Regulación Europea sobre Difusión de la Jurisprudencia en Internet

Rosario Duaso Calés

INTRODUCCIÓN

La difusión en Internet de la jurisprudencia plantea cuestiones en lo que respecta a la protección que debe ser acordada los datos personales que los textos de las sentencias contienen. La particularidad de estos datos es su naturaleza de "públicos", lo que nos lleva a plantearnos si estos datos merecen una protección y si la protección que se les debe acordar no entra en conflicto con el principio de transparencia judicial. El paso del "universo papel" a un contexto en el que las sentencias se presentan en diferentes formatos y circulan en la red, ha transformado el concepto de publicidad de las sentencias judiciales que existía en el pasado. En las próximas páginas haremos un estudio de la situación legislativa y doctrinal en Europa sobre las cuestiones relativas ala protección de los datos personales contenidos en las sentencias accesibles en Internet y analizaremos las diferentes modalidades de protección de dichos datos, profundizando especialmente en la anonimización de dichas sentencias.

I EL CRITERIO DE FINALIDAD COMO FUNDAMENTO DE LA PROTECCIÓN DE LOS DATOS PERSONALES DIFUNDIDOS EN INTERNET

I.1 La protección de los datos personales contenidos en los documentos públicos accesibles en Internet

Una de las cuestiones jurídicas más complejas en cuanto al tema que nos ocupa, es determinar si un dato de carácter personal, que ha sido hecho "público", debe seguir siendo protegido. La consecuencia de afirmar que estos datos deben beneficiar de una protección, es la aplicación respecto a estos datos de la normativa europea en la materia, incluso en un momento posterior a la publicación de los mismos.

En Europa, se afirma la aplicabilidad de las leyes de protección de datos a los datos personales que han sido hecho públicos por cualquier medio de publicación. La Directiva 95/46/CE es aplicable tanto al sector público, como al sector privado. En el Libro Verde sobre la información del sector público en la sociedad de la información se señala que la Directiva 95/46/CE realiza un equilibrio entre el acceso a la información del sector público y protección de datos personales[1]. Esto confirma que, el texto adoptado por la Comunidad Europea es aplicable en los casos en que los datos personales de carácter público han sido ya comunicados y se han hecho accesibles a los ciudadanos.

El Dictámen 3/99 relativo a la Información del sector público y a la protección de los datos personales señala que esta teoría debe ser aceptada sin problemas, ya que resulta de la misma aplicación de la legislación en la materia[2]. Como consecuencia, podemos afirmar que, un dato de carácter personal, aunque se haya hecho público, debe seguir siendo protegido, ya que no pierde su carácter de dato personal. Pero, el problema principal para que esta protección se haga efectiva reside en el hecho de que una vez que se han hecho públicos o accesibles a la ciudadanía estos datos, la divulgación imposibilita de forma radical la protección que les debe ser acordada[3].En cualquier caso, las autoridades europeas han querido dejar claro que, la protección de los datos personales, no debe impedir en ningún caso, el acceso de los ciudadanos a la información de carácter público, pero no se debe olvidar que la Directiva 95/46/CE no deja fuera de su ámbito de aplicación, los datos personales que han sido hecho públicos.

En cualquier caso, la cuestión jurídica más importante es el determinar si estos datos que son accesibles al público, pueden beneficiarse de la protección efectiva que otorgan las leyes en la materia. Para la doctrina americana, esta protección se hace especialmente necesaria cuando

---

[1]Libro Verde de la Comisión Europea titulado "La información del sector público : un recurso clave para Europa", COM (1998) 585. Aprobado el 3 de mayo de 1999, p.17.

[2]GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 DE LA DIRECTIVA 95/46/CE, Dictamen 3/99 relativo a la información del sector público y protección de datos personales. Contribución a la consulta iniciada con el Libro Verde de la Comisión Europea titulado "La información del sector público : un recurso clave para Europa", COM (1998) 585. Aprobado el 3 de mayo de 1999.

[3]MARCEL PINET, *"Données publiques ou accessibles au public et données personnelles"*, comunicación presentada en la XX Conferencia internacional de autoridades de protección de los datos de carácter personal celebrada en Santiago de Compostela del 16 al 18 de septiembre de 1998, disponible en esta dirección : http://www.cnil.fr/thematic/docs/annexe4.pdf. (Última visita : 03/02/2002).

estos datos están accesibles en soporte numérico o informático. En el pasado, antes de la llegada de las nuevas tecnologías, los documentos públicos pertenecían al "universo papel" y, se encontraban en registros en los que su búsqueda resultaba muy larga y, en muchas ocasiones, muy difícil y costosa. Estos registros públicos contienen una enorme cantidad de datos de carácter personal sobre los ciudadanos y las nuevas tecnologías han hecho desaparecer la confidencialidad que pudiera existir en el pasado[4]. En los archivos y en los registros públicos del universo papel, la confidencialidad estaba protegida por una opacidad u obscuridad "práctica" que las nuevas tecnologías han hecho desaparecer : en la actualidad resulta muy fácil encontrar datos sobre una persona[5].

Para algunos, sería bastante peligroso el afirmar que los documentos han de seguir siendo de carácter público cuando el encontrarlos resulta dificultoso y, que desde el momento en que la tecnología nos facilita su búsqueda, estos documentos deben ser sometidos a algún tipo de censura. Así, nos podríamos plantear si estos documentos y los datos personales que en ellos se contienen deben perder su carácter de "públicos" cuando ya no resulta difícil su búsqueda.[6]

En realidad, lo más importante es el determinar cuales son las diferencias que existen entre el universo "papel" y el de los documentos en soporte informático. En ambos casos, el contenido de los documentos de carácter público es el mismo, lo que cambia es su soporte. Por lo tanto, la cuestión es determinar si este cambio de soporte o de formato puede significar que documentos y ciertos datos contenidos en estos que, anteriormente eran totalmente accesibles a los ciudadanos, sean ahora de acceso más restringido y controlado. Podemos afirmar que uno de los supuestos más interesantes al que nos enfrentamos en la actualidad, es el caso de los datos personales que se encuentran en los textos de las sentencias judiciales que se difunden en Internet. El principio de finalidad, piedra angular de la normativa sobre protección de datos, es el criterio que debe guiar esta reflexión a fin de encontrar el equilibrio necesario entre protección de datos y acceso a los documentos de carácter público que los contienen, cuando estos no están en un soporte papel y en cambio, son accesibles en Internet en soporte informático.

I.2 La aplicación del criterio de finalidad como base de las medidas de protección

I. 2.a Mecanismos legales para garantizar el respeto del principio de finalidad y limitar los usos ilícitos de los datos personales

[4]ROBERT GELLMAN, *"Utilisation des fichiers publics aux États Unis"*, comunicación presentada en la XXIII Conferencia internacional de autoridades de protección de datos, celebrada en Paris, durante los días 24 a 26 de septiembre 2001, disponible en la dirección siguiente : http://www.cnil.fr/conference2001/fr/contribution/gellman_pdf. (Última visita : 15/06/2002).

[5]R. GELLMAN habla de *"practical obscurity"* en su artículo *"Public registers and privacy : conflicts with other values and interests"*, septiembre 1999, http://www.pco.org.hk/english/infocentre/files/gellman-paper.doc, (Última visita : 2/02/2002).

[6]PIERRE TRUDEL, "L'accès aux documents publics : des ajustements pour assurer la transparence de l'État en réseau", en service de la formation permanente, Barreau du Québec, Développements récents en droit de l'accès à l'information (2002), Cowansville, Éditions Yvon Blais, 2002, p.46.

El elemento esencial que permitirá encontrar una solución a los problemas jurídicos que se plantean en cuanto a la protección de la privacidad en los casos en que bases de datos de carácter públicos son accesibles en Internet, es el principio de finalidad. Es decir, la razón que ha motivado el tratamiento y la publicidad de esos datos, el motivo que justifica su difusión, es la clave para encontrar el equilibrio buscado. En cada caso y, para cada documento, el examen minucioso de la razón que ha motivado que unos documentos sean de carácter público y otros no, es la clave para llegar a determinar los usos lícitos que se pueden realizar de los datos personales contenidos en esos documentos. El hecho es que la naturaleza de los documentos es muy variada, es decir, para cada uno de los casos se deberá estudiar la razón que ha motivado su publicación, la finalidad que se busca al determinar su publicidad. Y, además, es necesario considerar que el medio de difusión y el soporte de estos documentos cambian radicalmente, por lo tanto, se ha de valorar si la finalidad que se invocaba en el pasado para que esos documentos fuesen públicos, pueden seguir siendo la misma con la llegada de la "revolución tecnológica".

