LA OBLIGACIÓN DE LOS PRESTADORES DE SERVICIOS EN LÍNEA DE REVELAR LA IDENTIDAD DE LOS USUARIOS QUE INFRINGEN DERECHOS DE PROPIEDAD INTELECTUAL A TRAVÉS DE REDES P2P[*]

Por Alfonso González Gozalo[**]
Profesor Ayudante Doctor
Universidad Autónoma de Madrid

SUMARIO: I. PLANTEAMIENTO. LA INFRACCIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL A TRAVÉS DE REDES P2P. II. LA IDENTIFICACIÓN DE LOS SUPUESTOS INFRACTORES Y LOS PROBLEMAS QUE PLANTEA. III. LA OBLIGACIÓN DE LOS PRESTADORES DE SERVICIOS EN LÍNEA DE REVELAR LA IDENTIDAD DE LOS USUARIOS QUE COMETEN INFRACCIONES DE DERECHOS DE PROPIEDAD INTELECTUAL EN NORTEAMERICA. IV. LA OBLIGACIÓN DE LOS PRESTADORES DE SERVICIOS EN LÍNEA DE REVELAR LA IDENTIDAD DE LOS USUARIOS QUE COMETEN INFRACCIONES DE DERECHOS DE PROPIEDAD INTELECTUAL EN EUROPA. EL DERECHO DE INFORMACIÓN DE LA DIRECTIVA 2004/48/CE. 1. Los derechos a la intimidad y a la protección de datos de carácter personal como obstáculos a la revelación de la identidad de los usuarios de internet por parte de los PSL. 2. Los artículos 15.2 y 18 de la Directiva sobre comercio electrónico y su incidencia sobre las legislaciones de los Estados miembros. 3. El derecho de información en la Directiva relativa al respeto de los derechos de propiedad intelectual. V. LA SITUACIÓN EN LA LEGISLACIÓN ESPAÑOLA VIGENTE. 1. El conflicto entre el interés de privacidad de los usuarios de Internet y la protección de los derechos de propiedad intelectual. 2. La recopilación de las direcciones IP de los supuestos infractores por los titulares de los derechos de propiedad intelectual. 3. El requerimiento a los prestadores de servicios en línea para que revelen la identidad de los supuestos infractores. a) *Problemas de índole procesal.* b) *La obligación de los PSL de retener los datos de conexión de los usuarios.* VI. EL DERECHO DE INFORMACIÓN EN EL PROYECTO DE LEY POR LA QUE SE AMPLÍAN LOS MEDIOS DE TUTELA DE LOS DERECHOS DE PROPIEDAD INTELECTUAL E INDUSTRIAL Y SE ESTABLECEN NORMAS PROCESALES PARA FACILITAR LA APLICACIÓN DE DIVERSOS REGLAMENTOS COMUNITARIOS.

[*] Este trabajo ha sido realizado en el marco del Proyecto de investigación *Derechos de propiedad intelectual en Internet* (ref. BJU 2002-00550), cuyo investigador principal es el profesor Rodrigo Bercovitz Rodríguez-Cano, y que financia el Ministerio de Ciencia y Tecnología.
[**] El autor agradece a Javier de Torres su disposición para discutir buena parte de las cuestiones tratadas en este trabajo, el cual se ha visto enriquecido con algunas de sus ideas en materia de derecho procesal y derecho de la competencia. Asimismo da las gracias a Luis Durand por sus pacientes explicaciones en torno al funcionamiento técnico de las redes digitales.

I. PLANTEAMIENTO. LA INFRACCIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL A TRAVÉS DE REDES P2P

Uno de los problemas más preocupantes hoy en día para los titulares de derechos de propiedad intelectual es el creciente número de infracciones que se cometen directamente a través de Internet [1]. Estas infracciones pueden ser de dos tipos. Pueden consistir, en primer lugar, en la puesta a disposición del público de obras o prestaciones protegidas a través de páginas *web*, foros o bases de datos en línea, para que los usuarios las descarguen gratuitamente o a cambio de una remuneración. En segundo lugar, puede tratarse del intercambio masivo de esas obras o prestaciones protegidas entre los propios usuarios a través de sistemas *peer to peer* (P2P), sean éstos centralizados o descentralizados [2]. En ambos casos, cuando dichos actos se realizan sin la pertinente autorización por parte del titular, se infringen los derechos exclusivos de reproducción y comunicación pública [3].

Desde el punto de vista económico, la importancia de estas infracciones que cometen los propios usuarios de Internet es innegable. Así, por ejemplo, en el ámbito musical, entre junio de 2002 y junio de 2003 se descargaron ilícitamente en España entre 180 y 200 millones de fonogramas [4]. En el ámbito

---

[1] Internet es una herramienta directa de infracción de derechos de propiedad intelectual cuando, sin la pertinente autorización, se pone a disposición del público a través de la red la obra o prestación protegida, de modo que los usuarios pueden descargársela inmediatamente en su ordenador. Pero puede también ser un instrumento indirecto o auxiliar para cometer infracciones, cuando la red funciona como vía para publicitar la distribución ilícita de CDs, DVDs o cualesquiera otros soportes que contengan la obra o prestación protegida.

[2] En los sistemas P2P centralizados, la búsqueda de las obras o prestaciones protegidas se canaliza a través de un servidor, que actúa como intermediario, al listar todos los archivos que están disponibles en la red, por haber sido ubicados por los usuarios conectados en sus carpetas compartidas. En los sistemas descentralizados, se prescinde de ese intermediario, de modo que las órdenes de búsqueda se transmiten de ordenador a ordenador dentro de la red, hasta encontrar el archivo deseado; los usuarios, por tanto, acceden directamente a las carpetas compartidas de los ordenadores de los demás usuarios conectados para descargar los archivos que éstos hayan puesto a disposición del resto.

[3] Sigue resultando difícil convencer a los usuarios de la ilicitud del intercambio de obras y prestaciones protegidas a través de redes P2P cuando no se cuenta con la autorización de los titulares de los correspondientes derechos de propiedad intelectual. Los usuarios invocan siempre el derecho de copia privada. Pero, sin perjuicio de que la Ley lo configura como un límite a los derechos de propiedad intelectual, y no como un derecho en sí mismo, lo que es evidente es que el intercambio de obras y prestaciones protegidas queda fuera del ámbito de la copia privada, pues la reproducción no es para uso privado del copista desde el momento en que esa copia se pone a disposición de los demás usuarios para que puedan descargarla si así lo desean. Esa puesta a disposición constituye un acto de comunicación pública, y determina que la copia realizada sea para uso colectivo, lo que impide la aplicación de la excepción. Sobre el particular pueden verse, entre otros, los trabajos de GARROTE FERNÁNDEZ-DÍEZ, I., «Acciones civiles contra los prestadores de servicios de intermediación en relación la actividad de las plataformas p2p - Su regulación en la Ley 34/2002 y en la Ley de Propiedad Intelectual», *Pe. i.*, núm. 16, enero-abril de 2004, págs. 55 y ss., y *La reforma de la copia privada en la Ley de propiedad intelectual*, Comares, Granada, 2005, págs. 217 y ss., y el de GONZÁLEZ DE ALAIZA CARDONA, J. J., «La lucha de los titulares de derechos de autor contra las redes "peer to peer" (P2P)», *Pe. i.*, núm. 18, septiembre-diciembre de 2004, págs. 25 y ss.

[4] Según se informa en el artículo «La SGAE usa el "caso Donkeymania" como advertencia a los usuarios del P2P», publicado el 15 de junio de 2004 en Libertad Digital (<http://www.libertaddigital.com/ noticias/noticia_1275770711.html>).

audiovisual, el número de descargas ilícitas durante 2003 se elevó hasta los diez millones[5], con unas pérdidas estimadas en el sector de 240 millones de euros, equivalente a casi un diez por ciento de la facturación conjunta de los sectores cinematográfico, videográfico y del videojuego[6]. Es tal el perjuicio que estas prácticas causan a la industria del entretenimiento[7] que se ha llegado a decir, de modo muy descriptivo, que constituyen verdaderos supuestos de «piratería doméstica»[8], con el agravante de que se trata de una forma de piratería socialmente aceptada[9].

Es precisamente esa aceptación popular lo que ha llevado a los titulares de derechos a emprender, en los distintos países de nuestro entorno, una importante campaña de concienciación social, consistente no sólo en proclamar con insistencia, en los más diversos foros, la ilicitud de la puesta a disposición del público de obras y prestaciones protegidas mediante páginas *web* y de su intercambio a través de redes P2P (siempre que no se cuente con el consentimiento del titular de los derechos), sino también en el ejercicio de acciones legales contra los infractores más contumaces, con un propósito casi más disuasorio que resarcitorio. La dificultad con la que se han encontrado a la

---

[5] Según informa CNN+, con base en datos suministrados por la Federación para la Protección de la Propiedad Intelectual en la Obra Audiovisual, más conocida como Federación Anti-Piratería (FAP). La FAP engloba a las principales distribuidoras videográficas españolas (como Buena Vista Home Entertainment, Paramount Home Entertainment, Columbia Tristar Home Entertainment, Lauren Films, Manga Films, Universal Pictures Video, Warner Home Video Española, 20th Century Fox Home Entertainment España, Sogepaq, etc.), a las principales distribuidoras e importadoras cinematográficas de ámbito nacional (como United Internationsal Pictures, Hispano Fox-Film, Columbia Tristar Pictures, Warner Sogefilms o Buena Vista International), a los principales editores y distribuidores de software de entretenimiento (Atari, Editorial Planeta, Electronic Arts Software, FX Interactive, Microsoft, Proein, Sony Computer Entertainment, Virgin Play, Vivendi-Universal Interactive Publishing...) y a la Motion Pictures Association, entre otras entidades.

[6] Vid. <http://www.plus.es/codigo/noticias/ficha_noticia.asp?id=393971>.

[7] Por poner un ejemplo muy ilustrativo, la película «Mortadelo y Filemón», según pusieron de manifiesto Asunción Balaguer y Carlos Álvarez ante la Comisión del Senado sobre Artes Escénicas en septiembre de 2003, había sido descargada ilícitamente a través de Internet por más de 150.000 personas, sólo siete meses después de su estreno cinematográfico, en febrero de 2002.

[8] Cfr. CARBAJO CASCÓN, F., «El pulso en torno a la copia privada», *pe. i.*, núm. 16, enero-abril de 2004, pág. 15. Esta expresión ha sido criticada por SÁNCHEZ ARISTI, R., «La copia privada digital», *pe. i.*, núm. 14, mayo-agosto de 2003, págs. 9 y 10. Personalmente, no me parece desatinada, si se entiende en sentido impropio, pues aunque es cierto que los usuarios no obtienen un beneficio comercial directo, es indudable que se lucran, en cuanto que se ahorran los costes de adquisición de esa obra o prestación protegida. No se olvide, en este sentido, que el concepto de beneficio económico que se maneja en el ámbito de la propiedad intelectual es muy amplio, como demuestra el artículo 19.3 TRLPI, cuando define el alquiler como «la puesta a disposición de los originales y copias de una obra para su uso por tiempo limitado y *con un beneficio económico o comercial directo o indirecto*» (el subrayado es mío).

[9] Según un informe publicado por la Motion Picture Association of America (MPAA) en julio de 2004 sobre la piratería en Internet a nivel mundial, disponible en la página *web* <http://www.mpaa.org/MPAAPress/index.htm>, aproximadamente uno de cada cuatro usuarios de Internet (un 24 por ciento de los usuarios, para ser más exactos) se ha descargado ilícitamente alguna película. Los porcentajes varían de unos países a otros, desde el 58 por ciento de Korea hasta el 10 por ciento de Japón, pasando por el 18 por ciento de Australia, el 19 por ciento de Alemania, el 20 por ciento de Reino Unido o Italia, el 24 por ciento de Estados Unidos o el 27 por ciento de Francia. Tan preocupante como el porcentaje de usuarios de Internet que han descargado ilícitamente películas a través de la red es que el 56 por ciento de tales usuarios esperan seguir haciéndolo, y que el 17 por ciento de los que todavía no han descargado películas por Internet esperan comenzar a hacerlo en el futuro.

hora de iniciar estos procesos judiciales es la imposibilidad de identificar a los infractores sin la colaboración de quienes les han prestado los servicios de alojamiento o acceso a Internet, agravada por las reticencias de estos prestadores de servicios a revelar la identidad de sus destinatarios, ante el temor de incurrir en un incumplimiento del contrato celebrado con el usuario en cuestión o, incluso, en una cesión ilícita de datos de carácter personal. La cuestión es, pues, si los prestadores de servicios de la sociedad de la información están obligados a comunicar a los titulares de los derechos de propiedad intelectual presuntamente vulnerados los nombres de los supuestos infractores y, en su caso, cuál es la vía para exigirles el cumplimiento de esta obligación. A tratar de darle respuesta se dedica este estudio, que se va a centrar únicamente en el supuesto más problemático en la práctica, que es el de las infracciones que se cometen a través de redes P2P.

II. LA IDENTIFICACIÓN DE LOS SUPUESTOS INFRACTORES Y LOS PROBLEMAS QUE PLANTEA

Para averiguar la identidad de quien infringe derechos de propiedad intelectual a través de redes P2P, el titular de los derechos en cuestión tiene que realizar, por sí o mediante tercero contratado a tal efecto, varias operaciones[10]. En primer lugar, debe conectarse a la red P2P a través de la cual cree que se están infringiendo sus derechos de propiedad intelectual, a fin de constatar si efectivamente se intercambian de manera ilícita las obras o prestaciones protegidas cuyos derechos le pertenecen. Una vez conectado a la red, buscará obras o prestaciones protegidas de su repertorio, para cerciorarse, de forma global, de que sus derechos están siendo infringidos. El siguiente paso es averiguar quién es el infractor. Lo normal, lógicamente, es que sean muchos usuarios los que estén poniendo a disposición de los demás esas obras o prestaciones protegidas. En estos casos, lo que suele hacer el titular de los derechos es centrarse en aquellos usuarios que intercambian obras o prestaciones protegidas de forma masiva, es decir, los que hayan copiado en sus carpetas compartidas un mayor número de ellas (estamos hablando de cientos, cuando no varios miles, de archivos). Cuando el supuesto infractor haya sido localizado, y previa copia del listado de los archivos que se encuentren ilícitamente alojados en su carpeta compartida (y, por ende, puestos a disposición de los demás usuarios conectados), deberá comprobarse, mediante su descarga, que tales archivos contienen efectivamente las obras o prestaciones protegidas en cuestión. Finalmente, si de las anteriores operaciones resulta aparente que se han infringido derechos de propiedad intelectual, su titular registrará, además de la fecha y hora exacta en que se produjo la supuesta infracción, tanto el *nick* o *alias* del supuesto infractor como, más importante, su dirección IP. Ambos datos son públicos, en el sentido de que están a

[10] Vid. la sentencia canadiense de la Corte de Apelación Federal en el caso *Glaxo Wellcome PLC contra M.N.R.* [1998], 4 F.C. 439 (C.A.). Lo habitual es que estas operaciones se realicen de forma automatizada, mediante agentes electrónicos programados para detectar infracciones e identificar al supuesto infractor.

disposición de todos los usuarios de la red P2P en cuestión, por lo que su obtención es sencilla [11].

Más allá de la averiguación del *nick* y la dirección IP de los supuestos infractores los titulares de derechos no pueden llegar por sí solos. Para descubrir quiénes son las personas que se esconden bajo esos datos, tienen necesariamente que recurrir a los prestadores de servicios de la sociedad de la información y, más en concreto, a los proveedores de acceso a Internet, pues sólo éstos pueden asociar un nombre (el de su cliente) a una dirección IP [12].

La identificación de la persona que está detrás de una dirección IP podría constituir una labor muy sencilla para el proveedor de acceso si las direcciones IP fueran estáticas, es decir, si cada usuario tuviera asignada una dirección IP fija, de tal manera que siempre que se conectara a Internet lo hiciera a través de esa dirección. Sin embargo, hoy por hoy, la escasez de direcciones IP imposibilita que todas ellas sean estáticas. Si lo fueran, no habría suficientes para todos los potenciales usuarios [13]. Por ello, partiendo de la base de que no todos esos usuarios en potencia querrán conectarse simultáneamente a Internet, se funciona mayoritariamente con direcciones dinámicas [14]. Esto significa que se asignan automáticamente por los servidores a los usuarios cuando se conectan a Internet [15], y únicamente para el tiempo que dure la sesión [16]. Ello implica que un mismo usuario puede tener una dirección IP distinta cada vez que se conecte a Internet. Y, de igual forma, una misma dirección de IP puede asignarse sucesivamente a varios usuarios. Lógicamen-

---

[11] Es esencial de cara a un eventual proceso judicial posterior preconstituir las pruebas en que pueda fundarse la ulterior demanda.

[12] Toda conexión a Internet genera datos de tráfico, entendiendo por tal, de acuerdo con el artículo 2 b) de la Directiva 2002/58, cualquier dato que necesariamente deba ser tratado para establecer una comunicación a través de una red de comunicaciones electrónicas o para facturarla. Uno de esos datos de tráfico es la dirección IP, sin la cual la conexión a Internet es imposible. Aunque tanto el operador de telecomunicaciones como el proveedor de acceso a Internet recogen los datos de tráfico que genera una conexión a Internet, sólo el prestador del servicio de acceso puede conocer la dirección de IP del usuario, pues es él mismo quien la adjudica al recibir la solicitud de conexión.

[13] La versión actual del Protocolo Internet IPV4 (Internet Protocol Version 4), que se usa desde hace más de veinte años, utiliza direcciones de IP de 32 bits, lo que proporciona un total de aproximadamente 4.295 millones de direcciones distintas para todo el mundo, sin duda insuficientes para todos y, además, mal distribuidas, pues la mayoría de esas direcciones están adjudicadas a servidores de Norteamérica. El problema de la escasez de direcciones IP se solucionará cuando el Protocolo IPV6 (Internet Protocol Version 6) esté totalmente implantado, ya que utiliza direcciones de 128 bits, lo que asegura más de 16 trillones de direcciones únicas.

[14] Las direcciones estáticas quedan para los elementos de la infraestructura de una red IP, como los enrutadores, los servidores *web*, o los servidores de correo, que, por su propia función, requieren direcciones fijas.

[15] Las direcciones de IP, como recurso escaso que son, las gestiona la ICANN (Corporación Internet para la asignación de nombres y números). En Europa, es la organización RIPE (Réseaux IP Européens) la que redirecciona las direcciones que le corresponden. A través de un procedimiento internacional tiene lugar la adjudicación de las direcciones IP a proveedores de acceso a Internet, quienes las reasignan a sus clientes. Cfr. *Privacidad en Internet*, documento de trabajo redactado por el Grupo de Trabajo sobre Protección de datos del artículo 29 de la Comisión Europea, adoptado el 21 de noviembre de 2000, 5063/00/ES/FINAL, pág. 10.

[16] Cuestión distinta es que si un usuario está conectado permanentemente a Internet, lo que permiten las líneas ADSL, mantenga la misma dirección IP durante todo ese tiempo.

te, el hecho de que las direcciones IP que se asignan a los usuarios de Internet sean dinámicas dificulta la determinación por parte de los proveedores de acceso de la identidad del usuario que utilizó una específica dirección IP en un momento dado. Para empezar, además del numero de IP, se le tiene que facilitar al proveedor de acceso el día y la hora exacta de la conexión durante la cual, supuestamente, se produjo la infracción. Con esos datos, el prestador de servicios podrá averiguar a qué cuenta de acceso a Internet correspondía esa dirección en ese concreto momento y, tras consultar otra base de datos distinta, determinar quién es su titular. Ahora bien, no puede dejar de señalarse que el proveedor de acceso tampoco puede llegar más allá de la averiguación del titular de la cuenta de acceso a través de la cual se ha cometido la infracción, lo que no garantiza la identificación del usuario que, sirviéndose de ese acceso, infringió los derechos de propiedad intelectual. En ocasiones ni siquiera asegura la identificación del ordenador desde el que presuntamente se cometió la infracción. Así sucede cuando varios equipos informáticos se conectan a Internet por medio de una única cuenta de acceso (por ejemplo, si se trata de una red de área local).

