webs e, incluso, aunque la publicación sea lícita.

Además, la STJUE se interrogó sobre si la Directiva 95/46 permitía, tras un determinado periodo de tiempo, exigir del buscador el borrado de resultados obtenidos de webs publicadas legalmente por terceros y con datos veraces. El TJUE tomó como referencia los *principios de calidad y necesidad* consagrados en el art. 6 de la Directiva que garantizan que los datos deben ser «adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente» debiendo ser «actualizados» y «conservados durante un período no superior al necesario para los fines para los que fueron recogidos».

A partir de los requisitos anteriores, el TJUE alcanzó las siguientes conclusiones:

1. «Un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con dicha Directiva cuando estos datos ya no

sean necesarios en relación con los fines para los que se recogieron o trataron» (punto 93);

2. El buscador deberá eliminar los datos verídicos publicados legalmente por terceros que, «en la situación actual», habida cuenta del conjunto de circunstancias, resulten incompatibles con el art. 6 de la Directiva por inadecuados, no pertinentes, o excesivos (punto 94).

En definitiva, el TJUE concluyó que «el paso del tiempo» afecta a la «calidad» —de forma que informaciones inicialmente pertinentes, adecuadas y no excesivas pueden dejar de serlo— y a la «necesidad» —por haberse cumplido y agotado la finalidad para la que se recabaron— de los datos y ampara su cancelación[15].

V. CASO FACEBOOK (C-362/14, 6-10-15): EL IMPACTO TRASATLÁNTICO DE LA PROTECCIÓN DE DATOS

La STJUE de 6 de octubre de 2015 (*Caso 362/14 Maximillian Schrems/Data Protection Commissioner*) anuló la Decisión 2000/520/CE de la Comisión Europea, de 26 de julio de 2000, que reconocía un nivel de protección adecuado de los datos personales en EEUU.

Para el TJUE, las autoridades nacionales de protección de datos a las que se hubiera presentado una queja individual podrían examinar si la transferencia de datos respeta las exigencias de la legislación de la Unión Europea sobre la protección de datos aun cuando una Decisión de la Comisión declarare que un país tercero ofrece un nivel de protección adecuado de los datos personales. Por ello, la autoridad irlandesa de protección de datos estaba obligada a examinar la reclamación de particulares y decidir si, en virtud de la Directiva, debía suspender la transferencia de datos de los usuarios europeos de Facebook a Estados Unidos porque ese país no ofrecía un nivel de protección adecuado de los datos personales[16].

15 La STJUE ejemplificó este argumentario en el caso concreto objeto de litigio: «dos páginas de archivos en línea de un periódico que contienen anuncios que mencionan el nombre de esta persona relativos a una subasta inmobiliaria vinculada a un embargo por deudas a la Seguridad Social …teniendo en cuenta el carácter sensible de la información contenida en dichos anuncios para la vida privada de esta persona y de que su publicación inicial se remonta a 16 años atrás, el interesado justifica que tiene derecho a que esta información ya no se vincule a su nombre mediante esa lista» (punto 98) y tiene derecho a exigir que se eliminen estos vínculos de la lista de resultados.

16 Martínez, R.: Safe Harbor: retos para el modelo europeo de la privacidad, 19-10-2015 (http://tecnologia.elderecho.com/tecnologia/privacidad/Safe-Harbor-modelo-europeo-privacidad_11_874180003.html); Álvarez Rigaudias, C.: El acuerdo sobre transferencias de datos a EEUU y Puerto Seguro declarado inválido por el TJUE (http://www.apep.es/monografico-safe-harbor/); Chicharro Lázaro, A.: La transcendencia práctica del caso Facebook en relación con la transferencia masiva de datos personales desde la Unión Europea a Estados Unidos (http://www.revistalatinacs.org/15SLCS/2015_libro/088_Chicharro.pdf);

La Directiva 95/46 establece, como regla general, que sólo se pueden transferir datos personales desde el territorio de la Unión Europea a un país tercero si éste garantiza un nivel de protección adecuado de dichos datos[17]. Conforme a la Directiva, la Comisión puede declarar que un país tercero garantiza un nivel de protección adecuado en razón de su legislación interna o de sus compromisos internacionales. Mediante la Decisión 2000/520/CE, la Comisión Europea reconoció un *sui generis* nivel de protección adecuado de los datos personales en EEUU llamado «régimen de puerto seguro» (*Safe Harbour*) consistente en proclamar una serie de principios de protección de datos personales a los que las empresas estadounidenses podían suscribirse voluntariamente.