Las leyes en la materia están redactadas teniendo como principios básicos el principio de proporcionalidad, el consentimiento del afectado, la seguridad de los datos y demás. Pero cabe señalar que el principio de finalidad es el principio vertebrador de todos estos y, en consecuencia, de la protección de los datos personales. Así, todas las leyes europeas, siendo fieles al espíritu de la Directiva 95/46/CE, hacen referencia más o menos explícita a este principio[7]. Frecuentemente en estos textos encontramos una referencia directa a este principio, pero lo cierto es que no existe ninguna disposición que nos ofrezca una definición del principio de finalidad, lo que hace que sea muy difícil determinación de sus límites. Sin embargo, la obligación de respetar el criterio de finalidad está siempre presente en estos textos legislativos.

El artículo 5 b) de la Convención 108 determina que los datos de carácter personal que sean objeto de un tratamiento automatizados se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades. Y el artículo 5 c) exige que estos datos de carácter personal sean adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado[8].

El artículo 6.1 b) de la Directiva 95/46/CE establece que los Estados miembros dispondrán que los datos personales sean recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines. El articulo 6.1 c) obliga a que esos datos sean adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.

Así, las leyes en la materia crean la obligación de que los datos personales sean únicamente recogidos para su tratamiento y someterlos a dicho tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para los que se hayan obtenido. Por otro lado, se exige que los datos

[7]Directiva 95/46/CE del Parlamento 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. De aquí en adelante : "Directiva 95/46/CE".

[8]Convención para la Protección de la personas con respecto al tratamiento automatizado de datos de carácter personal, Serie de Tratados Europeos, nº 108, hecho en Estrasburgo el 28 de enero de 1981, B.O.E. nº 274, 15/11/1985.

personales que son objeto de tratamiento, no sean usados para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. Por lo tanto, estas leyes crean la obligación de respetar la finalidad que ha sido declarada en el momento de la creación del tratamiento de los datos, finalidad que habrá de ser determinada, explícita y legítima. Toda modificación de esta finalidad ha de ser declarada ya que, en el caso contrario, el tratamiento puede ser considerado como ilegal.

La Commission nationale de l'Informatique et des Libertés (CNIL) ha señalado que los fines para los que el tratamiento se ha creado no deben ser definidos de forma abstracta o en términos que puedan prestar a confusión[9]. El peligro que se puede presentar en lo que se refiere a la protección de la intimidad se manifiesta cuando se desvirtúa o se desvía esta finalidad. Podemos afirmar que, en el contexto actual, en el que la información circula libremente "en la red", existe siempre un riesgo de que esto se pueda producir. Así, por ejemplo, un objetivo perseguido cuando se crea un tratamiento que contiene datos personales, como puede ser el derecho a la información de los ciudadanos, y que a la vez constituye la finalidad por la que son difundidos en Internet, puede verse desvirtuado, a causa del contexto en el que estos datos circulan. Por lo tanto, es de vital importancia que la finalidad por la que los datos se hacen públicos, sea explícitamente determinada, para así poder tomar medidas que tengan como objetivo el evitar la desviación de la misma. En cualquier caso, para poder hablar de esta desviación de la finalidad, es necesario dibujar claramente el principio de finalidad en sí mismo. Pero existe una gran dificultad para lograr este objetivo a causa de la naturaleza subjetiva e indeterminada del propio principio de finalidad.

Podemos plantearnos varias cuestiones en lo que se refiere a la determinación de la finalidad que justifica la difusión en Internet de ciertos datos de carácter público: quién ha de determinarla, qué criterios han de tenerse en cuenta para ello, cuales son las consecuencias de una determinación *a priori* o *a posteriori* de dicha finalidad y, sobre todo, porqué una finalidad que podía ser aceptable para poner a las disposición de los ciudadanos los documentos de carácter público del "universo papel" *,* en el contexto actual, debe ser revisada para ciertos tipos concretos de documentos.

Hay que señalar también que, el carácter subjetivo que caracteriza al criterio de finalidad tiene muchas veces su origen del hecho de que, en numerosas ocasiones, no existe una sola finalidad, sino que existe una pluralidad de finalidades, lo cual es mucho más evidente cuando nos referimos a los datos personales contenidos en los documentos de carácter público. En estos casos, el derecho a la información de los ciudadanos y la libertad de expresión, entre otros, parecen justificar el poder determinar varias finalidades *a priori.* Algunos especialistas en la materia han subrayado la dificultad que se presenta a la hora de determinar con precisión el objetivo que ha provocado la constitución de un tratamiento de datos personales y su posterior difusión en Internet. Una de las dificultades que podemos encontrar tiene su origen en la propia naturaleza de las bases de datos, ya que, éstas pueden tener "finalidades futuras", que ni siquiera se intuyen en el momento de su creación[10]. Esta idea se basa en que, las bases de datos se crean con el interés de que éstas puedan contener infinidad de datos y que, una determinación de una

[9]JEAN FRAYSSINET, Informatique, fichiers et libertés, Paris, Litec, 1992, p.73.
[10]André VITALIS, Informatique, Pouvoir et Libertés, Paris, Economica, 1981, p. 154.

sola finalidad, podría hacerlas ineficaces en un futuro. Pero, no hay que olvidar que las leyes en la materia han establecido la obligación de declarar las nuevas finalidades que se atribuyan a todo tratamiento. Se ha creado el concepto de "extensión de finalidad", que en ocasiones, tiene como objetivo el permitir el acceso de los investigadores y de otros profesionales, ya que, al existir finalidades evolutivas, es mejor proceder a esta extensión que, fijar en un principio una finalidad demasiado ambigua o general[11].En todo caso, parece ser que el llamado derecho al olvido debe ceder ante el tratamiento que se puedan a dar los datos con fines históricos, estadísticos o científicos. Algunos autores nos recuerdan que el juez, al hacer la balanza entre los diferentes derechos que se puedan enfrentar, va a privilegiar la aplicación del interés de la investigación y la libertad de prensa y de información y va a sacrificar la aplicación del derecho al olvido, admitiendo así que investigaciones sobre el pasado de una persona sean realizadas y se hagan públicas[12]. Como ya hemos visto, la Directiva 95/46/CE obliga a que los Estados miembros a tomar garantías al respecto. Así, el Considerando 29 de esta Directiva establece que el tratamiento ulterior de datos personales, con fines históricos, estadísticos o científicos no debe por lo general considerarse incompatible con los objetivos para los que se recogieron los datos, siempre y cuando los estados establezcan las garantías apropiadas. Pero este Considerando establece además que, dichas garantías deberán impedir que dichos datos sean utilizados para tomar medidas o decisiones contra cualquier persona. Vemos así, que estos datos no deben servir para otros usos que los que en este caso, se quieren proteger.