> En el caso de las redes de área local, lo habitual es que todos los ordenadores de esa red local accedan al exterior a través de un único enrutador (pueden ser más, si son muchos los ordenadores conectados a esa red), dotado de su propia dirección IP, que normalmente será estática. Ésta será la única dirección pública, es decir, la única que trasciende al exterior. Las direcciones concretas de los ordenadores incardinados en esa red local son privadas, en el sentido de que sólo se pueden conocer desde dentro de la propia red. Por consiguiente, si desde un ordenador conectado a una red de área local se intercambian archivos a través de una red P2P, el titular de los derechos sólo podrá averiguar la dirección IP del enrutador que da salida al exterior a ese ordenador. Con ese dato y, en su caso, con la hora exacta de la conexión (si se trata de una dirección IP dinámica), el proveedor de acceso podrá identificar al titular de la cuenta de acceso a Internet, es decir, al titular de la red de área local (por ejemplo, una empresa, o una Universidad). Pero no podrá llegar más allá. En concreto, no podrá saber desde qué dirección privada, dentro de esa red, se ha cometido la infracción. Esto es algo que, en su caso, sólo podrá conocer el titular de esa red local.

A los problemas anteriores se suma el del transcurso del tiempo. Como hemos visto, para identificar al supuesto infractor, o al menos al titular de la cuenta de acceso a partir de la cual se ha podido cometer la infracción, es necesario recuperar esa información de las bases de datos de proveedor de acceso. Cuanto más antigua es la información buscada, más difícil es recuperarla. A partir de cierto punto, la recuperación es imposible, bien porque se ha perdido en el maremagno de datos, bien porque, simplemente, se ha borrado. Por razones similares, cuanto más antigua es la información, menos fiables son los resultados que se pueden obtener, porque la posibilidad de error es mayor.

Si desde el punto de vista técnico la identificación del supuesto infractor no está exenta de dificultad, como acabamos de ver, desde el punto de vista

jurídico plantea también numerosos problemas, tanto sustantivos como procesales. Por un lado, puede entrar en colisión con derechos fundamentales, como la libertad de expresión, el derecho a la intimidad, la libertad informática y el derecho a la protección de datos personales. Por otro lado, y por más que el artículo 8 de la Directiva 2004/48 del Parlamento Europeo y del Consejo, de 29 de abril, relativa al respeto de los derechos de propiedad intelectual (en lo sucesivo, DRDPI) reconozca a los titulares de derechos de propiedad intelectual un *derecho de información* lo suficientemente amplio como para comprender el supuesto que aquí estudiamos, lo cierto es que nuestro ordenamiento vigente no contiene una vía procesal expresa para articularlo. Es más, el Anteproyecto de ley de transposición de esta Directiva omitía, al incorporar el mentado artículo 8, toda referencia al deber de informar que, según la norma comunitaria, tienen los prestadores de los servicios utilizados por el infractor para cometer la infracción. Afortunadamente, el Gobierno reaccionó a tiempo, y finalmente incluyó en el Proyecto de Ley por la que se amplían los medios de tutela de los derechos de propiedad intelectual e industrial y se establecen normas procesales para facilitar la aplicación de diversos reglamentos comunitarios, publicado en el BOCG de 28 de octubre de 2005, un deber de información a cargo de los prestadores de servicios intermediarios hasta cierto punto similar al de la Directiva 2004/48/CE.

A través de este trabajo pretendo buscar salidas a los problemas apuntados. A tal efecto, analizaré primero la experiencia de algunos países de nuestro entorno y la solución propuesta por la DRDPI, para centrarme a continuación en nuestro derecho interno, tanto el vigente como el proyectado.

III. LA OBLIGACIÓN DE LOS PRESTADORES DE SERVICIOS EN LÍNEA DE REVELAR LA IDENTIDAD DE LOS USUARIOS QUE COMETEN INFRACCIONES DE DERECHOS DE PROPIEDAD INTELECTUAL EN NORTEAMERICA

Tanto en los Estados Unidos de América como en Canadá se ha planteado si los proveedores de acceso a Internet están obligados a desvelar la identidad de aquellos destinatarios de sus servicios que presuntamente infringen derechos de propiedad intelectual a través de redes P2P.

Sabido es que, en los Estados Unidos, los titulares de derechos (primero las compañías discográficas y la RIAA [17], después las productoras y distribuidoras cinematográficas y la MPAA [18]) comenzaron su lucha contra el intercambio no autorizado de obras y prestaciones protegidas a través de redes P2P demandando a quienes ponían a disposición del público los medios técnicos para llevar a cabo el intercambio, al considerarlos responsables indirectos de la

[17] Recording Industry Association of America.
[18] Motion Picture Association of America.

infracción[19]. Pronto, sin embargo, y sobre todo a partir del revés que implicó la sentencia dictada por la Corte del Distrito de California en el caso *Grokster*[20], se dieron cuenta de que demandar sólo a quienes facilitaban los medios para intercambiar archivos a través de redes P2P era insuficiente. Por ello, pretendiendo atajar el problema desde su misma raíz, decidieron emprender acciones legales contra los propios usuarios, infractores directos de sus derechos. Como paso previo, lógicamente, tenían que averiguar la identidad de estos usuarios, y creyeron encontrar la vía para ello en la sección 512(h) de la *Digital Millenium Copyright Act* (DMCA).

De acuerdo con la sección 512(h) DMCA, el titular del *copyright* puede solicitar al oficial de cualquier Corte de Distrito federal que emita un requerimiento dirigido a un prestador de servicios en línea (PSL) a fin de que identifique a un supuesto infractor, para lo cual deberá presentar tres documentos: una copia de la notificación de infracción del *copyright* a la que se refiere la sección 512(c)(3)(A), una propuesta de requerimiento y una declaración jurada de que el propósito del requerimiento es obtener la identidad de un supuesto infractor y que la información sólo será utilizada a los efectos de la protección del *copyright*.

> La notificación de infracción del *copyright* a la que se refiere la sección 512(c)(3)(A) debe contener los siguientes elementos: (1) la firma del titular de los derechos; (2) la identificación de la obra objeto de *copyright* que supuestamente ha sido infringida; (3) la identificación del material que presuntamente infringe el *copyright* y que debe ser retirado, o el acceso al cual debe ser eliminado, e información razonablemente suficiente para permitir al PSL su localización; (4) información razonablemente suficiente para permitir al PSL ponerse en contacto con el solicitante del requerimiento; (5) una declaración de creencia de buena fe en que el material supuestamente infractor no es lícito de acuerdo con el derecho de *Copyright*; y (6) una declaración, bajo pena de perjurio, de que la notificación es correcta y de que la parte solicitante está autorizada para actuar en nombre del titular del *copyright*.

A la vista de los anteriores documentos, y si cumplen los requisitos formales establecidos por la ley, el oficial judicial firmará el requerimiento propuesto

---

[19] Vid. la resolución de la Corte del Distrito de California en el caso *A&M Records, Inc. y otros contra Napster, Inc*., 114 F.Supp.2d 896 (N.D. Cal. 2000), así como la de la Corte de Apelación del Noveno Circuito, que vino a confirmar la anterior (*A&M Records, Inc. y otros contra Napster, Inc.*, 239 F.3d 1004 [9th Cir. 2001]), concediendo las medidas cautelares solicitadas por los titulares de derechos contra la entidad que centralizaba el intercambio de archivos protegidos. Vid. asimismo las sentencias de la Corte del Distrito de California y la Corte de Apelación del Noveno Circuito en el caso *Grokster*, desestimando la demanda interpuesta por los titulares de derechos contra empresas que ponen a disposición del público programas que permiten el intercambio descentralizado de archivos a través de redes P2P (*Metro Goldwyn Mayer Studios, Inc. y otros contra Grokster, Ltd. y otros*, 259 F.Supp.2d 1029 [C.D. Cal. 2003] y *Metro Goldwyn Mayer Studios, Inc. y otros contra Grokster, Ltd. y otros*, 380 F.3d 1154 (9th Cir. 2004) [C.D. Cal. 2003]). La Corte Suprema, en sentencia de 27 de junio de 2005 (125 S.Ct. 2764 [U.S. 2005]), estimó el recurso interpuesto por los titulares de derechos, revocando la sentencia dictada en grado de apelación y devolviendo los autos para que se vuelva a decidir sobre el asunto, tomando como referencia las consideraciones hechas por Alto Tribunal Federal.

[20] Vid. nota anterior.

por el solicitante y se lo devolverá para que lo envíe. Recibido el requerimiento por el PSL, deberá revelar la información solicitada. Si no lo hace voluntariamente, el titular del *copyright* podrá solicitar la ejecución forzosa del citado requerimiento. En el ámbito de este proceso se dilucidará si efectivamente se cumplen los requisitos para la aplicación de la sección 512(h) o no.

Al amparo de esta sección 512(h), la RIAA requirió a numerosos PSL para que identificaran a quienes supuestamente infringían, a través de redes P2P, los derechos de los productores fonográficos. Muchos de estos PSL cedieron y revelaron las identidades solicitadas, lo que le permitió a la RIAA dirigirse directamente contra los presuntos infractores, alcanzando acuerdos en unos casos y teniendo que emprender acciones legales en otros. Otros prestadores, sin embargo, se negaron a suministrar la información requerida. Tal fue el caso de Verizon Internet Services. El 24 de julio de 2002 este PSL fue requerido por la RIAA, de acuerdo con el procedimiento de la sección 512(h) DMCA, a fin de que suministrara información suficiente para identificar a quien, mediante el intercambio de archivos en una red P2P, supuestamente infringía el *copyright* sobre ciertos fonogramas que se indicaban en la carta que acompañaba al requerimiento. En esta carta, y siempre de conformidad con lo dispuesto por la sección 512(h) DMCA, la RIAA indicaba la dirección IP del supuesto infractor, así como los ochocientos archivos ilícitamente comunicados, expresaba su creencia de buena fe de que el intercambio de archivos que llevaba a cabo este usuario infringía el *copyright* de sus asociados y solicitaba a Verizon su colaboración inmediata en la cesación de esa actividad no autorizada por parte del usuario. Verizon se negó a proporcionar la información solicitada, alegando que se había limitado a prestar el servicio de acceso a Internet, y que, en consecuencia, no le es aplicable la sección 512(h) DMCA. Ello obligó a la RIAA a instar la ejecución forzosa del requerimiento, siendo estimada su pretensión por la Corte del Distrito de Columbia el 21 de enero de 2003[21]. Antes de que la Corte del Distrito de Columbia resolviera sobre ese primer requerimiento, la RIAA envió un segundo requerimiento a Verizon. En esta ocasión, el PSL optó por oponerse judicialmente al mismo, planteando la posible inconstitucionalidad de la sección 512(h) DMCA. Su oposición, sin embargo, fue desestimada por la Corte del Distrito de Columbia en abril de 2003[22]. Recurridas ambas resoluciones por Verizon, y acumulados los dos recursos, la Corte de Apelación del Distrito de Columbia falló a favor del PSL[23], en una resolución que es firme, dado que el 12 de octubre de 2004 la Corte Suprema inadmitió el recurso preparado por la RIAA.

La Corte de Apelación del Distrito de Columbia vino a acoger buena parte de la argumentación de Verizon en cuanto a que la sección 512(h) DMCA no es aplicable a los proveedores de acceso. De acuerdo con esta resolución, en

---

[21] *In re Verizon Internet Servs., Inc..*, 240 F.Supp.2d 23 (D.D.C. 2003).
[22] *In re Verizon Internet Servs., Inc.*, 257 F.Supp.2d 244 (D.D.C. 2003).
[23] *Recording Industry Association Of America, Inc. contra Verizon Internet Services, Inc.*, 351 F.3d 1229 (C.D. 2003).

efecto, la sección 512(h) sólo es aplicable en relación a prestadores de servicios de alojamiento, *caching* y enlaces a materiales ilícitos, pero no con respecto a quien simplemente proporciona el acceso a Internet del que se sirven los usuarios para intercambiar ficheros a través de sistemas P2P. Al estimar este primer motivo del recurso, la Corte, desgraciadamente, no se vio obligada a entrar a conocer las alegaciones vertidas por el PSL cuestionando la constitucionalidad de la sección 512(h).

> Tres fueron los argumentos principales utilizados por la Corte de Apelación para afirmar que la sección 512(h) no se aplica a los proveedores de acceso. Primero, que los requisitos de la notificación de la sección 512(c)(3)(A), al que se remite la sección 512(h), demuestran que es necesaria la existencia de un material ilícito que pueda ser retirado por el PSL requerido, o el acceso al cual pueda ser eliminado por dicho PSL. Por consiguiente, si el PSL no puede retirar el material ilícito ni cortar el acceso al mismo, no se le puede hacer la notificación de la sección 512(c)(3)(A) ni, por tanto, se le puede requerir para identificar al supuesto infractor. El segundo argumento esgrimido por la Corte, complementario del anterior, es que la cancelación de la cuenta de acceso a Internet no equivale a la retirada del material ilícito o al corte del acceso al mismo al que hace referencia la sección 512(c)(3)(A). Se trata de una medida distinta, mucho más grave, además, que la Ley prevé específicamente para otros supuestos[24]. Finalmente, explica la Corte que no cabe recurrir al argumento de la interpretación subjetiva o teleológica del precepto, con base en lo que pudo pretender el Congreso cuando aprobó esta norma, ya que el problema del intercambio de obras y prestaciones protegidas a través de redes P2P no existía cuando se promulgó la DMCA, de modo que es imposible saber si la intención del Congreso era otorgarle o no el mismo tratamiento que a los supuestos de almacenamiento de material ilícito[25].

Un caso similar, resuelto en idéntico sentido por la Corte de Apelación del Octavo Circuito en enero de 2005, es el que enfrentó a la *RIAA contra Charter Communications, Inc.*[26]. Aquí la RIAA requirió a Charter Communications, Inc. para que revelara la identidad de 200 usuarios que, supuestamente, habían intercambiado fonogramas protegidos a través de redes P2P. El 3 de octubre de 2003 Charter se opuso judicialmente a este requerimiento. El 17 de noviembre de 2003 la Corte del Distrito Este de Missouri rechazó la oposición del PSL y le ordenó suministrar la información solicitada. Charter

---

[24] Como vemos, estos dos primeros argumentos responden a una interpretación literal de las secciones 512(h) y 512(c)(3)(A) DMCA.

[25] Curiosamente, este argumento bien podría haber dado pie a la aplicación analógica de la propia sección 512(h) al supuesto que aquí nos ocupa, en detrimento de la interpretación *a contrario*. En efecto, si la DMCA es anterior a la generalización de los sistemas P2P, es lícito acudir a la aplicación analógica de sus disposiciones para resolver los problemas jurídicos que aquéllos conllevan. Ello podría conducir a aplicar analógicamente la sección 512(h) a los proveedores de acceso de cuyo servicio se sirvan los usuarios para infringir derechos de propiedad intelectual a través de redes P2P. Piénsese que no se pretende la cancelación de la cuenta de acceso del usuario, sino únicamente la revelación de su identidad. En cualquier caso, no pueden pasarse por alto los importantes problemas que, desde el punto de vista de los derechos fundamentales de los usuarios, plantea una norma como la de la sección 512(h) DMCA.

[26] *In re Charter Communications, Inc.*, 393 F.3d 771.

recurrió en apelación esta resolución, pero, y aquí reside la especialidad del caso, no consiguió suspender la ejecución provisional de la orden de revelación de la identidad de los usuarios, por lo que se vio obligada a comunicársela a la RIAA. La Corte de Apelación del Octavo Circuito estimó el recurso interpuesto por el PSL, haciéndose eco de los argumentos utilizados por la Corte de Apelación del Distrito de Columbia en el caso Verizon. Ahora bien, como Charter ya había facilitado a la RIAA los datos requeridos, la Corte tuvo que ordenar a la asociación de productores fonográficos que devolviera al PSL toda la información obtenida a resultas del requerimiento, que destruyera cualquier registro que pudiera existir de dicha información y que se comprometiera a no utilizarla en lo sucesivo [27].

Tampoco la Corte de Apelación del Octavo Circuito tuvo necesidad de entrar a conocer las alegaciones de inconstitucionalidad de la sección 512(h) DMCA hechas por Charter. Sin embargo, no se resistió a manifestar sus dudas sobre la adecuación a la Constitución de una norma como la comprendida en este precepto. En este sentido, declaró lo siguiente [28]:

> «*A efectos de esta apelación, no abordamos los argumentos constitucionales presentados por Charter, pero sí debemos apuntar que esta Corte tiene cierta preocupación por el mecanismo del requerimiento de la sección 512(h). Comentamos, sin resolver al respecto, que este precepto puede invadir inconstitucionalmente las competencias del poder judicial mediante la creación de un marco legal a través del cual el Congreso,* via legge*, obliga a un oficial de un tribunal a emitir un requerimiento a través del cual ejercita una potestad judicial. Es más, creemos que puede defenderse la argumentación de Charter de que un requerimiento judicial de este tipo es una orden judicial que debe responder a un caso o a una controversia existente en el momento de su emisión*» [29].

Ciertamente, el gran problema que plantea la facultad que la sección 512(h) DMCA confiere a los titulares de derechos de requerir a los PSL información sobre la identidad de los supuestos infractores es que afecta a los derechos fundamentales de éstos sin control judicial alguno, ya que no es un juez quien autoriza el requerimiento, sino un oficial judicial, que se limita a constatar que se cumplen los requisitos formales exigidos por el citado procepto. La posibilidad de acceder a Internet y comunicarse a través de la red sin necesidad de revelar la propia identidad se ha relacionado, en efecto, con el de-

---

[27] A la sentencia referida acompaña el voto particular del magistrado Murphy, que disiente de la mayoría, por considerar que la sección 512(h) DMCA no excluye de su ámbito de aplicación a los PSL que prestan servicios de acceso a Internet y transmisión de datos, de modo que también a éstos se les puede requerir la revelación de la identidad de los usuarios que supuestamente infringen derechos de propiedad intelectual conforme a lo dispuesto en el indicado precepto.

[28] La traducción es propia.

[29] El magistrado Murphy, en su voto particular, señala, en contra de las dudas manifestadas por la mayoría, que esta disposición no es contraria al artículo III de la Constitución, porque la emisión de un requerimiento como el previsto por esta norma no es ejercicio de la función judicial, de modo que no tiene por qué emitirse en el marco de un litigio ya iniciado, y tampoco vulnera la Primera Enmienda, pues se establecen suficientes cautelas para asegurar que no se utiliza para coartar la libertad de expresión de los usuarios.

recho a expresarse anónimamente y, en esa medida, se ha considerado amparado por la Primera Enmienda.