Un ciudadano austriaco, Sr. Schrems, usuario de Facebook desde 2008, presentó una denuncia ante la Autoridad Irlandesa de Protección de Datos tras conocer las revelaciones realizadas en 2013 por Edward Snowden en relación con las actividades de la Agencia de Seguridad Nacional (NSA) de Estados Unidos. Conocedor de que los datos de los usuarios de Facebook residentes en la Unión Europea son transferidos a servidores situados en Estados Unidos, el Sr. Schrems motivo su queja en que Estados Unidos no garantizaban una protección suficiente de los datos transferidos a ese país frente a las actividades de vigilancia de sus autoridades públicas. La Autoridad Irlandesa de Protección de Datos desestimó su denuncia entendiendo que la Decisión de la Comisión Europea había estimado el *safe harbour* como un procedimiento de garantía del nivel adecuado de protección de los datos.

La High Court irlandesa presentó una cuestión prejudicial para evaluar si la mencionada Decisión impedía a la Autoridad nacional de Protección de Datos investigar dicha denuncia no sin antes advertir de lo que sigue:

1. que la vigilancia electrónica y la interceptación de los datos personales transferidos desde la Unión Europea a Estados Unidos servían a finalidades necesarias e indispensables para el interés público aunque las revelaciones de Snowden habían demostrado que la NSA había cometido «importantes excesos»;

Mendoza Losana, A.I.: Transferencias internacionales de datos personales: Estados Unidos no es un Puerto seguro, pero tampoco una isla inalcanzable (http://blog.uclm.es/cesco/files/2015/10/Transferencias-internacionales-de-datos-personales_Estados-Unidos-no-es-un-puerto-seguro-pero-tampoco-una-isla-inalcanzable.pdf).

17 A tal efecto, la Directiva 95/46 habilita a la Comisión Europea a evaluar y reconocer la adecuación de aquellos países que garantizan los principios básicos establecidos en la mencionada Directiva. De obtenerse dicho reconocimiento, los países terceros vienen a ocupar un *espacio paneuropeo* que los asimila a los Estados miembros de forma que la circulación de datos entre ellos no requiere de procedimiento o garantia adicional. Es el caso, hasta la fecha, de Canadá, Argentina, Uruguay, Suiza, Israel, Andorra, Nueva Zelanda, etc. Por el contrario, de no existir tal reconocimiento de adecuación, cada transferencia de datos operada por una institución o empresa desde un Estado miembro a un país tercero deberá ser objeto de un contrato autorizado por la Autoridad nacional de Protección de Datos en el que, para cada transferència internacional específica, se garantizará el cumplimiento de la normativa europea.

2. que los ciudadanos de la Unión no disponían de ningún derecho efectivo de audiencia por cuanto las acciones de los servicios de información estadounidenses se realizaban a través de un procedimiento secreto y no contradictorio;
3. que la Constitución irlandesa exigía que toda injerencia en la privacidad y el secreto de las comunicaciones fuera proporcionada y ajustada a las exigencias legales;
4. que el acceso masivo e indiferenciado a datos personales era manifiestamente contrario al principio de proporcionalidad y a los valores fundamentales protegidos por la Constitución irlandesa debiendo gozar de carácter selectivo sobre personas determinadas y estar objetivamente justificado en interés de la seguridad nacional o de la represión de la delincuencia;
5. que, conforme a la STJUE Digital Rights Ireland, el respeto de la vida privada garantizado por el artículo 7 CDFUE y por los valores esenciales comunes a las tradiciones de los Estados miembros quedaría invalidado si se permitiera a los poderes públicos acceder a las comunicaciones electrónicas de manera aleatoria y generalizada, sin ninguna justificación objetiva fundada en razones de seguridad nacional o de prevención de la delincuencia ligadas específicamente a los individuos afectados, y sin garantías adecuadas.

1. La interpretación de la legalidad europea conforme a los derechos constitucionalizados por la CDFUE y su salvaguarda por *autoridades independientes*

De nuevo, el TJUE enfatiza en su Sentencia del Caso Facebook que los derechos reconocidos por la legislación europea deben ser evaluados e interpretados atendiendo a su reconocimiento jurídico en la CDFUE. Así, siguiendo su reiterada jurisprudencia (entre otras, la STJUE recaída en el Caso Google), la Directiva 95/46 deberá enjuiciarse a la luz del derecho a la vida privada y a la protección de datos reconocidos en los arts. 7 y 8 CDFUE adquiriendo especial relevancia el que sus Considerandos 2 y 10 adviertan que Directiva 95/46 pretende garantizar no sólo una protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas frente al tratamiento de los datos personales, sino también «un elevado nivel de protección de esas libertades y derechos fundamentales» (punto 39).