Las particularidades de los datos personales que están contenidos en documentos públicos, como lo son las sentencias judiciales, se deben precisamente su naturaleza, se trata de datos personales "públicos". El ciudadano tiene un derecho al acceso a estos documentos y, la publicidad que les es acordada, tiene como objetivo que todos puedan ejercer su derecho de conocer estos documentos. El principio de finalidad está íntimamente ligado al concepto de libertad y a la protección de ciertos derechos fundamentales de la persona. Podemos pensar en el fenómeno que ha supuesto la utilización habitual de ciertas tecnologías destinadas a garantizar la seguridad en lugares públicos y que, desde hace años, viene creando un conflicto entre el derecho a la privacidad de los ciudadanos y la seguridad que éstas quieren garantizar. En el caso de los datos personales contenidos en los documentos de carácter público, que son accesibles en Internet, nos encontramos ante un conflicto permanente que enfrenta el derecho a la intimidad de las personas afectadas y otros derechos, como pueden ser el derecho a la información de los ciudadanos y el derecho a conocer las resoluciones procedentes del poder judicial. En el caso de las tecnologías de seguridad, se ha creado un cuadro legal que tienen como objetivo determinar claramente la finalidad que persigue su utilización y los usos legales de estas tecnologías. Este cuadro jurídico debe servir para "conciliar la libertad individual y la protección de la vida privada de las personas con las exigencias del orden público"[13]. Estas modalidades de regulación de las tecnologías de seguridad, como los sistemas de vigilancia por videocámara, tendrían que determinar en primer lugar, las finalidades de su utilización, para luego, poner en marcha su funcionamiento mediante un procedimiento administrativo transparente y, finalmente, fijar unas

[11]Jean FRAYSSINET, *op. cit.*, p.73.
[12]Roseline LETTERON, "Le droit à l'oubli", *Revue de Droit Public et de la science Politique*, 1996, vol. 112, nº 1-3, p. 393.
[13]Ver : Henri OBERDOFF, "La liberté individuelle face aux risques des technologies de sécurité", Mélanges Jacques Robert, "Libertés", Paris, Montchrestien, 1998, p. 184.

garantías para las personas que pueden verse afectadas por su utilización[14]. En cualquier caso, vemos que la fijación de la finalidad o las finalidades de los tratamientos de datos personales, es esencial para evitar los usos incompatibles de estos datos con dichas finalidades. Para ello, se ha de estudiar, caso por caso, las consecuencias que la publicación de los datos personales en soporte informático puede ocasionar y, establecer la finalidad lo más precisa posible por la cual, se ha creado el tratamiento y, sobre todo, la finalidad de su publicidad.

A. Perdriau, habla de la finalidad de la publicación de las sentencias judiciales en uno de sus artículos. Este autor mantiene la idea de que los datos personales contenidos en la jurisprudencia, pueden ser publicados para responder de este modo, a la finalidad concreta que se deriva de la necesidad de una perfecta transparencia de las sentencias judiciales. Pero, en ninguno de los casos deben servir para otras finalidades, especialmente para aquellas que posibilitarían hacer búsquedas a partir de criterios que, cambiarían radicalmente no solamente el objetivo de esta publicación, sino, también, la naturaleza de la misma[15]. El artículo 6.1 e) de la Directiva 95/46/CE establece que los Estados miembros deben disponer que los datos personales sean conservados en una forma que permita la identificación de los interesados durante un periodo no superior a al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente, recogiendo así, el principio del derecho al olvido, al especificar que los datos deben permitir la identificación de las personas afectadas durante el periodo necesario. Para garantizar el respeto de esta disposición, se puede proceder a la supresión de los datos o a la anonimización de los mismos. En el *Rapport Braibant*, que trata el tema de la transposición de la Directiva 95/46/CE al derecho francés, se subraya la idea de que la legislación francesa en la materia se basa en varios principios, entre los cuales se encuentra desde luego, el derecho al olvido que obliga a que los datos se conserven por un tiempo determinado y no por un periodo indefinido[16].

Ya hemos examinado varias de las disposiciones que regulan la protección de los datos de carácter personal de la Directiva 95/46/CE, disposiciones similares a las adoptadas en los distintos países europeos. Estas disposiciones tienen aplicación en lo que respecta a los datos personales contenidos en los documentos públicos y, como consecuencia, en los datos que puedan aparecer en las sentencias que se difundan en Internet. Conviene recordar la existencia de un derecho de acceso del interesado a sus datos personales que es reconocido por el artículo 12 de la Directiva 95/46/CE, que debería resultar ejercitable por aquellos cuyos datos están incluidos en una sentencia en formato informático difundida en la red. El derecho de rectificación que es reconocido en el artículo 12.c de este mismo texto comunitario, debería ser poder ejercitado cuando una sentencia ha sido recurrida para poder así evitar un perjuicio a las personas afectadas. Finalmente, el artículo 14 de la Directiva 95/46/CE que reconoce el derecho de oposición del interesado a que sus datos sean objeto de tratamiento, en las condiciones que este artículo establece, debería poder ser ejercitado para aquellos que no deseen que sus datos aparezcan en las sentencias que se difunden en Internet. Así, de estos derechos sería titular el

[14]Ibidem.
[15]André PERDRIAU, "L'anonymisation des jugements civils", *J.C.P.*, éd. G. 1999.I.163.p. 1615, nº37.
[16]Ver Guy BRAIBANT, *Rapport du Premier Ministre sur la transposition en droit français de la Directive 96/46*, Paris, La Documentation française, 1998, disponible en el sitio de la *Documentation française* : http://www.ladocumentationfrancaise.fr.

afectado, que debería poder ejercerlos ante el servicio o el organismo responsable del tratamiento cuando la jurisprudencia es difundida en Internet.

Por otra parte, el artículo 8.1 de la Directiva 95/46/CE establece las condiciones para el tratamiento de ciertas categorías especiales de datos. Esta disposición obliga a que los Estados miembros prohíban el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos ala salud o a la sexualidad. En los casos en que las sentencias judiciales puedan incluir datos de este tipo, por la naturaleza del proceso en concreto, esta disposición debería ser aplicable, siempre y cuando se haga en las condiciones establecidas en el apartado 2 de este artículo y, no sería aplicable cuando el afectado hubiera dado su consentimiento explícito a dicho tratamiento que se reconoce en el artículo 8.2 a) de la Directiva 95/46/CE.

El artículo 8.5 de la Directiva 95/46/CE regula otra de las categorías especiales de datos, al disponer que el tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones que prevean garantías apropiadas y específicas. Se establece, sin embargo, que sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos. Asimismo, se establece que los estados miembros van a poder establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen también bajo el control de los poderes públicos. La Directiva 95/46/CE, como vemos, establece una obligación respecto a los datos de carácter penal y, deja al arbitrio de cada Estado la determinación de las medidas que han de ser adoptadas respecto a los datos relativos a las sanciones de carácter administrativo y aquellos de los procesos civiles. En España, la Ley Orgánica de protección de datos de carácter personal, establece en su artículo 7.5 que "los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras"[17].

Todas estas disposiciones nos demuestran que , a causa del carácter sensible de ciertos datos personales, se debe tener un cuidado especial en lo referente a su protección cuando éstos son objeto de un tratamiento y se difunden en Internet.

Por lo tanto, tal y como hemos visto, es esencial que, mediante instrumentos legislativos se garantice en todo momento la aplicación del criterio de finalidad, para así, limitar también con medios serios y apropiados los usos que se pueden hacer de estos datos de carácter personal. En el contexto europeo, se mantiene la idea de que, se debe limitar de forma explícita los usos que deben ser acordados a los diferentes tipos de datos, mediante la enumeración de simples prohibiciones a este respecto[18]. Sin olvidar por otra parte que, la Directiva 95/46/CE y las leyes

[17]Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, B.O.E 298 de 14 de diciembre de 1999. De aquí en adelante "Ley Orgánica 15/1999 de Protección de datos de carácter personal".
[18]M. PINET, *loc. cit.*, p.7.

nacionales en esta materia, sancionan penalmente la desviación de la finalidad que puede ser hecha de los datos personales[19].

I.2.b Mecanismos técnicos para preservar el criterio de finalidad y limitar los usos ilícitos de los datos personales

La opacidad de los registros públicos que existía en el pasado, ha desaparecido con la llegada de las nuevas tecnologías que hacen posible las búsquedas de los diferentes documentos de forma rápida, eficaz y en todo momento. Por esta razón, el cambio de soporte que han sufrido estos documentos, constituye un elemento clave en esta cuestión y, la difusión en Internet de los datos personales que éstos contienen, hace que se deban revisar la lineas de protección que estaban establecidos para éstos en el pasado. El Grupo de trabajo sobre protección de datos del artículo 29 de la Directiva 95/46/CE, hace hincapié en que las condiciones técnicas de acceso a los documentos de carácter público, deben contribuir a que el criterio de finalidad sea preservado[20]. Se ha subrayado la idea de que, debido a las condiciones de acceso informático que puede ser efectuado por las personas, es muy difícil garantizar en la práctica la especificación de la finalidad, pero que, recurrir a las medidas técnicas de forma concreta y bien planeada, puede contribuir a llegar a conseguir este objetivo.