> La Corte Suprema de los Estados Unidos ha declarado que la decisión de un autor de permanecer en el anonimato se enmarca dentro de la libertad de expresión protegida por la Primera Enmienda[30]. Las Cortes inferiores han extendido esta doctrina, dictada en relación al discurso polícitco, a otros contextos, y en concreto, a las comunicaciones a través de Internet, con base en la resolución de la Corte Suprema en el caso *Reno contra ACLU*[31], que expresamente declaró que el ámbito de aplicación de la Primera Enmienda cubre las comunicaciones a través de Internet. Así, la Corte del Distrito Norte de Georgia, en el caso *ACLU contra Millar*[32], anuló una Ley de este Estado que prohibía a quienes se expresan a través de Internet utilizar nombres falsos, reconociendo por primera vez el derecho de los usuarios de Internet a permanecer en el anonimato[33]. Si, además, tenemos en cuenta que, según la sentencia de la Corte Suprema en el caso *Eldred contra Ashcroft*[34], la Primera Enmienda no protege únicamente el discurso propio, sino también la difusión del discurso ajeno[35], nos encontramos con que, en principio, la Primera Enmienda ampara la difusión de forma anónima de obras y prestaciones ajenas.

Que la Primera Enmienda ampare el derecho al anonimato en Internet no quiere decir, sin embargo, que no sea posible instar la revelación de la identidad de un usuario que se sirve de la red para cometer infracciones. Ahora bien, en estos casos, antes de revelar la identidad del supuesto infractor, es necesario hacer una adecuada ponderación de los distintos intereses implicados, que deberá efectuar un juez.

---

[30] La sentencia de la Corte Suprema en el caso *Talley contra California*, 362 U.S. 60 (1960) fue la primera en reconocer que la libertad de expresión comprende el derecho a expresarse anónimamente. La siguieron las sentencias dictadas en los casos *McIntyre contra Ohio Elections Comm'n*, 514 U.S. 334 (1995), *Buckley contra American Constitucional Law Foundation*, 525 U.S. 182 (1999) y *Watchowe Bible y Tract Society of New York, Inc. contra Village of Stratton*, 536 U.S. 150 (2002). Las cuatro resoluciones protegen el derecho al anonimato en el discurso político, anulando normas jurídicas que, de una manera u otra, imponían la obligación de identificarse antes de difundir ideas políticas, sobre la base de que semejante obligación, unida al temor a represalias o reacciones acaloradas por parte de terceros, podría disuadir a las personas de expresarse libremente. Pero, como ha señalado VOGEL, M. S., «Unmasking "John Doe" defendants: the case against excessive hand-wringing over legal standards», *Oregon Law Review*, núm. 83, 2004, págs. 837-840, de estas sentencias no se desprende que el derecho al anonimato sea absoluto. Más bien al contrario, de ellas se colige que cuando concurre con otros intereses colectivos legítimos, este derecho puede restringirse en alguna medida, lo que viene corroborado por la sentencia de la Corte Suprema en el caso *Branzburg contra Hayes*, 408 U.S. 665 (1972), según la cual la Primera Enmienda no concede a los periodistas el derecho a preservar el anonimato de sus fuentes cuando son requeridos judicialmente para ello en el ámbito de un proceso penal. No existe, sin embargo, ninguna sentencia de la Corte Suprema que reconozca el derecho del autor de una conducta supuestamente ilícita a permanecer en el anonimato con base en la Primera Enmienda.

[31] 521 U.S. 844 (1997).

[32] 977 F.Supp 1228 (1997).

[33] A esta sentencia han seguido otras muchas. Así, por ejemplo, pueden verse *ACLU contra Jonson*, 4 F.Supp.2d 1029 (D.N.M. 1998), confirmada por la Corte de Apelación del Décimo Circuito en 1999 (194 F.3d 1149), *ApolloMedia Corp. contra Reno*, 19 F.Supp.2d 1081 (C.D.Cal. 1998), confirmada por la Corte Suprema en 1999 (526 U.S. 1061)...

[34] 537 U.S. 186 (2003).

[35] Si bien reconoce que, en este segundo caso, el nivel de protección puede ser menor.

Esto ha llevado a las Cortes estadounidenses a establecer distintos criterios para determinar cuándo procede la revelación de la identidad del supuesto infractor y cuándo no. Así, por ejemplo, en el caso *Columbia Insurance Co. contra SeesCandy.com* [36], relativo a una supuesta infracción de marca a través de Internet, la Corte del Distrito Norte de California señaló que sólo puede obligarse al PSL a revelar la identidad del usuario cuando no hay otra forma de averiguar su identidad, y siempre que el demandante cumpla los siguientes requisitos: (1) identificar suficientemente al supuesto infractor, a fin de que pueda determinarse la competencia del órgano judicial; (2) exponer todos los pasos seguidos para localizar al supuesto infractor, para demostrar que ha realizado un verdadero esfuerzo por descubrir su identidad; (3) acreditar la apariencia de buen derecho y (4) presentar una solicitud motivada que contenga una lista de los individuos que pueden revelar la identidad del supuesto infractor. De forma similar, la Corte del Circuito de Virginia resolvió, en el caso *In re Subpoena Duces Tecum to America Online, Inc.* [37], sobre una supuesta difamación a través de Internet, que sólo puede ordenarse a un PSL la revelación de la identidad de un usuario cuando de las alegaciones y pruebas presentadas por el demandante se desprenda que tiene una base para creer de buena fe que ha sido víctima de una conducta ilícita, a condición de que la información requerida sea indispensable para poder seguir adelante con el proceso por difamación. La Corte Superior de la División de Apelaciones de New Jersey, por su parte, en el caso *Dendrite International contra Doe No. 3* [38], también relativo a una supuesta difamación en la red, declaró que sólo por orden judicial puede obligarse a un PSL a revelar la identidad del presunto difamador, estableciendo varios requisitos que debe cumplir el demandante para obtener dicha orden (requisitos que, en el caso concreto, no se daban). En primer lugar, debe notificar al demandado, todavía desconocido, su solicitud de revelación de identidad, de modo que éste pueda hacer las alegaciones que estime oportunas para oponerse. La notificación se hará a través del PSL. En segundo lugar, debe indicar las concretas manifestaciones del demandado que considera difamatorias. En tercer lugar, debe acreditar su apariencia de buen derecho. Si el demandante ha cumplido los anteriores requisitos, la Corte deberá ponderar el derecho al anonimato del usuario y tanto la apariencia de buen derecho del demandante como la necesidad de que se revele la identidad del usuario, y resolver en consecuencia [39]. Por último, puede citarse también la sentencia de la Corte del Distrito de Washington en el caso *Doe contra 2TheMart.Com, Inc.* [40], en relación a la publicación por un usuario anónimo de mensajes en un foro de Internet acusando a la empresa demandante de fraude. Los criterios que la sentencia tuvo en cuenta para conceder la orden de revelación de identidad son los siguientes: (1) que el requerimiento sea de buena fe y no pretenda un propósito impropio; (2) que la información requerida esté relacionada con la esencia de la demanda o la defensa; (3) que la información sea directa y materialmente relevante para el eje de la demanda o la defensa; y (4) que la información perseguida no pueda obtenerse de otra fuente.

[36] 185 F.R.D. 573 (N.D.Cal. 1999).
[37] 52 Va. Cir. 26 (2000).
[38] 775 A.2d 756 (2001).
[39] En el mismo sentido, vid. *Immunomedics, Inc. contra Doe*, 775 A.2d, 773 (N.J.Super. Ct. App. Div. 2001), que, a diferencia de la anterior, ordena la revelación de la identidad del supuesto difamador.
[40] 140 F.Supp.2d 1088 (2001).

En conclusión, cabe destacar que los tribunales estadounidenses han declarado que los titulares de derechos no pueden recurrir a la vía de la sección 512(h) DMCA para obligar a los proveedores de acceso a revelar la identidad de quienes, a través de la conexión a Internet que aquéllos les facilitan, infringen derechos de propiedad intelectual en redes P2P[41]. Es más, hemos visto que la propia sección 512(h) es de dudosa constitucionalidad, dado que, en última instancia, permite restringir el derecho a expresarse anónimamente en Internet sin control judicial alguno. Ahora bien, el hecho de que los titulares de derechos de propiedad intelectual se hayan visto privados de la facultad de requerimiento prevista en la sección 512(h) no significa que carezcan de medios legales para averiguar la identidad de los infractores[42]. Pueden presentar demandas contra infractores desconocidos (*John Does lawsuits*), en el curso de las cuales podrán solicitar que se dicte una orden judicial requiriendo a los PSL para que identifiquen a los usuarios[43]. Los PSL deberán notificar dicho requerimiento a los propios usuarios para que éstos, si lo estiman oportuno, impugnen la validez o procedencia del mismo. A menos que prospere esta impugnación, el PSL tendrá que revelar el nombre de los supuestos infractores para que pueda proseguir el proceso contra ellos. Esta es la vía que han tenido que seguir, de hecho, los titulares de derechos tras la resolución de los casos Verizon y Charter. Desde entonces han venido interponiendo demandas contra infractores desconocidos, en el ámbito de las cuales solicitan a los proveedores de acceso implicados la identificación de los supuestos infractores[44].

En Canadá, no existiendo una norma equiparable a la sección 512(h) DMCA, los titulares de derechos de propiedad intelectual infringidos a través de redes P2P han utilizado directamente la vía de las demandas contra infractores desconocidos (*John Doe actions*), en el curso de las cuales han solicitado a los PSL la revelación de la identidad de los demandados.

Eso es lo que ha sucedido, por ejemplo, en el caso *BMG Canada Inc. y otros contra John Doe y otros*[45]. Los demandantes, productores fonográficos, tras detectar que 29 usuarios de Internet no identificados habían descargado y puesto a disposición del público a través de redes P2P más de 1000 fonogramas protegidos cada uno, iniciaron un procedimiento conjunto contra todos ellos bajo la forma de una *John Doe action*[46]. Posteriormente, ya en el marco

---

[41] Recientemente la Corte del Distrito de Carolina del Norte se ha sumado a esta línea jurisprudencial, declarando que la sección 512(h) no es aplicable a los proveedores de acceso a Internet. Vid. *In re subpoena to University of North Carolina at Chapel Hill*, 2005 WL 1027099 (M.D.N.C. 2005).

[42] Cfr. OWEN JR., T. P. y KATZ, A. B., «RIAA v. Verizon Internet Services, Inc.: Peer-to-peer networking renders section 512(h) subpoenas under the Digital Millenium Copyright Act obsolete», *Loyola of los Angeles Entertainment Law Review*, núm. 24, 2004, págs. 633-634.

[43] Lo permite la regla 45 de las *Federal Rules of Civil Procedure*.

[44] Vid. Sony Music Entertainment Inc. y otros contra Does 1-40, 326 F.Supp.2d 556 (S.D.N.Y. 2004), Elektra Entertainment Group, Inc. contra Does 1-9, 2004 WL 2095581 (S.D.N.Y. 2004).

[45] Vid. resolución de la Corte Federal de 31 de marzo de 2004 (2004 FC 488), revocada por la Corte Federal de Apelación el 19 de mayo de 2005 (2005 FCA 193).

[46] De hecho, la demanda iba dirigida contra «John Doe, Jane Doe and all those persons who are infringing copyright in the plaintiffs' sound recordings».

de este proceso, solicitaron que se requiriera judicialmente a los proveedores de acceso a Internet de los demandados para que revelaran las identidades de éstos, sobre la base de las reglas 233 a 238 de las normas procesales[47]. Los PSL implicados se opusieron a dicha orden judicial. La Corte Federal estimó la oposición. Interpuesto recurso de apelación por los demandantes, éste fue desestimado por la Corte Federal de Apelación, que, sin embargo, sí matizó de forma considerable la resolución de primera instancia.

Ambos órganos jurisdiccionales consideraron que semejante orden judicial puede dictarse al amparo de la regla 238 de las *Federal Court Rules*, que permite requerir a un tercero antes de la celebración del juicio para que proporcione cierta información necesaria para seguir adelante. Sin embargo, llegaron a distintas conclusiones en cuanto a si se daban o no los requisitos para que, en el caso concreto, procediera dictar esta orden.

Los requisitos que, según la Corte Federal, deben cumplirse para que proceda la orden de revelación de identidad del supuesto infractor son los siguientes. Para empezar, el solicitante tendrá que acreditar una apariencia de buen derecho, en el sentido de que es probable que la sentencia sobre el fondo del asunto sea condenatoria. En segundo lugar, la persona a la que se requiere debe estar involucrada de alguna manera en la cuestión litigiosa, y no ser un mero testigo inocente. En tercer lugar, la persona requerida debe ser la única fuente práctica de información disponible para los solicitantes. En cuarto lugar, la persona requerida debe ser compensada razonablemente por los gastos en que incurra para cumplir la orden, así como por las costas legales. Y, finalmente, tras una adecuada ponderación de los intereses en juego, la Corte tiene que llegar a la conclusión de que el interés público de que se revele la identidad del presunto infractor es mayor que el legítimo interés de los supuestos infractores de preservar su intimidad. De estos requisitos, la Corte Federal estimó que sólo se cumplían el segundo y, en su caso, el cuarto.

> En efecto, la Corte declaró que los demandantes no habían acreditado su apariencia de buen derecho, para lo cual realizó un análisis en profundidad sobre la licitud del intercambio de obras o prestaciones protegidas a través de redes P2P conforme al derecho canadiense. En su opinión, la descarga de un fonograma para uso privado no constituye infracción alguna, ni siquiera aunque se realice a partir de una copia ilícita. Por otro lado, no consideró suficientemente acreditado que los supuestos infractores distribuyeran o autorizaran la reproducción de fonogramas, que es lo que exige la Ley para que se entienda producida la infracción del *copyright*. En su opinión, se limitaban a colocar sus copias privadas en directorios compartidos, accesibles para otros usuarios conectados a esa red P2P, algo que, por sí solo, no le parece ilícito. Para la Corte Federal, dado que en el derecho canadiense no se considera «autorizar la reproducción» el mero hecho de facilitar al público medios para la obtención de copias, no es posible deducir tal autorización de la simple colocación de la copia privada en un directorio compartido. Algo similar ocu-

[47] *Federal Court Rules*, 1998, SOR/98-106.

> rre con la distribución. Según la Corte, la distribución requiere un acto positivo por parte del distribuidor, como enviar él mismo las copias o anunciar que se encuentran disponibles para su descarga pública. Si su conducta es meramente pasiva, consistente en permitir que otros copien, no hay distribución propiamente dicha. Recordaba la Corte, asimismo, que en el derecho canadiense no existe todavía un derecho de puesta a disposición, que, de existir, es el que, en su caso, podría haber sido infringido. Por último, rechazó que pudiera entenderse cometida una infracción secundaria de los derechos de propiedad intelectual, pues semejante infracción exige el conocimiento por parte del infractor secundario de que facilita a los infractores directos los medios para infringir derechos, lo que no se había probado.
>
> Por lo que respecta al tercer requisito, la Corte Federal consideró que no se había acreditado suficientemente que la única vía para averiguar la identidad de los supuestos infractores fuera el requerimiento a sus proveedores de acceso.
>
> Finalmente, en cuanto al quinto requisito, la Corte Federal resolvió que, en vista de que la información solicitada no era reciente y podía no corresponderse con la realidad [48], el interés de privacidad de los 29 supuestos infractores pesaba más que el interés público de revelación de sus identidades.

La Corte Federal de Apelación mantuvo el fallo desestimatorio de primera instancia, pero corrigió algunos de los argumentos esgrimidos por el tribunal *a quo* [49]. La principal enmienda a la fundamentación jurídica de la resolución de la Corte Federal se centra en el primero de los requisitos expuestos. En opinión del tribunal de apelación, para emitir una orden de revelación de la identidad del supuesto infractor en una fase tan incipiente del proceso, no puede requerirse el *fumus boni iuris*. Tal exigencia sería excesiva en un momento en que ni siquiera se sabe quién puede ser el infractor. Lo que debe exigirse es que el solicitante tenga una acción legítima, o de buena fe, contra el supuesto infractor. En definitiva, que la finalidad de la información solicitada no sea otra que poder interponer una demanda por supuesta infracción de su *copyright*.

La Corte de Apelación matiza también el último de los requisitos exigidos por la Corte Federal, para lo cual parte de la base de que la legislación canadiense sólo permite la revelación de datos personales ajenos cuando lo consiente el propio afectado o cuando así lo ordena la autoridad competente [50]. Para determinar si procede una orden de revelación de datos personales, continúa, hay que ponderar los distintos intereses en juego: el interés de privacidad del afectado frente al interés público de que se desvelen sus datos a los exclusivos fines del proceso. Según la Corte de Apelación, cuando el demandante prueba

---

[48] En concreto, las direcciones IP se habían conseguido entre octubre y diciembre de 2003, pero la solicitud de revelación de la identidad de los usuarios no se había hecho hasta el 11 de febrero de 2004.

[49] De hecho, reconoció expresamente el derecho de los demandantes a solicitar nuevamente la emisión de una orden judicial de revelación de la identidad de los supuestos infractores teniendo en cuenta los fundamentos jurídicos de esta resolución.

[50] Sección 7(3) de la Personal Information Protection and Electronic Documents Act.

tener una acción legítima por supuesta infracción de sus derechos de propiedad intelectual contra una persona cuya identidad desconoce, tiene también el derecho a que se revele esa identidad a fin de poder ejercitar la acción pertinente. Sin embargo, antes de dictar la orden de revelación de identidad, la autoridad judicial debe cerciorarse de que el derecho a la intimidad del afectado se invade lo mínimo posible. Si, en el caso concreto, existe riesgo de que la información suministrada no sea fiable, por haber transcurrido un lapso de tiempo excesivo entre la fecha de solicitud de la identidad de los supuestos infractores y la fecha en que los demandantes recopilaron los datos necesarios para averiguar dicha identidad, la medida deberá ser denegada, para evitar la posibilidad de que se desvelen datos personales correspondientes a personas inocentes.

En síntesis, la situación en Estados Unidos y en Canadá es muy similar. Para obligar a los proveedores de acceso a revelar la identidad de quienes infringen derechos de propiedad intelectual a través de redes P2P es necesario instar la emisión de una orden judicial en el marco de una *John Doe action*. Para que proceda dictar esta orden, el solicitante tendrá que acreditar la necesidad de los datos requeridos para la continuación del procedimiento, así como la imposibilidad de obtenerlos por otras vías, proporcionar la información imprescindible para que el PSL pueda identificar al supuesto infractor, comprometerse a compensar al PSL los gastos de cumplimiento de la orden y obligarse a no utilizar los datos resultantes para una finalidad distinta de la continuación del proceso por infracción de derechos de propiedad intelectual.

IV. LA OBLIGACIÓN DE LOS PRESTADORES DE SERVICIOS EN LÍNEA DE REVELAR LA IDENTIDAD DE LOS USUARIOS QUE COMETEN INFRACCIONES DE DERECHOS DE PROPIEDAD INTELECTUAL EN EUROPA. EL DERECHO DE INFORMACIÓN DE LA DIRECTIVA 2004/48/CE

1. Los derechos a la intimidad y a la protección de datos de carácter personal como obstáculos a la revelación de la identidad de los usuarios de Internet por parte de los PSL

Si en los Estados Unidos las reticencias de los PSL a revelar la identidad de los usuarios que supuestamente infringen derechos de propiedad intelectual a través de Internet se fundan, desde el punto de vista constitucional, en el derecho de éstos a expresarse anónimamente a través de la red, en Europa son los derechos a la intimidad y a la protección de datos de carácter personal los mayores obstáculos con los que se pueden encontrar los titulares de derechos para averiguar la identidad de los presuntos infractores.