Una de las principales manifestaciones de la trascendencia otorgada al derecho a la protección de datos por el Derecho europeo reside en la obligatoria existencia de Autoridades Independientes que controlen su vigencia.

Así, el art. 28.1 de la Directiva 95/46 impone a los Estados miembros la obligación de instituir una o varias autoridades públicas encargadas del control,

con toda independencia, del cumplimiento de las normas de la Unión en materia de protección de las personas físicas respecto al tratamiento de datos personales. Pero debe resaltarse que esta exigencia está expresamente contemplada en el Derecho primario de la Unión Europea y, en particular, como recordaron las SsTJUE Comisión/Austria (C-614/10) y Comisión/Hungría (C-288/12), en el art. 8.3 CDFUE. Como señala la STJUE, la garantía de independencia de las autoridades nacionales de control pretende asegurar un control eficaz y fiable del respeto de la normativa de protección de datos personales y debe interpretarse a la luz de dicho objetivo: «Esa garantía se ha establecido para reforzar la protección de las personas y de los organismos afectados por las decisiones de dichas autoridades. La creación en los Estados miembros de autoridades de control independientes constituye, pues, un elemento esencial de la protección de las personas frente al tratamiento de datos personales» (punto 41).

Estas Autoridades independientes disponen de amplios poderes, facultades y medios para el cumplimiento de su misión de supervisión en el territorio del Estado miembro aunque no respecto a los tratamientos de datos realizados en un tercer país. Pero el Considerando 60 de la Directiva 95/46 establece que las transferencias internacionales de datos hacia terceros países sólo podrán efectuarse si, siguiendo sus arts. 25 y 26, los países terceros garantizan un nivel de protección adecuado —caso contrario, deberá prohibirse la transferencia—. A la Comisión Europea corresponde adoptar la Decisión que constate que un tercer país garantiza un nivel de protección adecuado pero tal Decisión «no puede impedir que las personas cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país presenten a las autoridades nacionales de control una solicitud, prevista en el artículo 28, apartado 4, de la Directiva 95/46, para la protección de sus derechos y libertades frente al tratamiento de esos datos. De igual forma, una decisión de esa naturaleza no puede dejar sin efecto ni limitar las facultades expresamente reconocidas a las autoridades nacionales de control por el artículo 8, apartado 3, de la Carta y por el artículo 28 de la referida Directiva» (punto 53).

Para el TJUE, el art. 28 de la Directiva 95/46 se aplica a todo tratamiento de datos personales de forma que, aunque exista una Decisión de la Comisión Europea de Adecuación de terceros países, las Autoridades de Protección de Datos a las que una persona haya presentado una solicitud de protección de sus derechos y libertades frente al tratamiento de datos personales que la conciernen, deben poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencias establecidas por la Directiva. Caso contrario, dichas personas quedarían privadas del derecho garantizado por el art. 8 CDFUE de presentar quejas a las autoridades: «una Decisión adoptada en virtud de la referida disposición, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se

hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado» (punto 66).

2. El enjuiciamiento por el TJUE del *débil* sistema estadounidense de protección de datos

El TJUE evaluó el alcance de la Decisión 2000/520 y el debilitado sistema norteamericano de protección de datos personales partiendo de que la adhesión de una entidad a los principios de puerto seguro siguiendo un sistema de autocertificación requiere del establecimiento de mecanismos eficaces de detección y de control para identificar y sancionar las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al respeto de la vida privada y del derecho a la protección de los datos personales. El TJUE constató que la aplicabilidad de esos principios podría limitarse por las exigencias de seguridad nacional, interés público y cumplimiento de la ley estadounidense incluso cuando la legislación estadounidense estableciera una obligación en contrario. De esta forma, la Decisión 2000/520 reconocía la primacía de las exigencias de seguridad nacional, interés público y cumplimiento de la ley estadounidense sobre los principios de puerto seguro de forma que las entidades estadounidenses que recibieran datos personales transferidos desde la Unión Europea estarían obligadas sin limitación a dejar de aplicar dichos principios si resultaran incompatibles. Además, las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitieran acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión.