En primer lugar, podemos afirmar que el paso de los documentos "papel" a los documentos numéricos o en soporte informático, ha supuesto una revolución en lo que respecta a la presentación de dichos documentos. Por otro lado, el fenómeno de la creación de miles de bases de datos, que contienen una enorme cantidad de información también ha contribuido a la llamada "revolución tecnológica". La posibilidad de consultar a distancia estas informaciones, que circulan por la red a nivel internacional, gracias a Internet, cambia la naturaleza de la accesibilidad que existía en el pasado a ciertos documentos. Hay que tener en cuenta además, que unas informaciones que se hacen publicas en un momento determinado, con un fin determinado y de forma justificada, deben contar con una protección especial teniendo en cuenta que en la actualidad, éstas van a ser conservadas durante un tiempo ilimitado. Podemos afirmar que en el caso de las bases de datos de jurisprudencia, nos encontramos ante una situación de este género. No hay que olvidar que los beneficios que comporta la utilización de las tecnologías de la información, vienen acompañados de una capacidad ilimitada para almacenar estos datos, de la creación de una "memoria total" y de la posibilidad de cruzar todas estas informaciones que son conservadas indefinidamente. En realidad, hay que recordar que, en las legislaciones en la materia se exige una limitación temporal de conservación de los datos de modo que permitan la identificación de las personas a quienes conciernen. Y esta medida equivale al reconocimiento del derecho al olvido del cual son titulares estas personas afectando especialmente a las personas cuyos datos aparecen en la jurisprudencia difundida en Internet. Así, el artículo 6 e) de la Directiva 95/46/CE obliga a los Estados miembros a que dispongan que los datos personales sean conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Y prosigue diciendo que los Estados miembros deberán establecer las garantías

[19]Ver : Herbert MAISL, Le droit des données publiques, Paris, L.D.G.J., 1996, p. 60 y 61.
[20]GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 DE LA DIRECTIVA 95/46/CE, *loc. cit.*, p.9.

apropiadas para los datos personales archivados por un periodo más largo del mencionado, con fines históricos, estadísticos o científicos.

Podemos decir que las posibilidades que ofrecen los motores de búsqueda hacen que el concepto de publicidad de las sentencias judiciales se vea transformado respecto al pasado a consecuencia del acceso permanente y durante un periodo de tiempo indefinido de los datos personales que estas contienen. La CNIL en su Recomendación del 29 de noviembre del 2001 nos habla de que las búsquedas mediante el criterio del nombre de una persona con un motor de búsqueda, como pueda ser *Google*, permite de forma gratuita encontrar el conjunto de las informaciones que le conciernen gracias a su difusión en Internet, en sitios situados geográficamente en lugares diferentes y de naturaleza diversa[21]. Vemos así que, la utilización de los motores de búsqueda de "tercera generación" que funcionan en la actualidad revolucionan el concepto de difusión y publicidad de la jurisprudencia. Estos motores son muy potentes ya que, efectúan búsquedas en texto integral en todos los sitios existentes, sin importar el formato del documento, lo cual no era posible anteriormente cuando únicamente eran repertoriados los documentos en formato html. Por otro lado, estos motores copian la totalidad del documento que es guardada en memoria y va a ser conservada sistemáticamente, bastando solo para ello que el motor de búsqueda haya encontrado el documento una sola vez.

Existen sin embargo, varias medidas de carácter técnico que tienen como objetivo evitar la captura sistemática de estos datos personales por los motores de búsqueda. El *Robots Exclusion Protocol* permite evitar que ciertas páginas web o partes de éstas sean encontradas por un motor de búsqueda. Para que este tipo de medidas técnicas sirvan para proteger a las personas afectadas, titulares de los datos personales, los creadores de los sitios Internet y los responsables del acceso a los datos que difunden, deben ser informados de las posibilidades que estos mecanismos técnicos nos ofrecen. En Europa, existe una tendencia a establecer y a definir en cada uno de los casos, la condiciones de búsqueda de los documentos públicos difundidos en Internet, mediante la limitación de los criterios de búsqueda que pueden ser utilizados en cada caso, para evitar de este modo, que los datos sean tratados posteriormente de manera incompatible con los fines para los que fueron difundidos. Son medidas que se toman en relación a las bases de jurisprudencia y también en relación a otras bases de datos de carácter público que son accesibles en Internet. La autoridad de protección de datos de Bélgica recomienda que las sentencias judiciales que se difunden en Internet no sean accesibles utilizando como criterio el nombre de las partes. En Grecia, las búsquedas que se realizan en el catastro, se tienen que hacer mediante la identificación de bien inmueble, para evitar así, poder encontrar la lista de los bienes que pertenecen a una misma persona. En Francia, se han limitado los criterios de búsqueda de los actos de nacimiento y de las guías telefónicas accesibles en Internet, para evitar así que los datos que se pudieran extraer sean utilizados para fines ilegítimos. El ejemplo de las guías telefónicas *"inversées"* que se han hecho accesibles en Internet, es interesante, ya que, estas guías contienen las mismas informaciones que las guías papel tradicionales. Sin embargo, se ha producido un cambio radical debido al criterio de búsqueda que se utiliza, ya que, ya no se busca un número de teléfono a partir de un nombre y una dirección que ya conocemos. En el caso de estas guías

[21]CNIL, *Délibération nº 01-057 portant recommandation sur la diffusion des données personnelles sur Internet par les banques des données de jurisprudence*, de 29 de noviembre del 2001, http://www.cnil.fr/textes/recommand/d01057a.htm, p.2. (Última visita : 10/06/2003).

telefónicas accesibles en Internet, podemos encontrar el nombre y la dirección de una persona gracias a un número telefónico que una persona nos ha facilitado. En ambos casos, los datos personales que se contienen son los mismos, salvo que el titular del número de teléfono haya manifestado su oposición expresa a que sus datos figuren en estas guías. Pero, buscar el nombre y apellidos y, sobre todo la dirección de una persona a partir de un número de teléfono que ésta ha querido desvelar, posibilita obtener una información que esta posiblemente no ha querido que sea conocida por cualquiera, causándole de este modo, un gran perjuicio.

El "carácter público" de las sentencias judiciales que contienen los nombres de las partes y de otras personas envueltas en el proceso, no puede justificar que éstas se integren en bases de datos, en formato numérico y que, sean disponibles por un tiempo indefinido. Por otro lado, hay que recordar que, el Registro de antecedentes penales que almacena todas las condenaciones que han sido hecho públicas mediante sentencia, están regidas por disposiciones legislativas muy fuertes que tienden a proteger la intimidad a las personas afectadas, para así, posibilitar su reinserción[22]. Existe, además, el problema de la existencia de registros paralelos de este tipo, de carácter privado que se puedan crear en la actualidad. La tecnología, en efecto, dificulta enormemente el reconocimiento del derecho al olvido, pues si se modifica o se borra uno público, esto no tendrá ninguna consecuencia en aquel de carácter privado, la condenación puede que no desaparezca jamás. El resultado es que la información que afecta a una persona condenada en el pasado y que, tiene un derecho a que esta información desaparezca del Registro de antecedentes penales público, quedará permanente accesible en Internet, ya que, es difícil que el afectado pueda encontrar al responsable del tratamiento y le pueda obligar a eliminar dicha información y también porque se hace casi imposible el ejercicio del derecho de acceso y de rectificación de sus datos[23]. No debemos olvidar que cuando estos registros se hacen accesibles en Internet, como sucede en Francia, las condiciones de acceso y de seguridad que se establecen en cuanto a las informaciones que este registro contiene, son muy restrictivas.

II LA ANONIMIZACIÓN COMO TÉCNICA DE PROTECCIÓN

La anonimización como medida de protección de los datos de la personas mencionadas en las sentencias judiciales publicadas en Internet ha sido objeto de estudio por la doctrina europea en los últimos tiempos. Existe una controversia en cuanto a las modalidades y a las condiciones de aplicación de esta medida que analizaremos en las próximas páginas.