La regulación del derecho a la protección de datos personales está muy armonizada en el seno de la Unión Europea, y ello por dos razones. Por un lado, porque se ha pretendido asegurar a los ciudadanos comunitarios un nivel de

protección mínimo en un ámbito en el que, hasta hace relativamente poco tiempo, estaban muy desprotegidos. Por otro lado, porque, dado el valor económico que han adquirido estos datos para las empresas que operan en el ámbito del Mercado Común, se ha hecho necesario establecer un marco regulador homogéneo a fin de eliminar las trabas al tráfico de estos datos entre los países de la Comunidad. Ese marco está compuesto principalmente por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas [51].

En relación al tema que nos ocupa, ya en 1997, el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales, órgano consultivo independiente creado al amparo del artículo 29 de la Directiva 95/46/CE, manifestó su preocupación por asegurar el anonimato a los usuarios de Internet, como única vía para proteger su intimidad [52]. Ahora bien, consciente de que Internet puede ser el medio para la comisión de ilícitos civiles y penales, mantenía asimismo que el derecho al anonimato en Internet no podía ser absoluto [53]. Como vemos, quedaban sentadas ya las bases para un debate que no ha comenzado a plantearse hasta ahora, cuando la generalización de las infracciones a través de redes P2P ha hecho necesario para los titulares de derechos de propiedad intelectual conocer la identidad de los usuarios presuntamente infractores, a fin de poder demandarlos. Y en este debate, las diversas partes implicadas han adoptado la postura que más conviene a sus intereses. Así, mientras que los usuarios, y, en su nombre, los PSL, se amparan en ese derecho al anonimato en Internet para mantener oculta la identidad de los supuestos infractores, los titulares de derechos se aferran al carácter relativo del derecho al anonimato, que no puede servir de escudo para quienes no pretenden otra cosa que violar impunemente los derechos de terceros.

Más allá de posiciones de principios, para dar una respuesta jurídicamente fundada al mencionado problema hay que resolver una cuestión previa, cual es si la dirección IP que una persona utiliza para conectarse a Internet cons-

---

[51] Que vino a derogar la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 17 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones.

[52] Vid. Recomendación 3/97, sobre el anonimato en Internet, adoptada el 3 de diciembre de 1997 (XV D/5022/97 ES final).

[53] Señalaba en concreto: «La posibilidad de anonimato no siempre resulta oportuna. A la hora de determinar en qué circunstancias lo es y en cuáles no, debe contrapesarse cuidadosamente los derechos fundamentales a la intimidad y a la libertad de expresión con otros objetivos importantes de orden público, entre ellos la prevención de la delincuencia. Las restricciones legales que pueden imponer los Gobiernos al derecho de mantener el anonimato o a los medios técnicos utilizados al efecto (p. ej., disponibilidad de productos de codificación) deberán en todo momento ser proporcionados y limitarse a lo estrictamente necesario para proteger un interés general específico en una sociedad democrática».

tituye un dato de carácter personal conforme al derecho comunitario. Esta misma pregunta se la hizo el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales. Y la respuesta fue afirmativa [54].

> «Un tercero puede llegar a averiguar la dirección IP dinámica de un usuario pero no ser capaz de relacionarla con otros datos que le permitan identificarlo. Obviamente, resulta más sencillo identificar a los usuarios de Internet que utilizan direcciones IP estáticas.
>
> Sin embargo, en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como *cookies* con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet que permite su identificación.
>
> Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, este documento parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, en Internet se tratan grandes cantidades de información personal para la cual son de aplicación las Directivas sobre protección de datos» [55].

Como vemos, el Grupo de Trabajo considera que las direcciones IP son datos personales porque es posible, partiendo de ellas, averiguar la identidad del usuario de Internet que está detrás, así como otros muchos datos, tales como las páginas *web* que visita, los foros en los que se comunica, etc. En efecto, de acuerdo con el artículo 2 a) de la Directiva 95/46/CE, lo decisivo a la hora de calificar una dirección IP como dato personal es la posibilidad de identificar a su titular a partir de ella [56]. Se entiende que la persona a la que hace referencia el dato es identificable cuando puede determinarse su identidad directa o indirectamente. Según precisa el considerando 26 de la propia Directiva, «para determinar si una persona es identificable, *hay que considerar el conjunto de medios que puedan ser razonablemente utilizados por el responsable del tratamiento, o por cualquier otra persona, para identificar al interesado*». Para los proveedores de acceso, por lo tanto, las direcciones IP son datos personales porque pueden, por medios propios sin duda razonables, determinar la identidad del usuario que se conectó a Internet a través de ellas. Para

---

[54] Cfr. *Privacidad en Internet*, documento de trabajo redactado por el Grupo de Trabajo sobre Protección de datos del artículo 29 de la Comisión Europea, adoptado el 21 de noviembre de 2000, 5063/00/ES/FINAL, pág. 13.

[55] Cfr. *Privacidad en Internet*, documento adoptado el 21 de noviembre de 2000, 5063/00/ES/FINAL, pág. 23.

[56] Dato de carácter personal, según el artículo 2 a) de esta Directiva, es «toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social».

el titular de derechos de propiedad intelectual que recaba esas direcciones IP a fin de averiguar quiénes infringen derechos de propiedad intelectual a través de Internet, se trata de datos personales, pues a partir de ellas puede identificar a los usuarios con la colaboración de los PSL.

> De conformidad con el considerando 26 de la Directiva 95/46/CE, es irrelevante que el titular de los derechos de propiedad intelectual no pueda por sí solo identificar al usuario que está detrás de una dirección IP para calificar ésta como dato personal. Ni siquiera en el hipotético caso de que consideráramos que la solicitud de una orden judicial de revelación de esa identidad no constituye un medio razonable para identificar a dicho usuario podríamos llegar a tal conclusión. Y ello porque el considerando 26 es claro cuando señala que un dato tiene carácter personal cuando puede ser razonablemente utilizado por el responsable del tratamiento *o por cualquier otra persona* (en nuestro caso, el PSL) para identificar al interesado.

El hecho de que las direcciones IP constituyan datos personales implica que su tratamiento no es libre, sino que está sometido a la normativa comunitaria sobre protección de estos datos cuando ese tratamiento se realiza total o parcialmente por medios automáticos o cuando, siendo el tratamiento manual, se trata de datos contenidos en un fichero o destinados a su inclusión en un fichero. Ello suscita la duda de si la obtención por parte de los titulares de derechos de propiedad intelectual de las direcciones IP de los supuestos infractores puede considerarse un acto ilícito[57]. En principio, parece que no. Según el artículo 7 f) de la Directiva 95/46/CE, los Estados miembros autorizarán el tratamiento de datos, aun sin el consentimiento del afectado, cuando sea necesario «para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado». La defensa de los propios derechos de propiedad intelectual es, sin duda, un interés legítimo, para cuya satisfacción es lícito recopilar las direcciones IP de los usuarios de Internet que supuestamente infringen esos derechos. Por otro lado, resulta evidente que, en este contexto, el derecho comunitario no obliga a los titulares de los derechos infringidos a comunicar a los presuntos infractores que se han recopilado sus datos personales con vistas a demandarlos. Así se desprende de los artículos 11.2 y 13.1 g), ambos de la Directiva 95/46/CE.

> El artículo 11.1 de la Directiva establece el derecho del interesado a ser informado de que se han recabado sus datos, así como de la identidad del responsable del tratamiento de los mismos y de la finalidad a que vayan a ser destinados. Sin embargo, tanto el artículo 11.2 como el artículo 13 de la misma Directiva establecen excepciones a esta norma, en el primer caso de incorporación obligatoria para los Estados miembros, en el segundo, de transposición facultativa. El artículo 11.2 excepciona de la anterior obligación,

[57] Lo habitual, en el ámbito en que nos movemos, es que la recolección de las direcciones IP de los supuestos infractores por los titulares de derechos se realice automáticamente, por lo que estaremos en el ámbito de aplicación de la Directiva.

> entre otros supuestos, aquel en el que la información al interesado es imposible o exija esfuerzos desproporcionados. En nuestro caso, dado que el titular de los derechos desconoce la identidad del infractor, no le puede comunicar la obtención de sus datos personales. El artículo 13, por su parte, faculta a los Estados miembros para limitar el alcance de las obligaciones y derechos del artículo 11.1 cuando tal limitación constituya una medida necesaria para la protección del propio interesado *o de los derechos y libertades de otra persona*, que es el caso que nos ocupa.

La Directiva 2002/58/CE no ha alterado la situación descrita, por más que, a partir de la misma, la dirección IP, así como el día y la hora de la conexión a Internet, en tanto que datos de tráfico, queden amparados por la confidencialidad de las comunicaciones [58]. En este sentido, aunque el artículo 5.1 de la Directiva reconoce el derecho de los usuarios a la confidencialidad de sus comunicaciones y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público, no puede pasarse por alto que el secreto de las comunicaciones es siempre en relación con terceros, no con las propias partes de la comunicación. Así lo pone de manifiesto el artículo 5.1, cuando precisa que los Estados miembros, en particular, «prohibirán la escucha, la grabación, el almacenamiento y otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas *por personas distintas de los usuarios*, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15» [59]. En la medida en que los titulares de derechos obtengan la dirección IP del supuesto infractor al comunicarse directamente con él a través de la red P2P, no contravendrán lo dispuesto por el artículo 5.1 de la Directiva 2002/58/CE.

Por tanto, el derecho comunitario no prohíbe la recopilación de direcciones IP de usuarios de Internet por parte de los titulares de derechos de propiedad intelectual, siempre que esos datos estén destinados a proteger sus derechos frente a las infracciones que dichos usuarios cometan a través de la red. Ahora bien, dado que tanto las direcciones IP como las identidades de sus usuarios son datos personales, los PSL no pueden sin más revelar a los titulares de los derechos infringidos los nombres de quienes se han conectado a Internet usando esas direcciones IP, tal y como se desprende del artículo 7 de la Directiva 95/46/CE. Lo que no quiere decir que los titulares de derechos queden desprotegidos, pues el artículo 7 f) ampara la comunicación de datos personales a terceros siempre que sea para satisfacer los intereses legítimos

---

[58] En efecto, conforme al artículo 2 b), se considerarán datos de tráfico cualesquiera tratados a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma. El considerando 15 de la Directiva precisa un poco más el concepto de datos de tráfico, al indicar que los datos de tráfico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión...

[59] El énfasis es mío.

de estos últimos. Por consiguiente, previa ponderación de los distintos intereses involucrados, cuya realización corresponderá a la autoridad judicial competente, podrán los titulares de derechos obtener la identidad de los supuestos infractores de los PSL[60].

2. Los artículos 15.2 y 18 de la Directiva sobre comercio electrónico y su incidencia sobre las legislaciones de los Estados miembros

Hemos visto que, de acuerdo con las Directivas relativas a la protección de datos de carácter personal, los titulares de derechos de propiedad intelectual pueden recabar la información relativa a la supuesta infracción, incluida la dirección IP del supuesto infractor, a efectos de emprender las acciones legales oportunas contra el supuesto infractor; pero también que los PSL no pueden revelar la identidad de los supuestos infractores a menos que medie una orden judicial en tal sentido. La cuestión es, entonces, si los titulares de derechos de propiedad intelectual tienen derecho, de conformidad con las normas comunitarias, a obtener semejante orden judicial.

La primera Directiva comunitaria que, siquiera de forma indirecta, hace referencia a esta cuestión, es la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, más conocida como la Directiva sobre el Comercio Electrónico (DCE)[61].

Su artículo 15.2 faculta a los Estados miembros para obligar a los PSL a comunicar a las autoridades competentes, a solicitud de éstas, información

---

[60] En esta línea, aunque mostrándose más desconfiado por lo que a las actividades de autotutela de los titulares de derechos se refiere, el Grupo de Trabajo sobre protección de datos ha puesto de manifiesto cómo la reutilización de los datos personales de los usuarios que se encuentran a disposición del público en la red puede ser un acto ilícito. Recuerda, en este sentido, que los contenidos de los ficheros y bases de datos, sean públicos o no, sólo pueden ser tratados y utilizados para fines compatibles con aquél para el que los datos se recopilaron. Recuerda asimismo que los PSL no pueden ceder esos datos a terceros sin el consentimiento del interesado; únicamente puede comunicar esos datos a las autoridades competentes cuando se den las circunstancias previstas en la Ley. Cfr. *Working document on data protection issues related to intellectual property rights*, adoptado el 18 de enero de 2005, 10092/05/EN, WP 104, pág. 7.

[61] Téngase en cuenta, eso sí, que la Directiva sobre Comercio Electrónico señala en su considerando 14: «La protección de las personas con respecto al tratamiento de datos de carácter personal se rige únicamente por la Directiva 95/46/CE y la Directiva 97/66/CE, que son enteramente aplicables a los servicios de la sociedad de la información (...) y, por tanto, no es necesario abordar este aspecto en la presente Directiva» [esto se plasma en el art. 1.5 b) DCE, de acuerdo con el cual «la presente Directiva no se aplicará a cuestiones relacionadas con servicios de la sociedad de la información incluidas en las Directivas 95/46/CE y 97/66/CE»]. Y continúa: «la aplicación y ejecución de la presente Directiva debe respetar plenamente los principios relativos a la protección de datos personales, en particular en lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios, la presente Directiva no puede evitar el uso anónimo de redes abiertas como Internet». Ello debe entenderse, por lo que aquí nos interesa, en el sentido de que la Directiva sobre Comercio Electrónico se limita a establecer en qué casos puede dictarse una orden judicial de revelación de la identidad del usuario que en un momento dado se conectó a Internet a través de una determinada dirección IP.

que les permita identificar a los destinatarios de los servicios con los que aquéllos hayan celebrado acuerdos de almacenamiento. Este precepto, que sin duda es el antecedente más inmediato del artículo 8 DRDPI, al que luego se hará alusión, no es todo lo útil que pudiera parecer para la causa de los titulares de los derechos, y ello por dos motivos. Primero, porque se trata de una norma facultativa, y no imperativa. Los Estados miembros no estaban obligados a incorporar semejante derecho de información a sus ordenamientos internos. Segundo, porque, como se aprecia claramente, no está pensando en los proveedores de acceso, que son los únicos que pueden identificar a quien ha usado una dirección IP en una red P2P, sino en quienes prestan servicios de almacenamiento [62].

Si el artículo 15.2 DCE, por sí solo, no sirve a los intereses de los titulares de derechos, no puede decirse lo mismo del artículo 18 DCE, que impone a los Estados miembros la obligación de velar «por que los recursos judiciales existentes en virtud de la legislación nacional en relación con las actividades de servicios de la sociedad de la información permitan adoptar rápidamente medidas, incluso medidas provisionales, destinadas a poner término a cualquier presunta infracción y a evitar que se produzcan nuevos perjuicios contra los intereses afectados». Como vemos, el tenor de este precepto es amplísimo, al referirse a cualquier recurso judicial tendente a la cesación de la presunta infracción y a evitarle al perjudicado nuevos daños. Comprende, por lo tanto, no sólo medidas provisionales (medidas cautelares anticipatorias) y definitivas de cesación, sino también aquellas otras sin las cuales esa cesación provisional o definitiva sería imposible. Y aquí hay que incluir, sin ninguna duda, aquellas medidas necesarias para identificar al infractor, como presupuesto para poder instar la cesación cautelar o definitiva de la conducta ilícita.

> Podría argüirse que, por aplicación del principio de especialidad, quedan fuera del artículo 18 DCE las medidas judiciales dirigidas a averiguar la identidad del presunto infractor, ya que a ellas se refiere el artículo 15.2 DCE. Sin embargo, la distinta finalidad de ambos preceptos excluye la aplicación del principio de especialidad. El artículo 15.2, en efecto, contempla una norma de incorporación facultativa para los Estados miembros destinada, en última instancia, a averiguar la identidad de los responsables de actividades ilícitas. El artículo 18, por su parte, establece una norma de incorporación obligatoria para los Estados miembros, dirigida a poner fin a las infracciones cometidas a través de la red. Así, cuando la averiguación de la identidad del supuesto infractor no es esencial para que prospere la medida de cesación, estamos en el ámbito del artículo 15.2. Es lo que sucede, por ejemplo, cuando la presunta infracción consiste en poner a disposición del público una obra o prestación protegida a través de una página *web*. En este caso, para obtener la cesación el titular de los derechos no necesita conocer la identidad del usuario que comunica públicamente la obra o prestación protegida a través de Internet, pues tiene siempre la posibilidad de dirigirse

[62] Cfr. GUIBAULT, L., «Vous qui téléchargez des oeuvres de l'Internet, pourrait-on savoir qui vous êtes?», *Revue du Droit des technologies de l'information*, núm. 18, 2004, pág. 23.

> contra el prestador del servicio de alojamiento, por más que éste pueda no ser responsable de la infracción conforme al artículo 14 DCE (vid., en concreto, considerando 45 y art. 14.3, ambos de la DCE). Por el contrario, cuando la averiguación de la identidad del infractor es presupuesto indispensable para conseguir la cesación de la conducta ilícita, entonces estamos en el ámbito del artículo 18 DCE, y no del artículo 15.2. Tal es el caso de las infracciones de derechos a través de redes P2P, ya que, como el servidor no almacena los archivos ilícitos, no puede ser el destinatario de la medida de cesación (no puede retirarlos, o cortar el acceso a los mismos)[63]. En este caso, sólo si se demanda al usuario infractor puede conseguirse la cesación, y para ello es absolutamente necesaria su previa identificación por parte del proveedor de acceso, al amparo del artículo 18 DCE. De hecho, esta interpretación podría explicar que el artículo 15.2 se refiera a prestadores de servicios de almacenamiento, y no a proveedores de acceso.

Al artículo 18 DCE, y para el concreto ámbito de la propiedad intelectual, se ha venido a añadir el artículo 8.2 de la Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derecho afines a los derechos de autor en la sociedad de la información (DDASI). Según este artículo, «cada uno de los Estados miembros adoptará las medidas necesarias para garantizar que los titulares de los derechos cuyos intereses se vean perjudicados por una actividad ilícita llevada a cabo en su territorio puedan interponer una acción de resarcimiento de daños y perjuicios y/o solicitar medidas cautelares y, en su caso, que se incaute el material ilícito y los dispositivos, productos o componentes a que se refiere el apartado 2 del artículo 6». Como el artículo 18 DCE; el artículo 8.2 DDASI destaca por su amplitud en cuanto a las medidas contempladas, entre las que, desde luego, cabe incluir la de revelación de la identidad del infractor. Esta medida, en efecto, es necesaria para garantizar que el titular de los derechos infringidos pueda interponer una acción de daños y perjuicios, en la medida en que ésta sólo cabe contra el responsable de la infracción, que, normalmente, no será el prestador de los servicios de los que se vale el usuario de Internet para cometer la infracción (vid. arts. 12-14 DCE), sino el infractor directo, a quien sólo se puede demandar si se conoce su identidad.

En el ámbito de las legislaciones nacionales, la incorporación de estas Directivas a los ordenamientos internos de los Estados miembros de la Unión Europea ha permitido a los titulares de derechos, en algunos casos, obtener de las autoridades judiciales competentes órdenes de revelación de la identidad de los supuestos infractores dirigidas contra los proveedores de acceso.

---

[63] Es cierto que, en teoría, cabría una medida consistente en exigirle al proveedor de acceso que dejara de prestar tal servicio al supuesto infractor. Pero no puede obviarse el hecho de que cualquier medida judicial destinada a poner fin a una infracción tiene que ser proporcionada, y mientras que lo es retirar el archivo ilícito, o cortar el acceso al mismo, no lo es dejar sin servicio al supuesto infractor sin demandarle, en la medida en que se le priva también de usos lícitos de su cuenta de acceso a Internet.