Por todo ello, tomando como referencia muy particular el Caso Digital Rights Ireland, el TJUE enjuició *indirectamente* el sistema estadounidense al censurar las debilidades de la Decisión 2000/520 en los siguientes términos:

1. Esta normativa, al permitir una injerencia en los derechos garantizados por los arts. 7 y 8 CDFUE, debería contener «reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de éstos» (punto 91).
2. Dichas garantías resultan especialmente relevantes cuando los datos personales se someten a un tratamiento automático y existe un riesgo elevado de acceso ilícito.
3. El respeto de la vida privada exige que las excepciones a la protección de datos y sus limitaciones no excedan de lo estrictamente necesario.

Singularmente concluyentes resultan las siguientes aseveraciones del TJUE sobre la realidad estadounidense:

a) «No se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización» (punto 93).
b) «En particular, se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta» (punto 94).
c) «Una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta … la existencia misma de un control jurisdiccional efectivo para garantizar el cumplimiento de las disposiciones del Derecho de la Unión es inherente a la existencia de un Estado de Derecho» (punto 95).

Finalmente, el TJUE tuvo especial interés en enfatizar la sustracción por la Decisión 2000/520 de las facultades de control sobre las transferencias internacionales a EEUU a las Autoridades nacionales de Protección de Datos. En consecuencia, no se garantizaría el derecho fundamental de protección de datos sobre las transferencias a EEUU procedentes de la Unión Europea. Según la Directiva 95/46 y el art. 8 CDFUE, las Autoridades nacionales deberían poder examinar con toda independencia cualquier solicitud de protección de los derechos y libertades de una persona frente a un tratamiento de datos personales que la afecte. Pero la Decisión 2000/520 establece una regulación específica de las facultades de las Autoridades Nacionales en virtud de la cual podrán suspender los flujos de datos hacia una entidad adherida a los principios de la Decisión 2000/520 de manera *restrictiva* pues estarán sometidas a numerosas condiciones. En definitiva, la Decisión 2000/520 priva a las Autoridades nacionales de las facultades que les confiere la Directiva 95/46 cuando se produzca una denuncia relativa a un tercer país al que se le haya reconocido un nivel de protección adecuado.

***

TITLE: *The Court of Justice of the European Union: Privacy Protection on the Internet*

ABSTRACT: *The origin and evolution of the data protection right has a clear European leadership. The global impact of this originally European legislalion has led to the proliferation of national laws for the protection of data in the rest of the continents and has forced global technology services —regardless of their geographical origin— to adapt to European data protection standards. In particular, these IT services have been adapted to the jurisprudence of the Court of Justice of the European Union on the privacy protection on the Internet. This article will demonstrate the extra European impact of three renowned recent judgments of the Court of Justice of the European Union: Case Digital Rights (Data Retention Directive), Case Google (Right to be Forgotten) and Case Facebook (Safe Harbour). These rulings are a milestone in the evolution of the data protection because of its global impact and, consequently, by the transference of the European standards of data protection to the rest of the planet.*

RESUMEN: *El origen y evolución del derecho a la protección de datos personales tiene una inequívoca impronta europea. El impacto mundial de esta normativa originariamente europea ha supuesto la proliferación de leyes nacionales de protección de datos en el resto de los continentes y ha obligado a los servicios tecnológicos globales —independientemente de su origen geográfico— a adecuarse a la normativa europea de protección de datos. En particular, estos servicios tecnológicos han tenido que adaptarse a la jurisprudencia del Tribunal de Justicia de la Unión Europea sobre protección de la privacidad en Internet. Este artículo evidenciará el impacto global de esta jurisprudencia y la inevitable fuerza expansiva extra europea de tres renombradas sentencias recientes del TJUE: Caso Digital Rights (Directiva conservación de datos), Caso Google (derecho al olvido) y Caso Facebook (Safe Harbour). Estas sentencias marcan un hito en la evolución de la protección de los datos personales por su impacto mundial y, en consecuencia, por la expansión de los estándares europeos de protección al resto del planeta.*

KEY WORDS: *Privacy, Data protection, Right to be forgotten, Internet, European Union, Court of Justice, Safe harbour, Data protection directive.*

PALABRAS CLAVE: *Privacidad, Protección de datos, Derecho al olvido, Internet, Unión Europea, Tribunal de Justicia, Puerto seguro, Directiva de protección de datos.*

FECHA DE RECEPCIÓN: *21.10.2016* FECHA DE ACEPTACIÓN: *01.02.2017*