II.1 El debate europeo sobre la anonimización de las sentencias difundidas en Internet : consecuencias de la práctica de esta técnica

Se pueden tener en cuenta numerosas técnicas que tendrían como resultado la protección de los datos de las personas implicadas las sentencias judiciales que son publicadas en Internet. La anonimización es una técnica que se debate y se analiza en la actualidad y que si se lleva a la

[22]CNIL, *op. cit.*, p. 4.
[23]Ver R. GELLMAN, *loc. cit.*, nota 4, p.7.

práctica, tiene como consecuencia el establecimiento de obligaciones para los responsables de las bases de jurisprudencia accesibles en Internet.

La *Commission nationale de l'informatique et des libertés,* que es el órgano de protección de los datos de carácter personal en Francia, ha dictado una recomendación en la que se estudian los problemas prácticos y jurídicos que la anonimización conllevaría. Esta deliberación establece dos recomendaciones, que en la práctica se convierten en obligaciones legales para los editores de bases de datos de jurisprudencia. La CNIL apunta que sería recomendable lo siguiente:

- que los editores de bases de jurisprudencia accesibles en Internet de acceso gratuito se abstengan, con el objetivo de proteger el derecho a la vida privada de las personas físicas afectadas y del fundamental derecho al olvido, de hacer figurar el nombre, los apellidos y la dirección de las partes implicadas en el proceso y de los testigos;

- que los editores de bases de jurisprudencia accesibles en Internet mediante pago o en CD-ROM se abstengan, con el mismo objetivo, de hacer figurar la dirección de las partes implicadas en el proceso y de los testigos.

Por otro lado, la CNIL recuerda a la totalidad de los editores de bases de datos de jurisprudencia accesibles por Internet o en formato de CD-ROM que si no se ocultan los nombres y apellidos de las partes y testigos de las sentencias que publican, tienen la obligación legal que la ley *Informatique et Libertés* impone de declarar el tratamiento automatizado de datos personales y de respetar las demás disposiciones que la ley impone[24].

Debemos subrayar que la recomendación que se establece para los editores de bases de jurisprudencia de acceso libre y gratuito, se extiende a las sentencias de todas las jurisdicciones, de todas las instancias y de todos los órdenes.

La CNIL, para justificar los dos tipos de recomendación que establece, se apoya en el hecho de que *a priori*, podemos suponer que las sentencias que son accesibles en bases de datos de jurisprudencia de acceso restringido a los abonados y a aquellas de los CD-ROM de jurisprudencia, son consultadas por un tipo de público concreto. En concreto, la hipótesis que mantienen es que estas sentencias son consultadas por profesionales del derecho y que, sobre todo, no son referenciadas por los motores de búsqueda, impidiendo así el encontrar las sentencias "por casualidad", siempre con el objetivo de impedir usos ilícitos de los datos personales contenidos en las sentencias.

Podemos decir que para la CNIL, el problema principal nace de los motores de búsqueda y por lo tanto, el riesgo de vulneración del derecho a la vida privada de las personas afectadas, disminuye desde el momento en que sus datos no se encuentran por este método.

Como es comprensible, estas recomendaciones de la CNIL han sido objeto de numerosas críticas y reacciones por parte de la doctrina. Para algunos, la distinción que se efectúa entre los

[24]*Loi relative à l'informatique, aux fichiers et aux libertés* (nº 78-17 del 6 de enero de 1978), J. O., 7 de enero y rectificativo del 25 de enero de 1978. De aquí en adelante : *"Informatique et Libertés"*.

dos tipos de bases de jurisprudencia, es criticable, ya que no es del todo cierto que el acceso restringido a las bases de datos de pago, deba traducirse por la ausencia de riesgo de una utilización ilícita de los datos de carácter personal de las sentencias[25].

Por otro lado, se pone en tela de juicio las razones que la CNIL nos presenta, en concreto, se nos recuerda que son muchas las bases de jurisprudencia de acceso mediante pago que crean páginas de acceso gratuito con el fin de ser encontradas mediante motores de búsqueda y darse a conocer[26].

Esta recomendación de la CNIL parece que puede crear un desequilibrio entre las diferentes bases de jurisprudencia, ya que la única recomendación que deberían seguir aquellas que son de acceso mediante pago, es la supresión de la dirección de las partes y de los testigos.

En Francia, el sitio *Légifrance*, es el portal jurídico gratuito que acaba de ser creado y permite el acceso a la totalidad de la jurisprudencia del país y que con anterioridad se publicaba en el sitio de pago *Jurifrance.* Los responsables de *Légifrance*, se han puesto como plazo un periodo de dos años para proceder a la anonimización de las sentencias que publican, siguiendo así al pie de la letra la recomendación de la CNIL[27]. Algunos autores han subrayado el hecho de que los editores de bases de jurisprudencia de acceso mediante pago se ven beneficiados por esta recomendación que les permite seguir publicando casi del mismo modo en que lo hacían en el pasado. Estos mismos autores, no dudan en afirmar que esta recomendación puede retrasar la publicación de la totalidad de la jurisprudencia francesa en el sitio *Légifrance*, beneficiando así a los sitios que imponen un pago para acceder a la jurisprudencia que publican[28].

La CNIL ha querido responder a estas críticas que se han levantado por parte de la doctrina francesa desde que esta recomendación fué emitida. Para comenzar, la CNIL apunta que si se desea consultar una sentencia incluida en un CD-ROM de jurisprudencia, la consulta será mucho más fácil que si se procede a su búsqueda en la secretaría de un juzgado o en una publicación papel tradicional de jurisprudencia, pero que en todo caso, la búsqueda es de la misma naturaleza. No se puede negar que, este tipo de búsqueda, no evita totalmente la posibilidad de hacer un uso ilícito de los datos personales contenidos en las sentencias así encontradas, pero que esto también es posible en el "mundo no virtual" del acceso a la jurisprudencia que siempre ha existido. Al contrario, cuando el acceso a la sentencia se realiza mediante a la conexión a un sitio de acceso libre en Internet, se produce en un cambio de naturaleza de esa búsqueda, ya que dicha sentencia que contiene datos de carácter personal podrá ser encontrada por alguien que en ningún momento tuvo la intención de consultarla.

Por otro lado, se nos recuerda que en ningún momento se ha querido exonerar a los editores de bases de jurisprudencia de acceso mediante pago de las obligaciones que las leyes de

[25]Guillaume DESGENS-PASANAU, "La publication des décisions de justice sur Internet", *Expertises des systèmes d'information*, doctr.nº 256.2002.70.
[26]Frédéric LEPLAT, "Décisions de justice publiées sur Internet : pour le droit à l'anonymisation sur simple demande", (10 de mayo 2002), http://www.droit-technologie.org/1_2.asp?actu_id= (Última visita : 08/06/2002).
[27]CNIL, *22º Rapport d'activité*, Paris, La Documentation française, 2002, p.276.
[28]Sylvie ROZENFELD, "Diffusion numérique des décisions de justice : Anonymisation des données pour les sites ouverts au public", *Expertises des systèmes d'information,* act. Nº 255.2002.3.

protección de datos francesas imponen. Es decir, desde el momento en que es difundida en Internet algún tipo de información que incluye datos de carácter personal, se debe respetar el marco jurídico aplicable que impone la ley francesa *Informatique et Libertés* y, por supuesto, la Directiva 46/95/CE.

Aquellos que consideran que el seguimiento de estas directrices ha de ser el mínimo, principalmente, los editores jurídicos y muchos de los usuarios de sus bases de jurisprudencia, se apoyan para justificar esta posición en varios argumentos. El principal de estos argumentos es el carácter público de las sentencias judiciales y como consecuencia, la preservación del principio de transparencia del sistema judicial que en ningún caso debe impedir el acceso a la jurisprudencia por parte de los profesionales del derecho, de los jueces y de los ciudadanos. La autoridad independiente de protección de datos de Bélgica, ha señalado a este respecto que, la finalidad de la publicación de las sentencias judiciales, ha de ser la de alimentar la discusión sobre la jurisprudencia como fuente del derecho y, en ningún caso, que los datos personales de las personas implicadas en un litigio sean conocidos por terceros que carezcan del interés anteriormente mencionado. Por esta razón, esta autoridad ha manifestado el interés de que la evolución tecnológica sea acompañada de una mayor precaución a la hora de difundir la jurisprudencia con los datos personales de las partes gracias a estas nuevas tecnologías de difusión.