Así, en el Reino Unido se han dictado ya órdenes judiciales, a instancia de productores fonográficos, para que los PSL revelen la identidad de quienes supuestamente han infringido los derechos de aquéllos a través de redes P2P, a los solos efectos de que se inste la acción civil correspondiente. Así ha sucedido en los casos *Universal Island Records Ltd. y otras contra NTL Group Ltd. y otros*[64] y *Emi Records y otros contra Eircom Ltd y BT Communications Ireland Ltd*.[65].

> La vía en ambos casos ha sido la llamada *Norwich Pharmacal order*. De acuerdo con la doctrina sentada por la Cámara de los Lores en el caso *Norwich Pharmacal Co. contra Customs and Excise Comrs*[66], cuando, sin culpa propia, una persona se ve involucrada[67] en actos dañosos realizados por otros, de tal manera que facilita la conducta ilícita de éstos, no incurre en responsabilidad, pero queda obligada a asistir al perjudicado, proporcionándole toda la información de que disponga, incluida, en su caso, la relativa a la identidad de los responsables. Entre los requisitos que deben cumplirse para ordenar al intermediario la identificación del infractor se suelen señalar los siguientes: la tenencia por parte del solicitante de una acción legítima (de buena fe) contra el supuesto responsable[68]; la existencia de alguna relación entre el presunto responsable y aquel a quien se solicita la información, que determine el conocimiento por parte de éste de los datos que se le requieren[69]; la imposibilidad de obtener la información de otra fuente; y, finalmente, la posibilidad que el solicitante compense al requerido cualquier perjuicio que la orden le ocasione[70].

En Holanda, el Tribunal de Primera Instancia de Utrecht, en un auto fechado el 12 de julio de 2005[71], declaró que, de acuerdo con la sección 6:196c del Código Civil holandés, que incorpora el artículo 15.2 DCE, los tribunales civiles pueden requerir a los prestadores de servicios de la sociedad de la información, a instancia de los titulares de derechos de propiedad intelectual, para que revelen la identidad de quienes infringen tales derechos a través de redes P2P. Dicha orden sólo podrá dictarse, sin embargo, cuando los titulares de derechos de propiedad intelectual hayan respetado las disposiciones legales en materia de protección de datos de carácter personal al recopilar la información necesaria para averiguar la identidad de los supuestos infractores.

> En el caso concreto, el Tribunal denegó la orden porque los titulares de derechos, para obtener dichos datos, habían contratado a una empresa nor-

---

[64] Orden de la *High Court of Justice (Chancery Division)* de 14 de octubre de 2004.
[65] Orden de la *High Court of Justice (Commercial)* de 8 de Julio de 2005.
[66] [1974] A.C. 133 (H.L.).
[67] Ya sea por una acción voluntaria por su parte o simplemente por cumplir con alguna obligación.
[68] A fin de asegurar que las solicitudes de revelación no se hagan frívolamente y sin justificación.
[69] No procederá la orden si éste es un mero testigo inocente que nada ha tenido que ver con la infracción.
[70] Sobre el funcionamiento de la *Norwich Pharmacal order*, puede consultarse RYAN, C., «Human rights and intellectual property», *European Intellectual Property Review*, 2001, págs. 526-527.
[71] En el caso *BREIN y otros contra U.P.C. Nederland B.V. y otros*.

> teamericana dedicada a esta actividad, la cual no se había atenido a las normas del derecho europeo, sino a las del derecho estadounidense, menos protector, para tratar los datos personales de los usuarios. Por otro lado, parece que se habían recabado más datos de los necesarios para poder identificar a los supuestos infractores y emprender acciones legales contra ellos.
>
> En cualquier caso, la resolución del Tribunal de Utrecht es destacable por dos motivos. Primero, porque expresamente se plantea si los tribunales civiles son competentes para ordenar a los proveedores de acceso, al amparo del artículo 15.2 DCE, que revelen la identidad de los usuarios de Internet, llegando a la conclusión de que, dado que el artículo 15.2 no precisa cuál es la autoridad competente para dictar este tipo de órdenes, puede serlo cualquiera, tanto civil como penal, según se colige asimismo del artículo 12.3 y del considerando 25 DCE[72].
>
> Y segundo, porque, aun partiendo de la consideración de las direcciones IP como datos personales de los usuarios de Internet, reconoce la licitud de su recopilación por los titulares de derechos de propiedad intelectual, cuando son necesarias para poder ejercitar una acción por la supuesta vulneración de tales derechos en redes P2P, siempre que el tratamiento de esos datos haya sido conforme con lo dispuesto por la legislación sobre protección de datos de carácter personal.

En Alemania, aunque todavía no se ha establecido en el ámbito civil la obligación de los PSL de revelar la identidad de quienes realizan actividades ilícitas valiéndose de sus servicios, sí es posible obtener órdenes judiciales en este sentido en el ámbito del proceso penal. Ello ha llevado a la industria discográfica a instar la apertura de procesos penales contra infractores cuya identidad se desconoce a fin de que la Fiscalía obtenga de los PSL el nombre de los mismos. Posteriormente, una vez que la identidad de los infractores se ha revelado en el ámbito penal, los titulares de derechos han ejercitado paralelamente acciones civiles contra los mismos[73].

En otros países, aunque todavía no ha habido un pronunciamiento judicial al respecto, la legislación ampara este tipo de órdenes judiciales de revelación de la identidad de los usuarios de Internet en el ámbito de procesos civiles por infracción de derechos de propiedad intelectual. Así, en Francia,

---

[72] Como vemos, el Tribunal se basa en ciertas disposiciones de la DCE en las que no se limita la competencia a los tribunales penales. Así, el artículo 12.3 establece que el artículo 12 «no afectará a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exija al prestador de servicios que ponga fin a una infracción o que la impida», lo que reiteran, en sus respectivos ámbitos, los artículos 13.2 y 14.3 DCE. La cita del considerando 25 se justifica por que hace referencia expresa a los tribunales civiles. De acuerdo con el mismo, «los tribunales nacionales, incluidos los tribunales civiles, que conocen de controversias de Derecho privado pueden adoptar medidas que establecen excepciones a la libertad de prestar servicios en el marco de la sociedad de la información de conformidad con las condiciones establecidas en la presente Directiva».

[73] LEWINSKI, S. VON, «Certain legal problems related to the making available of literary and artistic works and other protected subject matter through digital networks», *e-Copyright Bulletin*, enero-marzo de 2005, pág. 10.

el primer párrafo del artículo 6.II de la *Loi 2004/575 pour la confianse dans l'économie numérique*, de 21 de junio de 2004, en relación con el artículo 6.I.1 del mismo cuerpo legal, obliga a los proveedores de acceso a conservar los datos de la conexión, a fin de permitir la identificación de quien haya contribuido a la creación de los contenidos comunicados a través de ese acceso. Complementariamente, el párrafo tercero del mismo artículo 6.II faculta a la autoridad judicial (no precisa cuál, por lo que puede ser del orden jurisdiccional civil) para requerir a los proveedores de acceso la comunicación de esos datos[74]. Lógicamente, en el caso que nos ocupa, dicho requerimiento no se hará si no es a instancia del titular de los derechos infringidos. En este ámbito, y para facilitar la defensa de los derechos de propiedad intelectual, el artículo 9.4 de la *Loi 78-17 relative à l'informatique, aux fichiers et aux libertés*, de 6 de junio de 1978, tras la modificación introducida por la Ley 2004-801, de 6 de agosto de 2004, permite a las entidades de gestión de derechos de propiedad intelectual el tratamiento de datos personales para la defensa de los derechos que gestionan frente a eventuales infracciones. En este contexto, y con base en el citado precepto, la *Commission Nationale de l'Informatique et des Libertés* (CNIL) autorizó a una entidad de gestión[75], mediante resolución de 24 de marzo de 2005, la utilización de un sistema automatizado de detección de infracciones cometidas por los usuarios de redes P2P, el cual, entre otras cosas, recopila las direcciones IP de los supuestos infractores[76].

> La cuestión no está tan clara en aquellos países que se han limitado a reproducir lo dispuesto por el artículo 15.2 DCE. Al establecer la obligación de los PSL de comunicar a las autoridades competentes, a instancia de éstas, la información necesaria para identificar a los usuarios con los que han firmado contratos de almacenamiento, parecen eximir de dicha obligación a los proveedores de acceso. Es lo que ocurre en Bélgica (art. 21.2 de la *Loi sur certains aspects juridiques des services de la société de l'information*, de 11 de marzo de 2001), Italia (art. 17.2 b] del Decreto Legislativo n. 70, de 9 de abril de 2003) o Portugal (art. 13 b] del Decreto-Lei n. 7/2004, de 7 de enero de 2004).

3. El derecho de información en la Directiva relativa al respeto de los derechos de propiedad intelectual

Con el propósito de atajar la piratería, se aprobó en abril de 2004 la Directiva 2004/48/CE, relativa al respeto de los derechos de propiedad intelectual (DR-DPI), que prevé entre sus medidas el denominado «derecho de información», en el que pueden ampararse los titulares de derechos de propiedad intelectual

---

[74] El párrafo quinto de este artículo remite a un Decreto del Consejo de Estado (previo dictamen de la Comisión Nacional de la Informática y las Libertades) la definición de los datos a que hace referencia este artículo, así como la determinación de la duración y las modalidades de su conservación.

[75] En concreto, al *Syndicat des Editeurs de Logiciels de Loisiers*.

[76] Vid. la página *web* de la CNIL: <http://www.cnil.fr>.

para obtener de los prestadores de servicios de la sociedad de la información la identidad de quienes infringen sus derechos a través de redes P2P[77].

El derecho de información, que se regula en el artículo 8 DRDPI, tiene su antecedente en el artículo 47 del Acuerdo ADPIC, el cual permite a los Estados miembros «disponer que, salvo que resulte desproporcionado con la gravedad de la infracción, las autoridades judiciales puedan ordenar al infractor que informe al titular del derecho sobre la identidad de los terceros que hayan participado en la producción y distribución de los bienes o servicios infractores, y sobre sus circuitos de distribución».

La Comisión Europea, al elaborar la Propuesta de Directiva, fue más allá de lo que establecía el artículo 47 del Acuerdo ADPIC, al sugerir un derecho de información obligatorio en todos los Estados miembros y de mayor alcance que el previsto en aquel convenio internacional.

> En efecto, de acuerdo con el artículo 9 de la Propuesta de Directiva, por un lado, los sujetos pasivos del derecho de información, es decir, las personas a quienes se podría compeler a proporcionar información sobre la infracción, no tenían por qué ser infractores o supuestos infractores[78]. Bastaba con que hubieran sido halladas en posesión de las mercancías litigiosas o utilizando servicios litigiosos, con fines comerciales, o hubieran sido identificados por los anteriores como miembros de la cadena de distribución de las mercancías o de suministro de los servicios. Por otro lado, la información no se limitaba a la identidad de los terceros que hubieran participado en la producción y distribución de los bienes y servicios litigiosos y a sus circuitos de distribución, sino que abarcaba también los datos objetivos de la infracción (cantidades producidas, entregadas, recibidas o encargadas, así como el precio obtenido por las mercancías o servicios de que se trate). Por último, el derecho de información podía ejercitarse ante la mera sospecha de una infracción, antes incluso de iniciarse procedimiento judicial alguno para reclamar tutela provisional o definitiva[79]. En cualquier caso, como vemos, el

[77] Aunque se han intentado encontrar semejanzas entre este derecho de información y la facultad de requerimiento que, como hemos visto, la sección 512 (h) DMCA estadounidense reconoce a los titulares de derechos de propiedad intelectual, lo cierto es que se trata de figuras muy distintas. Primero, por el mayor ámbito de aplicación del derecho de información de la DRDPI, que no se circunscribe a las infracciones que se puedan haber cometido a través de redes digitales. Segundo, porque, a diferencia de lo que ocurre en Estados Unidos, la DRDPI exige una orden judicial para requerir la información al prestador de servicios en línea.

[78] En este sentido, no tengo más remedio que corregir la afirmación que realicé en un artículo anterior («La Propuesta de Directiva relativa a las medidas y procedimientos destinados a garantizar el respeto de los derechos de propiedad intelectual», *Pe. i.*, núm. 14, mayo-agosto de 2003, pág. 59) en el sentido de que el derecho de información «faculta al titular del derecho supuestamente infringido para solicitar al tribunal competente para conocer sobre el fondo del asunto o sobre una petición de medidas cautelares o provisionales que, salvo que se opongan a ello razones particulares, ordene *a los supuestos infractores* que faciliten información sobre el origen y las redes de distribución de las mercancías o de suministro de servicios que se sospecha infringen el derecho de propiedad intelectual».

[79] A este respecto, decía el artículo 9.1 PDA: «Los Estados miembros establecerán que las autoridades judiciales competentes para conocer las acciones declarativas de infracción de un derecho de propiedad intelectual o para estimar una petición de medidas provisionales o cautelares ordenen, a petición del titular, salvo que se opongan a ello razones particulares, que toda persona que se encuentre en alguna de las situaciones que se enumeran a continuación facilite

artículo 9 de la Propuesta de Directiva no preveía la posibilidad de requerir a los prestadores de servicios de la sociedad de la información para que revelaran la identidad de quienes, valiéndose de sus servicios, infringieran derechos de propiedad intelectual.

La Comisión de Asuntos Jurídicos y Mercado Interior del Parlamento Europeo, al pronunciarse sobre la Propuesta de Directiva de la Comisión Europea, amplió tanto la legitimación activa para solicitar la información, al titular de los derechos o a cualquier otro legitimado para instar su protección, como la legitimación pasiva de la medida, es decir, el grupo de personas obligadas a informar, suprimiendo la exigencia de que fueran halladas en posesión de las mercancías litigiosas o utilizando los servicios litigiosos a escala comercial. De este modo, podría ser sujeto pasivo del requerimiento de información cualquiera que fuera hallado con bienes ilícitos o utilizando servicios ilícitos, incluso aunque fuera un consumidor[80]. En cambio, parecía circunscribir el derecho de información a los procedimientos ya iniciados relativos a la supuesta infracción de derechos de propiedad intelectual, lo que exigía que ya se hubieran solicitado medidas provisionales o se hubiera interpuesto una demanda sobre el fondo[81].

Una de las enmiendas a la Propuesta inicial sugeridas por la Comisión de Asuntos Jurídicos y Mercado Interior del Parlamento tenía que ver justamente con el tema que aquí nos ocupa. Consistía en facultar a los Estados miembros para obligar a los prestadores de servicios en línea a informar sin demora a las autoridades competentes de presuntas infracciones o actividades ilícitas de los usuarios de sus servicios, o a transmitir a estas autoridades, a solicitud de éstas, los datos a través de los cuales pudiera determinarse la identidad de los usuarios de sus servicios con los que hubieran establecido acuerdos relativos al almacenamiento de la información. Se trataba de una enmienda innecesaria, pues coincidía en lo esencial con lo dispuesto por el artículo 15.2 DCE. Pero sirvió para abrir la puerta a la posibilidad de ampliar el alcance subjetivo del derecho de información, de manera que pudiera ejercitarse también frente a los prestadores de servicios en línea.

El texto definitivo del artículo 8 DRDPI reconoce a los titulares de derechos de propiedad intelectual un derecho de información de tal amplitud que les permite solicitar a las autoridades judiciales civiles que requieran a los proveedores de acceso para que revelen la identidad de quienes presuntamente intercambian ilícitamente obras y prestaciones protegidas a través de Internet. Establece, por lo que aquí nos interesa, lo siguiente:

---

datos sobre el origen y las redes de distribución de las mercancías o de suministro de servicios *que se sospecha infringen un derecho de propiedad intelectual*».

[80] Además, prohibía a las personas obligadas a informar comunicarse con sus proveedores u otros posibles infractores una vez comenzada la investigación y conminaba a los Estados miembros a establecer sanciones para quien incumpliera su obligación de informar.

[81] Según el artículo 9.1 propuesto por esta comisión parlamentaria en su enmienda 29, «Los Estados miembros establecerán que las autoridades judiciales competentes en el marco de un procedimiento relativo a la supuesta infracción de un derecho de propiedad intelectual o para estimar una petición de medidas provisionales o cautelares ordenen, en respuesta a una petición justificada y proporcionada presentada por el demandante, salvo que se opongan a ello razones particulares, que toda persona que se encuentre en alguna de las situaciones que se enumeran a continuación facilite datos sobre el origen y las redes de distribución de las mercancías o de suministro de servicios que se sospecha infringen un derecho de propiedad intelectual (...)».

> *8.1. Los Estados miembros garantizarán que, en el contexto de los procedimientos relativos a una infracción de un derecho de propiedad intelectual y en respuesta a una petición justificada y proporcionada del demandante, las autoridades judiciales competentes puedan ordenar que faciliten datos sobre el origen y las redes de distribución de las mercancías o servicios que infringen un derecho de propiedad intelectual el infractor o cualquier persona que:*
>
> *(...)*
>
> *c) haya sido hallada prestando a escala comercial servicios utilizados en las actividades infractoras; (...).*

El precepto citado, que, con respecto a la Propuesta modificada por la Comisión de Asuntos Jurídicos y Mercado Interior del Parlamento Europeo, mantiene la exigencia de solicitud de parte (que deberá ser justificada y proporcionada) para aplicar esta medida, así como la amplitud en cuanto a la legitimación activa para pedirla (cualquier legitimado conforme al art. 4 DRDPI para instar la aplicación de las medidas de la Directiva puede ejercitar este derecho) [82], ha acotado en otros aspectos el ámbito de aplicación de este derecho.

Para empezar, según el artículo 8 DRDPI, el derecho de información sólo operará en el marco de procedimientos ya iniciados sobre infracciones de derechos de propiedad intelectual («en el contexto de los procedimientos relativos a una infracción de un derecho de propiedad intelectual», dice el precepto). No basta, por lo tanto, la mera sospecha de la infracción, sino que debe haberse interpuesto ya la correspondiente demanda o, al menos, haberse solicitado la adopción de medidas cautelares al respecto. Ahora bien, en la medida en que la DRDPI es una Directiva de mínimos (art. 2 DRDPI), es admisible que los Estados permitan a los titulares ejercitar el derecho de información antes del inicio del proceso, y con la finalidad de prepararlo, por ejemplo a través de diligencias preliminares.

En segundo lugar, aunque el texto definitivo del artículo 8 DRDPI se hace eco de la Propuesta modificada por la Comisión de Asuntos Jurídicos y Mercado Interior del Parlamento Europeo en lo que respecta a la posibilidad de que el obligado a informar no sea un infractor, introduce alguna variación importante con respecto a la legitimación pasiva de esta medida. Por un lado, añade al elenco de obligados a informar sobre la identidad de los supuestos infractores a los prestadores de servicios utilizados por los infractores para cometer la infracción. Por otro lado, sin embargo, restringe en alguna medida la legitimación pasiva, al establecer que sólo tendrán que facilitar la información requerida quienes hayan sido hallados en posesión de las mercancías litigiosas, utilizando los servicios litigiosos o prestando servicios utilizados en las actividades infractoras, en los tres casos «a escala comercial», o hayan sido

[82] Es decir, los titulares de derechos, las personas autorizadas por éstos para utilizar estos derechos (cesionarios no exclusivos o licenciatarios), entidades de gestión de derechos de propiedad intelectual y organismos profesionales de defensa que representen a los titulares de derechos, siempre en la medida en que lo permita la legislación aplicable.

designados por los anteriores como implicados en la producción, fabricación o distribución de dichas mercancías o en la prestación de dichos servicios. Esto significa que a los consumidores finales, en principio, no se les podrá obligar a informar sobre el origen de la infracción.