Un punto muy interesante de esta controversia es la diferencia que alguna doctrina europea hace entre los conceptos de difusión y de publicidad. Así, la difusión tendría como objetivo primordial, el permitir el acceso a los documentos de carácter público para fines técnicos y científicos. Mientras que la publicidad de las sentencias está en estrecha relación con algunos de los principios básicos de todo sistema democrático, como lo son, el derecho a la información de los ciudadanos y el principio de transparencia de la justicia. Bajo esta distinción, se puede llegar a una conclusión : la publicidad justifica un conocimiento integral de cada sentencia judicial, para evitar así, cualquier tipo de lesión al principio de transparencia judicial. Por el contrario, la difusión de la jurisprudencia, puede ir acompañada en todo momento, de una anonimización de la misma[29].

Para muchos, es de vital importancia el poder tener acceso a una sentencia judicial utilizando como criterio de búsqueda el nombre de las partes. En el mismo sentido, se nos recuerda que las sentencias más importantes, aquellas que crean importantes precedentes jurisprudenciales, son citadas y conocidas, en muchas ocasiones, por los nombres de las partes. Por este motivo, se debería seguir pudiendo efectuar búsquedas bajo este criterio, por ejemplo en el caso en que se quiera recopilar información sobre una persona célebre gracias a los procesos en que ha estado implicado en el pasado. Los que hacen resaltar esta circunstancia, piensan que la anonimización de la jurisprudencia accesible en Internet, puede llegar a impedir a los juristas, a los estudiantes de Derecho y a sus profesores, el que puedan citar una sentencia judicial haciendo referencia a los nombres de las partes. De todos modos, para otros, este argumento en contra de la anonimización, no tiene mucho peso ya que, existen muchos otros criterios de identificación

[29]Catherine TROCHAIN, "L'anonymisation des banques de données juridiques", p. 10, http://www.courdecassation.fr/BICC/550a559/550/communication/REUNION-Id-TROCHAIN550.htm (Última visita : 13/05/2002).

de las sentencias judiciales, como el número de la sentencia o la búsqueda utilizando como criterio los términos contenidos en el texto de la sentencia o por alguna de las disposiciones legales en las que se apoyan los fundamentos jurídicos de la sentencia.

No hay que olvidar que las recomendaciones de la CNIL, serían aplicables única y exclusivamente a la jurisprudencia en formato "numérico" y, que en ningún caso, se quieren crear nuevas reglas para la publicación en formato papel de la misma. Es decir, que no se debe olvidar que la justicia es pública, permitiéndose así, el acceso de los ciudadanos a una copia de todas las sentencias dictadas por los tribunales y, que sus recomendaciones no serían aplicables a las sentencias recogidas en los volúmenes de jurisprudencia que se publiquen en un futuro ni a las bases de datos para el uso interno de los juzgados y tribunales. Por lo tanto, quieren dejar claro que estas recomendaciones tienen su origen en las particularidades que la difusión en Internet presenta en lo referente a las posibles lesiones del derecho a la privacidad.

Finalmente, existen razones de carácter puramente económico que juegan en contra de la anonimización de la jurisprudencia accesible en Internet. En realidad, no se puede negar que el coste económico de la anonimización puede ser muy elevado si se ha de proceder al tratamiento de toda la jurisprudencia que ya es accesible via Internet y, si se deben tener en cuenta múltiples criterios de anonimización, según la naturaleza de cada una de las sentencias. Aunque, es evidente que, la anonimización tendría como una de sus consecuencias de más utilidad, el acabar con el problema de la actualización de las informaciones nominativas que es exigida sobre todo, por las disposiciones relativas a la amnistía[30].

En realidad, el mayor problema reside en la gran tarea que supone para los editores de bases de jurisprudencia, el llevar a cabo una anonimización de la totalidad de las sentencias judiciales que se difunden en Internet. Son varios aquellos que han descartado la posibilidad de recurrir a una "solución técnica", que no podría ser eficaz en ninguno de los casos. Las razones que nos harían descartar esta solución es que los datos que permiten una identificación de las personas involucradas en un proceso pueden ser variados: no sólo el nombre de las partes, sino también de un tercero, el nombre de un lugar, una fecha o un hecho de una naturaleza que permite ser asociado fácilmente con un individuo. Por esta complejidad, parece imposible poder contar con un mecanismo de tipo informático que sea capaz de realizar esta tarea[31]. La "solución humana" representa un trabajo enorme para aquellos que deban proceder a la anonimización, siendo también el error humano algo que no podemos olvidar y que debe ser tenido en cuenta si queremos proceder a una anonimización correcta de la totalidad de la jurisprudencia.
Para C. Trochain, la solución más realista es la puesta en funcionamiento de una "acción conjunta del hombre y de la técnica", que no obstante, no evitaría totalmente los posibles errores a la hora de anonimizar. Esta técnica consistiría en el establecimiento de un procedimiento por el que se atribuiría a cada sentencia un "ficha de anonimización" que comportaría una lista de los datos que deben ser anonimizados en cada situación[32].

[30]Emmanuel LESUEUR DE GIVRY, "La question de l'anonymisation des décisions de justice", http://www.courdecassation.fr/_rapport/rapport00/etudes&docs/LSUEUR.htm,
[31]C. TROCHAIN, p. 7.
[32]Id, p. 8.

No sería posible el proceder en este artículo al estudio de todas las políticas de anonimización que están siendo aplicadas en los diferentes países. No obstante, consideramos que sería de gran interés el análisis de la situación que presenta el caso de España.

En España fué creado en el año 1997, el Centro de Documentación Judicial (CENDOJ), por el Consejo General del Poder Judicial (CGPJ). El CENDOJ tiene como objetivo principal el ofrecer la documentación jurídica permanentemente actualizada al propio CGPJ, a sus distintos órganos, a los órganos de gobierno del Poder judicial y a los órganos jurisdiccionales con el fin de asegurar la conexión del CENDOJ con todos los Juzgados y tribunales en términos de plena efectividad en el acceso directo, inmediato y suficiente a los datos obrantes de él[33].

El CENDOJ, según el artículo 1 de su Reglamento, es un órgano técnico del CGPJ, que tiene como funciones la selección, ordenación, tratamiento, difusión y publicación de información jurídica legislativa, jurisprudencial y doctrinal. Asimismo, este centro tiene a su cargo la creación y el mantenimiento de un servicio central de jurisprudencia. La Sección de Jurisprudencia del Centro, según el art. 8 de su Reglamento, debe llevar a cabo la recopilación y difusión, en la forma que se determine, de la jurisprudencia del Tribunal Supremo y de las sentencias de los Tribunales Superiores de Justicia y Audiencias Provinciales, así como de otras resoluciones judiciales cuya trascendencia e interés doctrinal justifique su difusión. Es decir, que prácticamente la totalidad de las sentencias dictadas por los tribunales españoles a nivel nacional, autonómico y provincial son enviadas a este Centro para su posterior tratamiento. Una vez que las sentencias son remitidas al Centro, se procede a su ulterior tratamiento en base de datos, su edición en soporte informático y a su difusión, facilitando así el acceso a estas de todos los miembros de la Carrera Judicial en sus Juzgados y tribunales[34].

El objetivo más inmediato del CENDOJ es efectuar el tratamiento de la totalidad de las sentencias de los tribunales españoles. Por el momento, una vez que las sentencias judiciales son tratadas, son vendidas en las mismas condiciones de venta a las diferentes empresas editoriales que publican jurisprudencia española en soporte papel y en soporte informático. De forma paralela, se realiza una distribución gratuita de las sentencias a ciertos organismos con los que el CGPJ ha firmado acuerdos.

En cuanto al tratamiento de las sentencias que el CENDOJ realiza, conviene señalar lo que el Pleno del CGPJ apuntaba a este respecto:

"(...), la realización en condiciones adecuadas del proceso de recopilación, tratamiento y difusión de las sentencias y de otras resoluciones judiciales que por su interés lo requieran, permitirá garantizar el acceso de todos los interesados a dichas resoluciones y a su contenido doctrinal y científico, asegurando al propio tiempo la protección de los derechos fundamentales

[33]El CENDOJ se crea por el Acuerdo del CGPJ de 7 de mayo de 1997, B.O.E. nº 123 de 23 de mayo de 1997, (pág. 15956), en virtud del Reglamento 1/1997 del Centro de Documentación Judicial, Aranzadi, RCL 1997/1248 (Legislación Norma Vigente).

[34]Acuerdo del Pleno del Consejo General del Poder Judicial de 18 de junio de 1977, por el que se aprueba la instrucción sobre la remisión de las resoluciones judiciales al Consejo General del Poder Judicial para su recopilación y tratamiento por parte del Centro de Documentación Judicial, B.O.E. nº 123, del 23 de mayo de 1997, Compendio de Derecho Judicial, Madrid, 9 de julio 2001, p´g. 811.

al honor, a la intimidad y a la propia imagen, puesto que, si bien corresponde primariamente a los propios Juzgados y tribunales excluir de la publicidad de sus resoluciones aquellos contenidos que pudieran afectar a tales derechos, conforme a lo que disponen los artículos 1793 de la Ley de Enjuiciamiento Civil y 906 de la ley de Enjuiciamiento Criminal, es indudable que la centralización, tratamiento y difusión de las resoluciones judiciales dictadas por los órganos jurisdiccionales, por los órganos de gobierno del Poder Judicial ha de contribuir también a la preservación de dichos valores, en los términos requeridos tanto por la doctrina constitucional, como por la doctrina jurisprudencial, que han venido poniendo de manifiesto la necesidad de salvaguardar los derechos fundamentales y las libertades públicas en el acceso a las resoluciones judiciales ."[35]

Es decir, que el CENDOJ tiene como atribuida la obligación de proceder a la difusión de las sentencias teniendo en cuenta las reglas de procedimiento civil y criminal al efecto, que establecen reglas que tienden a proteger a las partes en ciertos tipos de procesos, y, además, deben tener en cuenta los riesgos potenciales que han surgido con la difusión de bases de datos de jurisprudencia.

Por otra parte, cabe señalar que el artículo 2.d) de la Ley Orgánica 5/1992 de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal , excluía de su ámbito de aplicación el tratamiento de datos de informática jurídica[36]. No obstante, se impone el respeto a las disposiciones de el Convenio108 y de la Directiva 95/46/CE y la Recomendación nº R (95) 11 relativa a la selección, tratamiento, presentación y archivo de las resoluciones judiciales en los sistemas de documentación jurídica automatizados[37]. Por lo tanto, en la medida en que se limite a reproducir resoluciones judiciales que han sido objeto de publicación, en la presentación y difusión de las resoluciones objeto de recopilación y tratamiento debe procurarse en todo momento la preservación de aquellos aspectos que pudieran afectar al derecho al honor, a la intimidad personal y familiar y a la propia imagen.

En cualquier caso, conviene señalar que la Ley Orgánica 15/99 de Protección de Datos de Carácter Personal[38] ha sido adoptada en España para responder a la obligación de adecuación a la normativa comunitaria y, más concretamente, a la Directiva 95/46/CE. Esta nueva ley española no excluye de su campo de aplicación a los datos de informática jurídica y, establece un nivel de protección equivalente al de la Directiva 95/46/CE.

En el Anexo II de la Recomendación nº R (95) 11 se establece una política de protección de los datos de carácter personal. Así, toda cuestión que afecte a la protección de la vida privada

[35]Acuerdo de 18 de junio de 1997, del Pleno del Consejo General del Poder Judicial, por el que se modifica el Reglamento, nº 5/1995, de 7 de junio, de los Aspectos Accesorios de las Actuaciones Judiciales, B.O.E. nº 157, de 2 de julio de 1997, Compendio de Derecho Judicial, Madrid, 9 de julio 2001, pág. 1089.

[36]Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento automatizado de los datos de carácter personal, B.O.E. nº 262, de 31 de octubre de 1992.

[37]Recomendación nº R (95) 11, del Comité de Ministros del Consejo de Europa, relativa a la selección, tratamiento, presentación y archivo de las resoluciones judiciales en los sistemas de documentación jurídica automatizados. De aquí en adelante : "Recomendación nºR (95) 11".

[38]Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, B.O.E. nº 298 de 14 de diciembre.

y a la protección de datos personales que se pueda plantear en relación a los sistemas de informática jurídica, debe ser contemplada bajo los principios de la Convención 108 y los textos que la desarrollan.

El artículo 5 bis del Reglamento 5/1995, de 7 de junio, de los Aspectos Accesorios de las Actuaciones Judiciales enuncia lo siguiente :

"En el tratamiento y difusión de las resoluciones judiciales se procurará la supresión de los datos de identificación para asegurar en todo momento la protección del honor e intimidad personal y familiar."[39]

Se protege de este modo el derecho al honor y a la intimidad personal y familiar que establece et articulo 18.1 de la Constitución Española y el artículo 18.4 de la misma, que dispone que la ley debe limitar los usos de la informática para asegurar así el derecho al honor y a la intimidad personal y familiar de los ciudadanos y el ejercicio de los derechos que las leyes en la materia les otorgan[40].

En cualquier caso, este cuadro legislativo, lleva al CENDOJ a realizar una anonimización de las sentencias judiciales, lo cual, implica que la jurisprudencia que es difundida via Internet está anonimizada, ya que, los editores y difusores del sector público y los del privado, tienen acceso a las sentencias judiciales, una vez que estas han sido tratadas y anonimizadas. Esto no quiere decir que se impida el acceso a las sentencias en su forma original, ya que el artículo 120.3 CE así lo exige, al establecer que las sentencias se publicarán en audiencia pública.

Como se ha manifestado en alguna ocasión, el derecho a la publicidad de las resoluciones judiciales no puede actuarse única y exclusivamente a través del CENDOJ, ya que una cuestión es que la selección, ordenación, tratamiento, difusión y publicación de las sentencias judiciales se realice por medio de este organismo, con la finalidad de garantizar el derecho fundamental a la intimidad y a la normativa en materia en protección de datos y otra muy distinta es el acceso de todo ciudadano al libro de sentencias de la Secretaría de un Juzgado[41]. En esta misma linea, se puede afirmar que, en ningún caso debemos considerar que la publicación que realiza el CENDOJ colmaría el derecho a la publicidad de las sentencias, ya que por el momento, el CENDOJ, realiza una selección que no contiene la totalidad de las sentencias, no pudiendo quedar este derecho al criterio de este seleccionador y, además, esta selección implica que se

[39]Reglamento nº 5/1995, de 7 de junio de junio, de los Aspectos Accesorios de los Actuaciones Judiciales, modificado por el Acuerdo de 18 de junio de 1977, del Pleno del Consejo General del Poder Judicial, anteriormente citado. Sobre este tema, consultar el artículo siguiente : Antonio SABÍN GONZÁLEZ, "El funcionario de la administración de justicia como usuario de las bases de datos judiciales", Revista Jurídica de la Comunidad de Madrid, nº 6, enero-febrero 2000, http://www.comadrid.es/pres_serv_juridicos/revista_juridica/numero6/comentario4.htm. (Última visita : 10/11/2002).

[40]Constitución Española de 6 de diciembre de 1978, B.O.E. nº 3111.1, de 29 de diciembre de 1978. De aquí en adelante : "CE".