> Obsérvese la ambigüedad de la definición de «escala comercial» contenida en el considerando 14 de la Directiva, según el cual «los actos llevados a cabo a escala comercial son los realizados para obtener beneficios económicos o comerciales directos o indirectos», lo que «excluye normalmente los actos realizados por los consumidores finales de buena fe». Si el primer inciso de la definición parece reconducirnos a actividades lucrativas, es decir, aquellos actos a través de los cuales el infractor espera conseguir una ganancia patrimonial derivada directa[83] o indirectamente[84] de la infracción, el segundo genera dudas cuando señala que *normalmente* quedarán excluidos los actos realizados por los consumidores finales de buena fe[85]. Por definición, un consumidor final, sea de buena o mala fe, no desarrolla una actividad lucrativa en el sentido expuesto, por más que pueda lucrarse en la medida en que se ahorra los costes de adquisición de la obra o prestación protegida, o del producto auténtico[86]. Por eso mismo, no deja de resultar inquietante que el considerando 14 establezca que, en algún caso, es posible que un consumidor final, y además de buena fe (es decir, que ha actuado sin dolo, desconociendo el carácter ilícito de su acto), cometa una infracción a escala comercial. Este segundo inciso abre la puerta, me da la sensación, a una noción de «acto realizado a escala comercial» basada más en la entidad económica de la infracción que en el propio carácter comercial de la infracción.

Sin embargo, y esto es justamente lo que se pretendía, a quienes sí se impone el deber de identificar la fuente de la infracción, a requerimiento judicial, es a los prestadores de servicios de intermediación que actúan a escala comercial. Según el artículo 8.1 c) DRDPI, en efecto, están obligados a revelar la identidad de los usuarios que se valen de sus servicios para infringir derechos de propiedad intelectual.

En este sentido, no puede negarse que el artículo 8.1 c) DRDPI es una norma conscientemente engañosa, porque si, de acuerdo con el considerando 14 de la Directiva, las medidas judiciales más graves de protección de los derechos de propiedad intelectual, entre ellas la del artículo 8, quedan para los «actos lleva-

---

[83] Así, la distribución o puesta a disposición del público de una obra o prestación protegida a cambio de una remuneración.

[84] Por ejemplo, la puesta a disposición en línea de obras o prestaciones protegidas de forma gratuita, cuando el lucro deriva de la inserción de publicidad en la página *web* que ofrece esos objetos para que el público los descargue

[85] En este sentido, Janelly Fourtou, ponente de la Comisión de Asuntos Jurídicos y del Mercado Interior del Parlamento Europeo que analizó la Propuesta de Directiva relativa a las medidas y procedimientos destinados a garantizar el respeto de los derechos de propiedad intelectual, declaró tras la aprobación por el Parlamento de la Directiva, que «sólo un juez puede decretar que se practiquen registros en los hogares [de los supuestos infractores] o que se secuestren cuentas bancarias, y ello sólo cuando se ha infringido la Ley con fines comerciales... Esto excluye, *en principio*, actos realizados de buena fe por los consumidores finales».

[86] Ánimo de lucro no es lo mismo que actividad lucrativa, como señala SÁNCHEZ ARISTI, R., «La copia privada digital», *pe. i.*, núm. 14, págs. 12-13.

dos a cabo a escala comercial»[87], lo que induce a pensar que el «derecho de información» está destinado a identificar a los grandes infractores, en la práctica, en el ámbito de las infracciones cometidas a través de Internet, va a servir fundamentalmente para identificar a los pequeños infractores, a los usuarios finales, a los consumidores (de buena o mala fe)[88]. Y ello porque el artículo 8.1 c) no exige que la infracción haya sido cometida a escala comercial para obligar al prestador de servicios a revelar la identidad del usuario, sino que, con independencia de la relevancia económica de la infracción, *el prestador de servicios actúe en el tráfico a escala comercial*. Por consiguiente, todo prestador de servicios a escala comercial (por ejemplo, el proveedor de acceso a Internet que, de forma directa o indirecta, obtiene una ganancia derivada de esta actividad) tiene que informar sobre la identidad de los usuarios que, a través de su conexión a Internet, infringen derechos de propiedad intelectual, aunque tales infracciones no hayan sido cometidas a escala comercial.

> En lo demás, el artículo 8 DRDPI no difiere apenas del texto del artículo 9 de la Propuesta de Directiva presentada por la Comisión Europea. No presenta novedad ni en cuanto a los datos que el obligado a informar tiene que suministrar[89], que en el ámbito que nos ocupa consistirán en el nombre y el domicilio del presunto infractor, ni en cuanto a las disposiciones legales cuya aplicación no podrá verse perjudicada por el ejercicio de este derecho, en relación a las cuales simplemente añade aquellas que rijan la protección de la confidencialidad de las fuentes de información y el tratamiento de los datos personales, lo que resulta, por otra parte, lógico[90]. Que el artículo 8 DRDPI no desplace la normativa comunitaria relativa a la protección de datos de carácter personal significa que los titulares de derechos han de cumplir las exigencias sobre el tratamiento de datos personales tanto al recopilar las direcciones IP, a fin de ejercitar su derecho de información, como una vez que le sea revelada la identidad de los usuarios.

---

[87] Señala el primer inciso del considerando 14 DRDPI: «Las medidas que establecen el apartado 2 del artículo 6, el apartado 1 del artículo 8 y el apartado 2 del artículo 9 tienen que aplicarse sólo con respecto a actos llevados a cabo a escala comercial».

[88] De hecho, es la facultad que el artículo 8 DRDPI concede a los titulares de derechos una de las que más preocupó a los internautas y a los prestadores de servicios de la sociedad de la información durante la tramitación de la Directiva. Se ha dicho que, aplicada abusivamente, vulnera el derecho a la intimidad de los usuarios de Internet (cfr. GROSS, R. D., «Europe's proposed Intellectual Property Enforcement Directive unmasked: Overbroad proposal threatens civil rights, innovation and competition», *IP Justice White Paper on Proposed European Union IP Enforcement Directive*, 2003, pág. 3, disponible en la página *web* <http://www.ipjustice.org/ipenforcewhitepaper.shtm>).

[89] Entre los datos que hay que proporcionar figuran en el artículo 8 DRDPI, por un lado, los nombres y direcciones de los productores, fabricantes, distribuidores, suministradores y otros poseedores anteriores de las mercancías o servicios, así como de los mayoristas y minoristas destinatarios; por otro lado, la información sobre las cantidades producidas, fabricadas, entregadas, recibidas o encargadas, así como sobre el precio obtenido por las mercancías o servicios de que se trate.

[90] Las disposiciones a las que no afecta el derecho de información del artículo 8 DRDPI son las siguientes: las que conceden al titular derechos de información más amplios; las que regulen la utilización de los datos que se comuniquen con arreglo al presente artículo en procedimientos civiles o penales; las que regulen la responsabilidad por abuso del derecho de información; las que ofrezcan la posibilidad de negarse a facilitar datos que obliguen a la persona a la que se refiere el apartado 1 a admitir su propia participación o la de sus parientes cercanos en una infracción de un derecho de propiedad intelectual; y las que rijan la protección de la confidencialidad de las fuentes de información o el tratamiento de los datos personales.

> Quizás la última diferencia significativa con respecto a la Propuesta de la Comisión Europea es que se ha suprimido el apartado 4 del artículo 9 de ésta, que permitía a las autoridades competentes comunicar a los titulares de los derechos los datos obtenidos de los obligados a informar, sin perjuicio de la aplicación de las normas de protección de datos personales, a fin de que pudieran ejercitar las acciones pertinentes. La supresión es razonable por dos motivos. Primero, porque con la regulación final del derecho de información, el titular de los derechos infringidos tiene que haber ejercitado ya la acción por infracción de sus derechos [91]. Segundo, porque es el propio titular de los derechos el que tiene que solicitar a la autoridad judicial que recabe dicha información, la cual deberá incorporarse necesariamente al procedimiento en curso.

Para terminar, hay que recordar que el artículo 8 DRDPI debe interpretarse en relación con el artículo 15.1 DCE, del que se desprende que no puede imponerse a los PSL una genérica obligación de vigilancia, salvo que en el caso concreto la autoridad competente haya adoptado una medida en este sentido. Cuestión distinta es que pueda establecerse legalmente un deber genérico de conservación de los datos de conexión y tráfico de los usuarios durante un tiempo determinado, entre otras cosas para facilitar la averiguación de la identidad de supuestos infractores. Ahora bien, como ha señalado repetidamente el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales, para que la retención de los datos de tráfico sea lícita, según se infiere del artículo 6 de la Directiva 2002/58/CE, ha de ser necesaria, y el tiempo de mantenimiento, el menor posible; debiendo estar claramente regulada por ley esta práctica, de forma que se proteja a las personas contra el acceso ilícito a tales datos o cualquier otra forma de abuso [92]. Y aquí es donde reside hoy el mayor problema para los titulares de derechos: no está convenientemente regulada la obligación de los prestadores de servicios de la sociedad de la información de retener los datos de tráfico necesarios para identificar al usuario.

V. LA SITUACIÓN EN LA LEGISLACIÓN ESPAÑOLA VIGENTE

1. El conflicto entre el interés de privacidad de los usuarios de Internet y la protección de los derechos de propiedad intelectual

Como en los ordenamientos que hemos estudiado hasta ahora, la pretensión de los titulares de derechos de propiedad intelectual de que los PSL les revelen la identidad de quienes supuestamente infringen sus derechos a través de redes P2P puede entrar en conflicto con los derechos fundamentales de los usuarios de Internet. En concreto, los derechos implicados son los de intimidad (art. 18.1 CE) y protección de datos de carácter personal (art. 18.4 CE),

---

[91] Al menos, debe haber solicitado ya la adopción de medidas cautelares.

[92] Vid. *Working document on data protection issues related to intellectual property rights*, redactado por el Grupo de Trabajo sobre Protección de Datos del artículo 29 de la Directiva 95/46/CE, adoptado el 18 de enero de 2005, 10092/05/EN, WP 104, pág. 7.

a los que puede añadirse la libertad de expresión (art. 20.1 CE), en su modalidad de decidir si se quiere que el discurso sea anónimo o no.

> A raíz de la sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983[93], suele distinguirse entre el derecho a la intimidad y el derecho a la autodeterminación informativa, es decir, al control de los datos personales. Mientras que el primero salvaguarda la esfera privada de la persona, tanto en el ámbito personal como familiar, el segundo le otorga el poder de decisión en cuanto al tratamiento de sus datos personales, protegiéndole frente a la recogida, el almacenamiento, la utilización y la transmisión ilimitados de los mismos.
>
> La autonomía de este derecho a la autodeterminación informativa frente al derecho a la intimidad ha sido reconocida en España por nuestro Tribunal Constitucional. La STC 292/2000, de 30 de noviembre, es clara en este sentido, cuando ubica el derecho a la intimidad en el artículo 18.1 CE y el derecho a la protección de datos en el artículo 18.4 CE. De acuerdo con esta sentencia, en efecto, el artículo 18.4 protege a la persona frente a las agresiones potenciales a su libertad y dignidad provenientes de un uso ilegítimo del tratamiento mecanizado de datos[94]. Reconoce lo que el Tribunal Constitucional denomina la «libertad informática». La libertad informática, según esta misma sentencia, es «el derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5 y 94/1998, FJ 4)».
>
> La distinción entre el derecho a la intimidad y el derecho a la protección de datos es importante, pues significa que el artículo 18.4 CE no protege sólo los datos íntimos de la persona, sino cualquier dato personal de la misma, aunque sea público[95]. En este sentido, el artículo 3 a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), considera *dato personal* «*cualquier información* concerniente a personas físicas identificadas o identificables»[96], en términos parecidos a lo dispuesto por el artículo 2 a) de la Directiva 95/46/CE, anteriormente estudiada.
>
> De acuerdo con lo recién expuesto, es evidente que la recopilación de los datos de conexión a Internet de una persona que se comunica a través de redes P2P, con el propósito de averiguar su identidad, puede vulnerar tanto el derecho a la intimidad como el derecho a la protección de datos personales, así como el derecho a expresarse anónimamente. El derecho a la intimidad, porque, una vez revelada la identidad del usuario, y a partir del contenido de la carpeta que comparte con los demás usuarios de la red P2P, es posible conocer mucha información relativa a la vida privada de esa persona[97]. El derecho

---

[93] Disponible en castellano en *BJC*, núm. 33, 1984, págs. 126 y ss.
[94] Establece el artículo 18.4 CE: «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».
[95] Cfr. STC 292/2000.
[96] El énfasis es mío.
[97] Para ilustrar la afirmación anterior, imaginemos que el usuario, protegido por el supuesto anonimato que le proporciona el *alias* con el que opera en la red P2P, se dedica a intercambiar

> a la protección de datos, porque, constituyendo las direcciones IP datos personales de acuerdo con nuestro derecho, como se verá más adelante, su tratamiento, aunque sean datos públicos, no es enteramente libre. Y el derecho a expresarse anónimamente, porque, si consideramos que el intercambio de archivos a través de redes P2P es una modalidad de expresión [98], la revelación de la identidad del usuario que se comunica por esa vía supone la identificación del autor del mensaje concebido para su difusión anónima [99].

En principio, tratándose de derechos fundamentales, el conflicto de intereses tendría que resolverse a favor de los usuarios de Internet, si no fuera porque, desde el punto de vista de los titulares de los derechos infringidos, también está en juego un derecho fundamental: el derecho a la tutela judicial efectiva. Téngase en cuenta, en efecto, que, si no se les comunica la identidad de los presuntos infractores, no podrán seguir adelante con el proceso [100]. En esta colisión de derechos fundamentales, la solución deberá partir de una adecuada ponderación de los intereses en juego.

2. La recopilación de las direcciones IP de los supuestos infractores por los titulares de los derechos de propiedad intelectual

Con base en la legislación sobre protección de datos de carácter personal y sobre el secreto de las comunicaciones, podría cuestionarse la licitud de la recopilación de las direcciones IP de los presuntos infractores por los titulares de los derechos de propiedad intelectual supuestamente infringidos.

a) Desde la perspectiva de la protección de datos de carácter personal hay que señalar, ante todo, que en España, aunque todavía no se ha pronunciado al respecto ningún órgano jurisdiccional, se tiende a considerar que las direcciones IP constituyen datos personales, como en Francia o en Holanda. La Agencia Española de Protección de Datos (AEPD), como anteriormente el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, así lo ha declarado en su Informe 327/2003 [101].

---

fotografías eróticas. En este caso, parece obvio que la revelación de su identidad por el proveedor de acceso sin duda podría afectar a su derecho de intimidad. Téngase en cuenta que los archivos que una persona pone a disposición de los demás usuarios a través de su carpeta compartida dicen mucho sobre sus gustos, inquietudes e intereses. Mientras su identidad está oculta, lo único que trasciende es el listado de archivos que se encuentran en esa carpeta compartida cuyo titular es desconocido. Y dado que esa información transciende por decisión propia del usuario, es indudable que no puede haber vulneración alguna de su derecho de intimidad por el hecho de que alguien acceda a esa carpeta. Ahora bien, cuando, contra la voluntad del titular de esa carpeta compartida, se revela su identidad, el contenido de esa carpeta permite conocer datos de su esfera privada, y aquí sí entra en juego el derecho de intimidad.

[98] Igual que se expresa quien parafrasea a otro, lo hace quien comunica al público canciones, películas o fotografías a través de Internet.

[99] Hay que insistir una vez más en que el anonimato permite a muchos usuarios de Internet expresar libremente lo que no comunicaría si tuviera que identificarse.

[100] En este sentido, vid. VOGEL, M. S., «Umasking "John Doe" defendants: the case against excessive hand-wringing over legal standards», *Oregon Law Review*, núm. 83, 2004, págs. 795 y ss., especialmente págs. 809-810.

[101] El Informe es indicativo de la opinión de la AEPD al respecto, pero sus conclusiones no se han reflejado todavía en ninguna resolución o recomendación. Está disponible en la página *web* <https://www.agdp.es>.

> Lo explica de la siguiente manera: «Los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP. Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet, normalmente mantiene un fichero histórico con la dirección IP (fija o dinámica) asignada, el número de identificación del suscriptor, la fecha, la hora y la duración de la asignación de dirección. Es más, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación. En estos casos, ello significa que, con la asistencia de terceras partes responsables de la asignación, se puede identificar a un usuario de Internet, es decir, obtener su identidad civil (nombre, dirección, número de teléfono, etc.), por medios razonables, con lo que no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 3 de la Ley 15/1999 (...). Aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se considerarán datos de carácter personal resultando de aplicación la normativa sobre protección de datos» [102].

Que la dirección IP constituye un dato de carácter personal es algo que se desprende del artículo 3 a) LOPD, que los define como «cualquier información concerniente a personas físicas identificadas o identificables». En la medida en que, con la ayuda del proveedor de acceso, puede identificarse a la persona que, en un momento dado, ha utilizado una determinada dirección IP para conectarse a Internet, debe entenderse que, efectivamente, se trata de un dato personal [103].

Ahora bien, que las direcciones IP constituyan datos personales no quiere decir que, en todo caso, esté sometida a la LOPD la recopilación por parte

---

[102] En este Informe, la AEPD ha venido a reiterar la argumentación que ya utilizó en 1999 en relación a una consulta sobre si las direcciones de correo electrónico son datos personales. Entonces señaló que si la dirección de correo es tal que revela información relativa a su titular (por ejemplo, si la dirección es del tipo nombre.apellido@xxxx.es), constituye un dato personal porque lo identifica. Y si, por el contrario, y este es el supuesto que nos interesa, la dirección no muestra información sobre la persona que, por sí sola, la identifique, será de todas formas un dato personal, ya que cabe la posibilidad de identificar a su titular consultando al servidor de correo. En definitiva, la dirección de correo electrónico constituye siempre un dato personal, bien porque identifica directamente al usuario, bien porque permite su identificación indirecta, a través del prestador del servicio de correo electrónico. Sobre este particular, vid. <https://www.agpd.es/index.php?idSeccion=234>.

[103] Téngase en cuenta que el artículo 1.5 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica 5/1992, de 29 de octubre, cuya subsistencia deriva de la Disposición Transitoria Tercera LOPD, define la «identificación del usuario» como «cualquier elemento que permita determinar *directa o indirectamente* la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada». Recuérdese, asimismo, que la propia Directiva 95/46/CE establece que el afectado es identificable cuando puede ser identificado a través de medios razonables por el responsable del tratamiento del dato en cuestión *o por un tercero*. En contra, RIBAS, J., «La dirección IP como dato disociado», publicado en la *web* de Comunidad Thursday®, y disponible en la página *web* <http://noticias.juridicas.com/external/nj_thursday/200410-555174910142761.html>.

de los titulares de derechos de propiedad intelectual de las direcciones IP usadas por los supuestos infractores para vulnerar esos derechos. En efecto, el artículo 2.1 LOPD, en relación con el ámbito de aplicación de la Ley, establece: «La presente Ley Orgánica será de aplicación a los datos de carácter personal *registrados en soporte físico*, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores púbico y privado»[104]. Este precepto (en concreto, la exigencia de que los datos estén registrados en soporte físico) debe interpretarse en el sentido de que la LOPD sólo se aplica a aquellos datos contenidos en ficheros o destinados a incluirse en ficheros[105]. Los datos aislados, cuando no están registrados en un fichero, ni están destinados a su inclusión en un fichero, podrán ser datos personales, pero su tratamiento, en principio, no está sometido a las disposiciones de la LOPD[106]. Ahora bien, de acuerdo con el artículo 3.1 de la Directiva 95/46/CE, habrá que entender que las disposiciones de la LOPD (que incorpora la mentada Directiva) se aplicarán también siempre que los datos personales sean objeto de tratamiento total o parcialmente automatizado, estén o no incluidos en ficheros o destinados a su incorporación a los mismos[107].