[41]Ver sobre este tema : Voto particular que presentan la Excma. Sra. Dña. Montserrat Comas d'Argemir i Cendra y los Excmos. Sres. Don Javier Martínez Lázaro, Don Luis Aguiar de Luque y Don Alfonso López Tena, Vocales del CGPJ al Acuerdo del Pleno del CGPJ de 9 de octubre de 2002 relativo a la desestimación del recurso de alzada nº 118/02 interpuesto por Alfredo correa Figueroa.

omiten datos, que imposibilitan el hacer reconocible para el público dicha resolución judicial, impidiendo así, la publicidad en sí misma. Varios vocales del CGPJ nos recuerdan lo siguiente :

"(...) debe tenerse en cuenta que son cuestiones distintas la publicidad de las sentencias y la posible construcción de ficheros informáticos sobre datos personales que se realicen con los datos extraídos de las sentencias. Aunque estos ficheros fuesen ilícitos ello no afectaría al principio de publicidad y por tanto al conocimiento público de los libros de sentencias."[42]

Por lo tanto, podemos afirmar que, en ningún caso debe ser confundida la difusión de la jurisprudencia que se realiza en Internet, que debe ir acompañada de medidas específicas destinadas a proteger la intimidad de las personas y la publicidad de las sentencias que debe ser asegurada por el acceso a éstas por los ciudadanos.

II.2 Modalidades de anonimización

En Europa, la doctrina y las autoridades de ciertos países están adoptando ciertas medidas de anonimización de la jurisprudencia difundida en Internet. Hemos estudiado en las páginas anteriores el planteamiento que ha sido adoptado en España, analizaremos a continuación algunas de los planteamientos seguidos en otros países europeos.

Podemos considerar en primer lugar, una anonimización total que comportaría la supresión de los datos que permitan la identificación de las personas físicas y morales. Las excepciones a este principio general serían establecidas en función del tipo de litigio o por una decisión razonada por parte de la autoridad judicial. Aunque, quedaría por determinar quien y en qué condiciones se establecerían estas excepciones y quien deberá estimar su pertinencia. El Ministerio de Justicia francés ha impuesto el principio de la anonimización para sus bases de datos de jurisprudencia difundidas en Internet[43]. En cambio, la Cour de Cassation francesa, no ha optado por esta medida en la difusión en Internet de su jurisprudencia, ya que consideran que una medida de este tipo dificultaría en gran medida la lectura por parte de la ciudadanía de sus sentencias que, en la mayoría de los casos, resultan difíciles de leer por lo técnico y lo lapidario que es el lenguaje utilizado en su redacción. Por otra parte, este tribunal estima que las personas morales no deberían ser tratadas en este caso, en las mismas condiciones que las personas morales, salvo en algunas excepciones[44].

Por otro lado, son muchos aquellos que creen que la anonimización debería ser realizada en el momento mismo de la "producción" de la sentencia, ya que las dificultades que la anonimización comporta, se resolverían en este momento. Por lo tanto, el juez productor de la decisión asume el papel de "anonimizador". Así, esta opción, tendría la ventaja de que el juez, deberá ser aquel que decida cuales son los datos personales que deberán ser anonimizados en cada caso. Para algunos, el juez es aquel que se encuentra en la mejor posición para determinar en cada una de las sentencias, por la naturaleza del litigio y por las personas implicadas en este,

[42]Idem.
[43]GRUPO DE PROTECCIÓN DE TRABAJO SOBRE PROTECCIÓN DE DATOS DELA ARTÍCULO 29 DE LA DIRECTIVA 95/46CE, *op. cit*, pag. 7.
[44]E. LESUEUR DE GIVRY, loc. cit., p. 8.

cuales de los datos que permiten la identificación de partes y testigos habrán de ser anonimizadas. Por otra parte, el coste económico y la cantidad de trabajo y de tiempo que se requieren para una anomización en un momento posterior, se evitarían si se lleva a la práctica esta modalidad de supresión de datos personales[45].

La autoridad belga de protección de la intimidad estima que, si no se procede a una anonimización total, se debería al menos establecer unos criterios de anonimización según el tipo de litigio, la jurisdicción (ellos estiman que las sentencias dictadas por la Cour Suprême, que son citadas muy a menudo por el nombre de las partes, no deberían ser anonimizadas), las partes y testigos. Por otro lado, las partes deberían poder expresar su consentimiento a que sus datos aparezcan en las sentencias o en su caso, manifestar su negativa, sin perjuicio de que el juez pueda decidir en todo momento sobre la anonimización. Las autoridades belgas son conscientes de las dificultades y los costes que esta opción conllevaría y, por lo tanto, mantienen que si no se procede a una anonimización en estos términos, se ha de evitar en todo caso que las búsquedas en Internet de las sentencias judiciales se puedan realizar utilizando como criterio de búsqueda el nombre de las partes.

Otra de las opciones que plantea la doctrina es que las partes del proceso puedan pedir de forma motivada la anonimización de sus datos, independientemente de que el juez pueda de oficio ordenar esta medida en todo momento durante la duración del proceso y una vez vez que se haya dictado sentencia.

Esta orientación se inspira en el artículo 47.3 del Reglamento del Tribunal Europeo de Derechos Humanos que posibilita a aquel que así lo pida, a evitar que su identidad sea revelada en ciertos casos justificados y excepcionales, cuando el presidente del tribunal así lo autorice[46]. En todo caso, esta opción conllevaría que los juzgados y tribunales serían aquellos que deberían gestionar todas las demandas de anonimización y, la carga de trabajo que supondría para estos, hace que sea difícil que ellos juzguen como pertinente esta orientación.

Por todo esto, se ha hablado de un "derecho a la anonimización bajo petición", es decir, bastando un simple requerimiento, derecho que encuentra su fundamento en la Directiva 46/95/CE y en las leyes europeas que se inspiran en esta. Podemos llegar a este razonamiento en la medida en que, la Directiva 95/46/CE y las leyes europeas en materia de protección de datos otorgan a los interesados cuyos datos sean sometidos a tratamiento, un derecho de rectificación y cancelación y un derecho de oposición, cuando las circunstancias lo justifiquen[47].

Esta opción ha sido criticada por ser puramente subjetiva y, sobre todo, porque no siempre el justiciable puede apreciar el interés que para él supone la supresión de sus datos. Como ya hemos mencionado anteriormente, el juez de oficio también podría decidir la

[45]C. TROCHAIN, *loc. cit*., p. 8.
[46]Reglamento del Tribunal Europeo de Derechos humanos, 1998. Consultar sobre esta cuestión : E. LESUEUR DE GIVRY, *loc. cit*., p. 8.
[47]Consultar sobre este "derecho a la anonimización" : F. LEPLAT, *loc. cit*., p.2.

anonimización de ciertas sentencias, pero para algunos, esto podría dar lugar a juicios paralelos y a jurisprudencias enfrentadas sobre este tema[48].

Finalmente, nos debemos preguntar si la simple aplicación efectiva de las legislaciones en materia de protección de datos que la Directiva 95/46/CE ha harmonizado y, que aseguran un alto nivel de protección de los datos que son objeto de tratamiento, no sería suficiente para garantizar los derechos que dicha normativa establece[49]. Estas leyes, que reconocen numerosos derechos a aquellas personas cuyos datos personales son objeto de tratamiento, serían aplicables a los datos contenidos en las bases de jurisprudencia que son difundidas en Internet.

CONCLUSIÓN

Como hemos podido comprobar, el objetivo que se debe lograr, es el encontrar un punto de equilibrio entre el principio de transparencia de la justicia y el derecho al olvido y a la protección de los datos personales de las personas afectadas por la difusión de la jurisprudencia en Internet. Teniendo en cuenta que, la "memoria total" que constituye Internet se enfrenta de forma radical a la memoria humana, que tiene sus límites, muchos de los criterios que eran aplicables en el pasado, es necesario que sean revisados en la actualidad. Como ya hemos visto, para lograr proteger a las personas afectadas cuando la jurisprudencia es difundida en formato numérico en Internet, el criterio de finalidad juega un papel protagonista en el establecimiento del marco legal que se impondrá en el futuro. Las medidas legales y técnicas que pueden ser adoptadas determinarán el grado de protección que se establecerá para los datos personales contenidos en el texto de las sentencias judiciales accesibles via Internet. Las medidas de anonimización, con todas sus diferentes modalidades, deben tenerse en cuenta para llegar al punto de equilibrio necesario que se hace necesario como consecuencia de la evolución que el concepto de publicidad de las sentencias ha sufrido con la llegada de nuevos formatos en que la jurisprudencia nos es presentada y por su difusión en la red.

[48] Idem.
[49] E. LESUEUR DE GIVRY, *loc.cit.*, p. 9.