Ello nos lleva a una nueva pregunta: ¿qué es jurídicamente un fichero? La respuesta nos la proporciona la propia LOPD en su artículo 3 b), según el cual fichero es «todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso». No todo listado de datos personales constituye, por consiguiente, un fichero. Sólo los *conjuntos organizados* de datos son ficheros. La AEPD ha precisado, en relación a los archivos no automatizados, que, para que se trate de ficheros, es necesario que los datos que contienen estén ordenados conforme a criterios específicos y determinados relativos a las personas.

> Ha dicho, en efecto: «Como ya se citó anteriormente, la definición de fichero prevista en la Ley es: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
>
> Los archivos (carpetas o conjunto de carpetas) o ficheros manuales, así como sus portadas, que no estén estructurados conforme a criterios específicos y determinados relativos a las personas, en un principio, se puede interpretar que no están comprendidos en el ámbito de aplicación de la Ley.

---

[104] El énfasis es mío.
[105] Así se desprende del artículo 3.1 de la Directiva 95/46/CE, que, al definir su ámbito de aplicación, se refiere al «tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero».
[106] En este sentido, GRIMALT SERVERA, P., *La responsabilidad civil en el tratamiento automatizado de datos personales*, Comares, Granada, 1999, págs. 70-71, señala que para que el tratamiento de datos quede sometido a la LOPD es necesaria cierta organización de esos datos.
[107] De lo contrario, resultaría que no se habría transpuesto la Directiva por lo que respecta al tratamiento automatizado de datos personales no registrados en ficheros ni destinados a incorporarse a los mismos.

> Por lo tanto, un fichero manual estará incluido dentro del ámbito de aplicación, cuando el fichero o archivo contenga un conjunto estructurado de datos personales que sean accesibles fácilmente a los datos personales con arreglo a criterios determinados» [108].

De acuerdo con lo anterior, es evidente que una red P2P no es un fichero. Por consiguiente, el titular de los derechos de propiedad intelectual podría, por sí o por mediación de un tercero, obtener de esa red las direcciones IP de los supuestos infractores, y a ese acto no se le aplicaría la LOPD, a menos que esas direcciones se recabaran a través de dispositivos automáticos (agentes electrónicos o inteligentes) o estuvieran destinadas a incluirse en un fichero en el sentido del artículo 3 b) LOPD. Ello implica que la mera recopilación manual por parte de los titulares de derechos de propiedad intelectual de las direcciones IP de los presuntos infractores es libre, siempre y cuando no se pretenda crear un fichero con tales datos. La dificultad estriba, claro está, en determinar a partir de qué momento el conjunto de datos así recabados por los titulares de derechos se puede considerar un fichero. El criterio cuantitativo puede ser útil. Es evidente que la anotación de una única dirección IP no dará lugar a un fichero. Probablemente tampoco un listado de menos de diez direcciones, y ello porque, cuando el número de datos es tan reducido que no es necesario ordenarlos para poder encontrar rápidamente aquel que se busca en un momento dado, es irrelevante que el conjunto esté o no estructurado, por lo que la exigencia de organización del artículo 3 b) carece de sentido. Pero, como vemos, el criterio cuantitativo es insuficiente por sí solo para calificar una lista de datos como fichero. Hay que atender necesariamente al criterio cualitativo de la organización. Si los datos, aunque sean numerosos, no están ordenados de forma tal que sean fácilmente accesibles a partir de criterios determinados de búsqueda, no constituirán un fichero.

Incluso en el caso de que los titulares de derechos de propiedad intelectual se valgan de agentes electrónicos para recolectar las direcciones IP de los supuestos infractores (tratamiento automatizado de datos), o pretendan crear verdaderos ficheros con las direcciones IP recabadas manualmente, supuestos en los que sí se aplicará la LOPD [109], la obtención de esos datos será lícita aun cuando no medie este consentimiento, en los términos que se exponen a continuación.

---

[108] Cfr. Memoria de la AEPD del año 2000, pág. 54.

[109] Téngase en cuenta que si el titular de derechos de propiedad intelectual creara un fichero con las direcciones IP de los supuestos infractores, tendría que adoptar las medidas de seguridad previstas por el artículo 9 LOPD y desarrolladas por el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Obsérvese que las medidas de seguridad se prevén en relación a los ficheros de datos personales, no en cuanto a los datos personales que sean objeto de tratamiento automatizado al margen de ficheros. Por otra parte, si el listado de direcciones IP recogidas por el titular de derechos de propiedad intelectual constituyera un fichero, tendría éste que notificar a la AEPD su constitución, así como inscribirlo en el Registro General de Protección de Datos (cfr. art. 26 LOPD).

Aunque como regla general es preciso el consentimiento del afectado para tratar sus datos personales (art. 6.1 LOPD), la Ley exime de la necesidad de recabar este consentimiento en determinados supuestos enumerados en el artículo 6.2 LOPD. De tales supuestos el que nos interesa es el último. Según el artículo 6.2 *in fine*, no se precisará el consentimiento del afectado cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado [110]. El concepto de «fuente accesible al público» lo establece la propia LOPD en su artículo 3 j), según el cual fuentes accesibles al público son «aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación». La enumeración de fuentes accesibles al público contenida en el artículo 3 j) LOPD constituye un *numerus clausus* (de ahí el uso del adverbio *exclusivamente*) [111]. Eso significa que Internet en general, y una red P2P en particular, sólo pueden considerarse fuentes accesibles al público, a los efectos del artículo 6.2 LOPD, si los incardinamos dentro de los *medios de comunicación* [112], lo que me parece plausible, dado que tanto Internet como las redes P2P constituyen una vía a través de la cual se puede comunicar cualquier información al público [113]. La consecuencia de considerar las redes P2P como

---

[110] Debe ponerse de manifiesto la divergencia que el artículo 6 LOPD presenta con respecto al artículo 7 de la Directiva 95/46/CE. Para empezar, el artículo 7 de la Directiva establece los supuestos en los que puede efectuarse el tratamiento de datos personales, uno más de los cuales es el caso en el que el propio interesado ha dado su consentimiento de forma inequívoca. El consentimiento del afectado, por lo tanto, no se configura como la regla general, frente a la cual los demás supuestos son excepciones, como sí se hace, en cambio, en el artículo 6 LOPD. Pero es que, además, la letra f) del artículo 7 de la Directiva no es tan restrictiva como el artículo 6.2 *in fine* LOPD. Según la Directiva, cabrá el tratamiento de datos personales «si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva». Queda claro, por tanto, que no exige que los datos se hayan obtenido de fuentes de acceso público. El legislador español ha contravenido, de esta forma, lo dispuesto por la Directiva, cuyo artículo 5, además, obliga a los Estados miembros a regular las condiciones en que son lícitos los tratamientos de datos personales «dentro de los límites de las disposiciones» del Capítulo II de la Directiva.

[111] Cfr. VIZCAÍNO CALDERÓN, M., Comentarios a la Ley orgánica de protección de datos de carácter personal, Civitas, Madrid, 2001, pág. 87.

[112] En contra de lo que pudiera parecer si nos atuviéramos al primer inciso del artículo 3 j) LOPD, para que estemos ante una fuente accesible al público no es preciso que se trate de un fichero. Si así fuera, no tendría sentido la mención de los medios de comunicación, que no constituyen ficheros del artículo 3 b) LOPD.

[113] Avala esta lectura de los artículos 6.2 y 3 j) LOPD el principio de interpretación conforme con el derecho comunitario. Como se ha indicado con anterioridad, la Directiva 95/46/CE, cuando faculta para el tratamiento de datos personales a quien tenga un interés legítimo, no lo

medios de comunicación es que el tratamiento de los datos personales a los que se accede a través de ellas no requiere el consentimiento de los afectados, siempre que no vulnere otros derechos fundamentales, como por ejemplo el de intimidad. Por consiguiente, hay que concluir que para obtener de la red la dirección IP del supuesto infractor no hace falta el consentimiento de éste, de conformidad con el artículo 6.2 LOPD [114].

Tampoco están obligados los titulares de derechos a informar a los supuestos infractores de que han recogido sus direcciones IP a fin de preparar las correspondientes demandas por vulneración de su propiedad intelectual, como con carácter general exige el artículo 5.4 LOPD. Según el apartado 5 del mismo artículo, ello no es necesario cuando resulte imposible, que es lo que ocurre en nuestro caso, ya que el responsable del tratamiento de esos datos desconoce la identidad de los interesados (de hecho, ésa es la razón por la que recoge sus direcciones IP). A mayor abundamiento, el párrafo segundo del artículo 5.5 LOPD establece que tampoco podrá exigirse la información a los afectados cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten. Es cierto que nos encontramos ante una excepción a una regla general (la de la necesidad de información al titular de los datos) y que, como norma excepcional, debe interpretarse restrictivamente y no es susceptible de aplicación analógica. Sin embargo, no dejan de ser llamativas las similitudes con nuestro caso. El artículo 5.5.II LOPD exime de informar de la recogida de los datos en los términos del artículo 5.4 a quien los ha obtenido de una fuente accesible al público para destinarlos a fines publicitarios, pero ello no significa que no tenga que informar al interesado. El mismo artículo dispone que tendrá que hacerlo en cada comunicación comercial que le dirija. Con ello se pretende evitar reiteraciones, pero no privar al afectado de su derecho de información sobre la recogida de los datos. Paralelamente, en el caso que nos ocupa, el titular de derechos que obtiene de una fuente accesible al público como es la propia red P2P las direcciones IP de los supuestos infractores, a fin de interponer las oportunas demandas judiciales, no está obligado a informar de ello a los afectados según lo dispuesto en el artículo 5.4 LOPD, entre otras cosas porque desconoce quiénes son éstos. Ahora bien, los infractores conocerán cómo se recabaron sus datos al sustanciarse el proceso judicial que se siga contra ellos.

Es lícito, por otro lado, que los titulares de derechos de propiedad intelectual contraten a empresas especialistas para que recaben los datos necesarios para poder ejercitar una acción judicial en defensa de sus derechos [115]. Lo permite el artículo 12.2 LOPD, que impone, sin embargo, tres exigencias. Primero, que

---

condiciona a que obtenga los datos de una fuente accesible al público. Ello obliga a interpretar nuestra Ley del modo más amplio posible.

[114] No se olvide que, aunque el artículo 6 se refiere al tratamiento de datos personales, el concepto de tratamiento incluye la recogida de los datos, de acuerdo con el artículo 3 c) LOPD.

dicho contrato conste por escrito o en alguna otra forma que permita acreditar su celebración y contenido. Segundo, que se establezca expresamente que el encargado del tratamiento sólo tratará los datos conforme a las instrucciones del responsable del tratamiento y que no los aplicará o utilizará con una finalidad distinta de la que figure en el contrato, ni los comunicará a terceros. Y tercero, que en el contrato se indicarán las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

Fuera del supuesto anterior, y siempre que estemos dentro del ámbito de aplicación de la LOPD, no cabrá en principio la comunicación de los datos personales recabados por el titular de los derechos de propiedad intelectual, o a instancia de él, salvo en el improbable caso de que lo consienta el supuesto infractor (art. 11.1 LOPD). Ahora bien, si los datos han sido obtenidos directamente de la red P2P, y consideramos que ésta constituye una fuente accesible al público, no se precisará dicho consentimiento (art. 11.2 b] LOPD). Esta interpretación permitiría, por ejemplo, que una entidad de gestión, o una asociación de defensa profesional, comunicara las direcciones IP de los supuestos infractores a sus asociados a fin de que fueran éstos los que interpusieran las correspondientes demandas.

Por último, por lo que a la perspectiva de la protección de datos se refiere, hay que indicar que, en aquellos casos en los que es de aplicación la LOPD (recuérdese, recogida automática de direcciones IP o recogida manual de las mismas a fin de incorporarlas a un fichero), para que la recopilación de las direcciones IP de los supuestos infractores sea lícita ha de hacerse de conformidad con lo dispuesto en el artículo 4 LOPD. Por consiguiente, no pueden recogerse otros datos que los que sean adecuados, pertinentes y no excesivos a fin de preparar el proceso por la supuesta lesión de los derechos de propiedad intelectual (art. 4.1). Esos datos son la dirección de IP, el *nick* o *alias* del usuario, la fecha y hora de la conexión y las obras o prestaciones protegidas del repertorio del responsable del tratamiento ilícitamente puestas a disposición del público. Los datos así obtenidos no podrán usarse para una finalidad distinta de la preparación del proceso judicial contra el supuesto infractor (art. 4.2), y deberán ser exactos (art. 4.3). Finalmente, una vez cumplida su finalidad, deberán ser cancelados (art. 4.5).

b) Si la recopilación de direcciones IP por los titulares de derechos de propiedad intelectual es lícita desde el punto de vista del derecho a la protección de datos de los usuarios de Internet, también lo es desde la perspectiva del derecho al secreto de las comunicaciones, reconocido por el artículo 18.3 CE.

Cabría alegar que el derecho al secreto de las comunicaciones opera en el ámbito de procesos de comunicación cerrados, es decir, privados [116]. En el intercambio de archivos a través de redes P2P las comunicaciones no suelen ser

---

[115] De hecho, es lo que suele ocurrir en la práctica.

[116] Cfr. MARTÍN MORALES, R., El régimen constitucional del secreto de las comunicaciones, Civitas, Madrid, 1995, pág. 46; FERNÁNDEZ RODRÍGUEZ, J. J., *Secreto e intervención de las comunicaciones en Internet*, Civitas, Madrid, 2004, págs. 98-99.

privadas. Los usuarios lo que hacen es poner sus archivos a disposición de los demás para que quien esté interesado los descargue a través de una transmisión de datos, la cual, eso sí, será punto a punto. Se trata, por tanto, de una comunicación al público de archivos [117]. Si la comunicación es pública, es cuanto menos discutible que pueda estar amparada por el secreto de las comunicaciones. Ahora bien, frente a lo anterior cabe defender, acertadamente a mi juicio, que también en este ámbito opera el derecho al secreto de las comunicaciones, si se precisa que lo que se protege no es el acto de comunicación consistente en la puesta a disposición del público de uno o varios archivos, sino el consistente en la transmisión del archivo una vez solicitado por un concreto usuario.

Para entender por qué es lícito que los titulares de derechos de propiedad intelectual recopilen las direcciones IP de quienes ponen a disposición del público obras y prestaciones protegidas a través de redes P2P, no puede perderse de vista cuál es el bien jurídico protegido por el derecho al secreto de las comunicaciones. Lo que protege el artículo 18.3 CE no es el contenido de la comunicación, que, en su caso, estará amparado por otros derechos de los comunicantes, como el derecho a la intimidad o el derecho a la protección de datos de carácter personal. Lo que protege el artículo 18.3 CE es el propio proceso de comunicación [118]. Por ello mismo, si no se intercepta la comunicación, no se vulnera el derecho al secreto de las comunicaciones por el simple hecho de anotar la dirección IP del comunicante. Así sucede cuando quien obtiene esa dirección IP participa en ese acto de comunicación [119], que es lo que ocurre normalmente en el supuesto que nos ocupa, donde el titular de los derechos de propiedad intelectual o un tercero por él contratado se introduce en la misma red P2P en la que actúa el infractor y se comunica directamente con él, recogiendo en ese acto de comunicación su dirección IP [120].

> Fuera del caso en que el titular de derechos de propiedad intelectual, o la persona contratada por él a tal efecto, participa del acto de comunicación a

---

[117] De ahí, justamente, que si tiene por objeto obras o prestaciones protegidas, y no media la autorización del titular de los derechos sobre las mismas, constituya una conducta ilícita.

[118] Cfr. FERNÁNDEZ RODRÍGUEZ, *Secreto e intervención de las comunicaciones en Internet, cit.*, págs. 94-95.

[119] Cfr. STC 114/1984, según la cual sobre los comunicantes no pesa este deber de secreto de las comunicaciones, «sino, en todo caso, y ya en virtud de norma distinta a la recogida en el artículo 18.3 CE, un posible "deber de reserva" que —de existir— tendría un contenido estrictamente material, en razón de cuál fuese el contenido mismo de lo comunicado (un deber que derivaría, así, del derecho a la intimidad reconocido en el artículo 18.1 de la Constitución)».

[120] Vid. en el mismo sentido GONZÁLEZ DE ALAIZA CARDONA, «La lucha de los titulares de derechos de autor contra las redes "peer to peer" (P2P)», *cit.*, págs. 60-61. Como señala este autor, contravendrían el derecho al secreto de las comunicaciones tanto la utilización de *sniffers* (programas de ordenador que rastrean el tráfico en la red a fin de recoger determinados datos que puedan circular por ella) como la utilización de *supernodos* que, por su potencia, actúen como intermediarios entre los ordenadores de los usuarios, de tal modo que puedan interceptar los datos comunicados entre éstos. Hay que recordar, asimismo, que el artículo 33 de la Ley General de Telecomunicacione impone a los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público el deber de garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

través del cual recoge las direcciones IP de los supuestos infractores, sólo cabría obtener esos datos previa autorización judicial, amparada por una ley habilitante. La Ley de Enjuiciamiento Civil no prevé entre sus medidas la posibilidad de intervenir las comunicaciones de nadie. De hecho, en el seno del Derecho Privado sólo cabe la intervención de las comunicaciones en el ámbito del concurso de acreedores [121]. Por tanto, ningún órgano jurisdiccional civil podría autorizar la intercepción de transmisiones de datos a través de redes P2P a los efectos de averiguar las identidades de los supuestos infractores de derechos de propiedad intelectual.

3. El requerimiento a los prestadores de servicios en línea para que revelen la identidad de los supuestos infractores

Una vez que el titular de los derechos ha recopilado los datos relativos a la conexión del supuesto infractor necesarios para identificarlo, lo que hemos visto que es lícito si se hace en los términos expuestos en el epígrafe anterior, le queda el paso más importante y, a la vez, el más problemático desde el punto de vista jurídico, que no es otro que requerirle al proveedor de acceso para que revele la identidad de ese presunto infractor.

Si el requerimiento es extrajudicial, el PSL no sólo no está obligado a proporcionarle al titular de los derechos de propiedad intelectual la información solicitada, sino que, de hecho, tiene prohibido por ley suministrar dicha información. Así se desprende del artículo 11.1 LOPD, que requiere el consentimiento del interesado para la comunicación a terceros de los datos personales objeto de tratamiento, salvo que concurra alguna de las excepciones del artículo 11.2, ninguna de las cuales resulta aplicable a nuestro caso [122].

En relación con la revelación a los titulares de derechos de propiedad intelectual de la identidad de los supuestos infractores por parte de los PSL no se plantean las dudas sobre la aplicación de la LOPD que, como vimos antes, se suscitan en cuanto a la recogida de direcciones IP por parte de los titulares de derechos. La razón es que al PSL se le solicita la comunicación de datos personales (nombre y domicilio del usuario que se ha conectado a Internet a través de una concreta dirección IP) que se encuentran registrados en sus propios ficheros (las bases de datos de clientes, en las que aparecen sus nombres, domicilios, números de teléfono, cuentas de acceso a Internet, cuentas de correo electrónico, datos de facturación, etc.). Por otra parte, estos ficheros son privados, no accesibles al público, por lo que no es aplicable la excepción a la necesidad de consentimiento del afectado del artículo 11.2 b) LOPD.

---

[121] Cfr. artículo 1 L.O. 8/2003, de 9 de julio, para la Reforma Concursal.

[122] En el mismo sentido, el artículo 34 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, establece que «los operadores que operen redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal», lo que conduce igualmente a la aplicación del artículo 11 LOPD.

Para obtener la identidad de los supuestos infractores, el titular de los derechos tendrá que instar una orden judicial de revelación de esos datos. Así se desprende del artículo 11.2 d) LOPD, según el cual no es preciso el consentimiento del interesado cuando la comunicación que tenga que efectuarse tenga por destinatario a los jueces o tribunales (entre otros) en el ejercicio de las funciones que tienen atribuidas.

El problema con el que se encuentran los titulares de derechos es que, a la espera de que se incorpore el artículo 8 DRDPI a nuestra legislación interna, no está prevista aún en nuestro ordenamiento una vía procesal específica para obtener semejante orden judicial. Y, lo que es tanto o más grave, tampoco existe una obligación clara para los PSL de retener los datos necesarios para identificar a los presuntos infractores. Veamos estos problemas separadamente.

a) *Problemas de índole procesal*

En el ámbito del proceso civil, la única vía que ha previsto nuestro legislador para obtener la información necesaria para preparar un juicio son las diligencias preliminares, reguladas en los artículos 256 y ss. LEC. Según la doctrina del Tribunal Supremo, sentada en el auto de 11 de noviembre de 2002 [123], las diligencias preliminares son tasadas, es decir, no hay más que las establecidas por la Ley [124]. En este sentido, el artículo 256.1 LEC contiene un elenco de diligencias preliminares que, de acuerdo con su apartado 7.º, debe completarse con aquellas otras previstas por las correspondientes leyes especiales. El problema es que ninguna de las diligencias preliminares previstas expresamente en nuestro ordenamiento, ya sea en la LEC, ya en otras leyes especiales, se refiere específicamente a la cuestión que estamos estudiando. Peor aún, la Ley de Propiedad Intelectual no contiene ni tan siquiera una diligencia preliminar expresa. Ello obliga, lógicamente, a buscar soluciones alternativas, a fin de no dejar en la más absoluta indefensión a los titulares de los derechos de propiedad intelectual infringidos.

La primera solución la encontramos en la Ley de Competencia Desleal (LCD), que es una de esas leyes especiales, aludidas por el artículo 256.1.7.º LEC, que prevén diligencias preliminares. En concreto, su artículo 24.1 legitima a quien pretenda ejercitar una acción de competencia desleal para solicitar la práctica de diligencias para la comprobación de aquellos hechos cuyo conocimiento resulte objetivamente indispensable para preparar el juicio. Sin duda, pocos

[123] RJ 2003/575.

[124] Pero vid. el Acuerdo de la Audiencia Provincial de Madrid núm. 10/2004, de 23 de septiembre (JUR 2004/307394), que, tras reconocer que las diligencias del artículo 256.1 LEC constituyen un *numerus clausus*, propugna una interpretación flexible y extensiva de los términos empleados en los supuestos legales, para adecuarla a las exigencias del derecho a la tutela judicial efectiva. A favor de la interpretación extensiva del artículo 256.1 LEC, y de la posibilidad de su aplicación analógica a supuestos no expresamente previstos, pero similares, vid. BANACLOCHE PALAO, J., *Las diligencias preliminares*, Civitas, Madrid, 2003, págs. 59-72.

hechos son más importantes para preparar un juicio que la identidad del demandado.

Las diligencias preliminares de la LCD sirven a los efectos que aquí nos interesan porque, según dispone el artículo 11.1 LCD, constituye una deslealtad concurrencial la imitación de prestaciones amparadas por un derecho de exclusiva reconocido por la Ley, que es lo que ocurre en nuestro caso. En efecto, no se discute que la imitación comprende la reproducción idéntica de la prestación [125]. Tampoco que entre los derechos de exclusiva a los que se refiere el artículo 11.1 LCD se incluyen los derechos exclusivos de propiedad intelectual. Tampoco que la puesta a disposición del público a través de una red P2P de obras o prestaciones protegidas entraña tanto su reproducción (en la carpeta compartida del ordenador del usuario) como su comunicación pública, por lo que si estos actos no han sido autorizados por el titular de los correspondientes derechos, se están vulnerando sus derechos exclusivos. Y tampoco, por último, que unos mismos hechos pueden considerarse ilícitos tanto desde el punto de vista de la propiedad intelectual como de la competencia desleal, pudiendo ejercitarse simultáneamente las acciones dimanantes de la LPI y de la LCD [126].

La única duda que podría suscitarse es si la LCD puede aplicarse a meros usuarios de Internet. Al respecto, debe señalarse que el ámbito de aplicación de la LCD es muy amplio. Su ámbito subjetivo, según su artículo 3, comprende no sólo a los empresarios, sino también «a cualesquiera otras personas físicas o jurídicas que participen en el mercado», incluso aunque no exista una relación de competencia entre el sujeto activo y el sujeto pasivo del acto de competencia desleal (art. 3.2 LCD). El requisito de la participación en el mercado conduce implícitamente al ámbito objetivo de aplicación de la Ley, que se regula en su artículo 2, según el cual la ley se aplicará a aquellos actos que se realicen en el mercado y con fines concurrenciales (art. 2.1 LCD), presumiéndose la finalidad concurrencial «cuando, por las circunstancias en que se realice, se revele objetivamente idóneo para promover o asegurar la difusión en el mercado de las prestaciones propias o de un tercero» (art. 2.2. LCD).

De los artículos citados se colige que la aplicación o no de la LCD no depende de quién realice el acto, ni de si dicho acto tiene o no finalidad comercial, ni de si es un acto esporádico o una actividad continuada. Depende de las consecuencias que ese acto produzca o pueda producir en el mercado [127]. La LCD se aplica a aquellos actos que trascienden de la esfera privada de quien los realiza y producen efectos en el ámbito económico [128], afectando a las relaciones económicas que existen en el mercado o a las posiciones competitivas de sus agentes. En este sentido, el usuario de Internet que pone a disposición del

---

[125] Cfr. MASSAGUER FUENTES, J., *Comentario a la Ley de Competencia Desleal*, Civitas, Madrid, 1991, pág. 337.
[126] Vid. SAP Madrid de 25 de marzo de 2004 (JUR 2004/248592).
[127] Cfr. MASSAGUER FUENTES, *Comentario a la Ley de competencia desleal, cit*., págs. 122-123.
[128] Cfr. OTAMENDI RODRÍGUEZ-BETHENCOURT, J. J., *Comentarios a la Ley de competencia desleal*, Aranzadi, Pamplona, 1994, pág. 143.

público copias de mil fonogramas, por ejemplo, claramente compite con los productores y distribuidores discográficos, pues quien descargue esos fonogramas a través de la red P2P no necesitará adquirir una copia legítima del fonograma en cuestión. Es más, si tomamos en consideración la conducta global de todos cuantos se conectan a una misma red P2P para intercambiar música o productos audiovisuales, no podemos sino concluir que esa práctica común distorsiona la competencia [129]. No hay, por consiguiente, razón jurídica alguna para excluir de la aplicación de la LCD a los usuarios de Internet.

Si los titulares de derechos de propiedad intelectual pueden ejercitar demandas por competencia desleal contra los supuestos infractores de sus derechos exclusivos, al amparo del artículo 11.1 LCD, es evidente que también pueden solicitar las diligencias de comprobación previstas por el artículo 24.1 LCD para preparar esos juicios. Y entre esas diligencias dirigidas a comprobar los hechos relacionados con la infracción, debe incluirse, desde luego, el requerimiento a los PSL para que revelen la identidad de los titulares de las cuentas de acceso a Internet que en el momento de cometerse la infracción tenían asignadas las direcciones IP a través de las cuales se lesionaron los derechos de propiedad intelectual.

La segunda solución parte del deber que tienen los prestadores de servicios de la sociedad de la información de colaborar con las autoridades judiciales en la cesación de conductas ilícitas realizadas a través de la red, y se sustenta en el artículo 12 de la Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), interpretado de conformidad con el derecho comunitario. Dos recientes autos de audiencias provinciales han venido a señalar que la remisión del artículo 256.1.7.º LEC a las diligencias preliminares previstas en leyes especiales comprende también aquellas diligencias implícitas en deberes de colaboración e información establecidos en esas leyes especiales. Dado que el artículo 12 LSSI establece uno de estos deberes de colaboración e información, hay que entender que contiene asimismo una diligencia preliminar implícita.

> El primero de estos autos es el de la Audiencia Provincial de Barcelona, de 21 de marzo de 2005 [130], que acordó como diligencia preliminar, a instancia de una entidad de gestión de derechos de propiedad intelectual, la exhibición de documentos y libros contables de una sociedad deudora de la remuneración por copia privada, al amparo del artículo 256.1.7.º LEC, en relación con el artículo 25.21 LPI. Lo justificaba de la siguiente manera: «La remisión prevista en el artículo 256.1.7.º LEC alcanzaría no sólo a las diligencias preliminares específicamente reguladas en otras leyes especiales, como las de patentes y competencia desleal antes mencionadas, sino también a las

[129] Obsérvese que se genera una especie de «sociedad virtual», a la que los usuarios de la red contribuyen aportando los archivos que se encuentran alojados en sus carpetas compartidas, y cuya finalidad es ahorrarse los costes de adquisición de obras y prestaciones protegidas (lo que bien podría verse como una ganancia que se obtiene a costa de los titulares de derechos de propiedad intelectual).

[130] JUR 2005/125276.

> que se inducen de los específicos deberes de colaboración e información que se imponen a los deudores del canon por copia privada frente a las entidades de gestión, acreedores de este derecho, al amparo del artículo 25.21 TRLPI».
>
> El segundo es de la Audiencia Provincial de Madrid, de 3 de marzo de 2005 [131], que acordó como diligencias preliminares la entrega de las historias médicas de una paciente fallecida a sus familiares, para que éstos pudieran preparar una demanda sobre responsabilidad médica, con base en el artículo 256.1.7.º LEC, en relación con los arts. 16 y 18 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica Estos preceptos, aunque no contemplan expresamente la diligencia en cuestión, sí reconocen un derecho de acceso (y el correlativo deber de facilitar dicho acceso) al citado historial clínico.
>
> En ambos casos, la razón que subyace en la concesión de las diligencias preliminares es la misma. Si no se considerara que están implícitas en el deber de colaboración o información que se impone a determinadas personas, éste quedaría prácticamente vacío de contenido.

En nuestro caso, el deber de colaboración e información del que dimanan las diligencias preliminares de revelación de la identidad del supuesto infractor deriva del artículo 12 LSSI. Después de establecer un genérico deber de retención de datos de conexión y tráfico que incumbe a los prestadores de servicios de la sociedad de la información, al que luego me referiré, el párrafo cuarto del artículo 12.2 dispone lo siguiente: «Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios a los que se refiere este artículo no podrán utilizar los datos retenidos para fines distintos de los indicados en el apartado siguiente *u otros que estén permitidos por la Ley*, y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos». Y continúa el apartado 3: «Los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública o la defensa nacional, *poniéndose a disposición de los Jueces o Tribunales* o del Ministerio Fiscal que así lo requieran» [132].

La interpretación literal y aislada del artículo 12 LSSI podría conducir al error de entender que sólo contempla el deber de información de los PSL en el marco del proceso penal [133]. Sin embargo, una interpretación conforme con lo dispuesto por el derecho comunitario [134], y en concreto con los artícu-

---

[131] JUR 2005/108748.

[132] Los énfasis son míos.

[133] Vid. GONZÁLEZ DE ALAIZA CARDONA, «La lucha de los titulares de derechos contra las redes "peer to peer" (P2P)», *cit.*, pág. 64, quien propone alternativas de interpretación del artículo 12.3 LSSI para que también en el proceso civil pueda exigirse a los PSL la revelación de la identidad de los usuarios de Internet.

[134] De acuerdo con la STJCE de 10 de abril de 1984 (asunto 14/83), los jueces están obligados a dar a la legislación nacional adoptada en ejecución de una Directiva una interpretación y una aplicación conformes con las exigencias del Derecho comunitario. Este principio de interpretación conforme opera incluso en relación a Directivas pendientes de transposición y aun en el ámbito de las relaciones litigiosas horizontales. Así se desprende de la STJCE de 13 de noviem-

los 15.2 y 18.1 DCE, 8.2 DDASI y 8 DRDPI, estudiados con anterioridad, nos lleva a una conclusión bien distinta. En efecto, hemos visto ya cómo el derecho comunitario obliga a los Estados miembros a prever recursos judiciales que permitan poner fin a las infracciones y asegurar a los perjudicados el resarcimiento de los daños sufridos. Uno de esos recursos, que de hecho contempla el propio ordenamiento comunitario (art. 8 DRDPI), es el requerimiento judicial a los PSL para que revelen la identidad de quienes cometen infracciones de derechos de propiedad intelectual a través de la red. Sin esta medida, no sería posible ejercitar las acciones de cesación y de indemnización de daños y perjuicios que garantiza el derecho comunitario. Pues bien, el artículo 12, que procede, además, del artículo 15.2 DCE, debe interpretarse de tal modo que permita cumplir las obligaciones que le imponen al Estado español los citados preceptos comunitarios. Y esa interpretación no es otra que la de entender que los PSL están obligados a revelar la identidad de quienes utilizan sus servicios para infringir derechos de propiedad intelectual, siempre que así se lo requiera un tribunal civil a instancia del titular de los derechos, y que dicha información sirva para la preparación de un proceso civil para la defensa de esos derechos de propiedad intelectual.

Avalan esta lectura del artículo 12 LSSI otros argumentos, además del principio de interpretación conforme con el derecho comunitario. En primer lugar, el párrafo cuarto del artículo 12.2 permite que los datos de conexión y tráfico retenidos por los PSL se utilicen para otros fines distintos del expresamente contemplado en el artículo 12.3, siempre que estén permitidos por la Ley. Entre esos usos posibles se encuentra la revelación de los datos a los titulares de derechos infringidos a través de la red a requerimiento de un tribunal civil, que está implícito en el propio artículo 12 LSSI, interpretado conforme al derecho comunitario. En segundo lugar, el artículo 12.3 LSSI, y esto no admite duda, obliga a los PSL a facilitar a las autoridades competentes en el ámbito del proceso penal la información necesaria para identificar a quienes cometen delitos contra la propiedad intelectual a través de Internet. La información así obtenida podría en última instancia servir también para instar procedimientos civiles complementarios, como ha ocurrido en Alemania. Pero resulta contrario al principio de mínima intervención del derecho penal obligar al titular de los derechos de propiedad intelectual a perseguir la infracción por la vía penal, por ser el único modo de obtener los nombres y direcciones de los presuntos infractores. En tercer lugar, el derecho a la tutela judicial efectiva de los titulares de los derechos de propiedad intelectual

---

bre de 1990 (asunto C-106/89), según la cual «al aplicar el derecho nacional, ya sea disposiciones anteriores o posteriores a la directiva, el órgano jurisdiccional nacional que debe interpretarla está obligado a hacer todo lo posible, a la luz de la letra y de la finalidad de la directiva, para, al efectuar dicha interpretación, alcanzar el resultado a que se refiere la directiva y de esta forma atenerse al párrafo tercero del artículo 189 (actual art. 249) del Tratado». En la misma línea pueden verse las SSTJCE de 16 de diciembre de 1993 (asunto 334/92) o 7 de diciembre de 1995 (asunto C-472/93). Nuestro Tribunal Supremo, haciéndose eco de esta doctrina, ha declarado que las directivas comunitarias deben servir de guía para la interpretación del derecho nacional, tanto anterior como posterior, a fin de alcanzar el resultado perseguido por la directriz comunitaria (cfr. STS 20-11-1996 [RJA 8371]).

infringidos a través de redes P2P impone una interpretación amplia del artículo 12 LSSI, de modo que obligue a los PSL a revelar la identidad de los infractores también el ámbito del proceso civil [135].

Ya sea por la vía del artículo 24 LCD, ya por la del artículo 12 LSSI, es defendible que los titulares de derechos de propiedad intelectual pueden solicitar como diligencias preliminares el requerimiento a los PSL para que revelen la identidad de quienes, utilizando una concreta dirección IP, presuntamente han infringido sus derechos a través de redes P2P. A la vista de los fundamentos de la solicitud, el juez competente (el juez de lo mercantil del lugar del domicilio del PSL, de acuerdo con el art. 257.1 LEC, en relación con el art. 86 ter de la LOPJ) concederá las diligencias solicitadas si se cumplen los tres requisitos exigidos por el artículo 258.1 LEC. En primer lugar, que la diligencia sea adecuada a la finalidad perseguida por el solicitante, lo que ocurrirá siempre que la orden judicial de revelación de la identidad de los supuestos infractores sea la única vía para identificarlos, con vistas a interponer la correspondiente demanda. En segundo lugar, que concurra justa causa, es decir, que la solicitud se apoye en una base jurídica razonable, que la información requerida sea necesaria para preparar el proceso posterior y que el solicitante no pueda obtener la información por sus propios medios. Y en tercer lugar, que el solicitante tenga un interés legítimo, para lo cual entiendo que basta con que acredite su legitimación activa para interponer la demanda que, a través de estas diligencias preliminares, pretende preparar. Es en este momento cuando la autoridad judicial ponderará los distintos intereses en conflicto: el de privacidad de los supuestos infractores frente al derecho a la tutela judicial efectiva del titular de los derechos. En este sentido, cuanto más consistente sea la pretensión del solicitante, más fácilmente se dictará la orden judicial de revelación de información (algo similar a lo que ocurre con las medidas cautelares y la apariencia de buen derecho).

Si, finalmente, el juez accede a la pretensión del titular de los derechos y ordena al proveedor de acceso la revelación de la identidad de quienes estaban detrás de las direcciones IP a través de las cuales supuestamente se cometieron las infracciones, el PSL deberá cumplir la orden de acuerdo con las normas relativas al deber de retención de datos de conexión y tráfico de los usuarios de Internet, a las que seguidamente haré alusión, y a su propia *lex artis* [136]. Es posible, por lo tanto, que la orden resulte infructuosa, si la información suministrada al PSL para cumplir su cometido es insuficiente, o

---

[135] En la misma línea, le parece claro a GARROTE FERNÁNDEZ-DÍEZ, *La reforma de la copia privada en la Ley de Propiedad Intelectual*, *cit.*, pág. 272, que el artículo 12.3 LSSI es aplicable también en el ámbito de los procesos civiles, lo que justifica escuetamente: «es claro que también se incluyen en el tenor de dicha norma los ilícitos civiles, pues de otro modo se estaría dando carta blanca a dichas actividades sin que hubiera una vía legalmente habilitada para identificar a los infractores».

[136] El cumplimiento de la orden judicial generará normalmente gastos para el PSL que deberán ser compensados por los titulares de derechos que hayan solicitado las diligencias preliminares (art. 256.3 LEC). Para asegurar esta compensación, el juez, al conceder las diligencias solicitadas, fijará caución (art. 259.1 LEC).

tiene incorrecciones, o si se han borrado ya los datos necesarios para poder identificar a los usuarios. Cabe también la posibilidad de que el resultado no arroje suficiente luz sobre quién puede ser el infractor. Así sucede, por ejemplo, cuando la dirección IP facilitada al PSL resulta ser la dirección pública correspondiente a un enrutador que da salida a Internet a una red de área local de cierta envergadura. En este caso, si el titular de los derechos quiere precisar más, no tendrá más remedio que solicitar unas nuevas diligencias preliminares, esta vez contra el titular de la red de área local, para que determine desde qué ordenador de esa red de área local se cometió la infracción, y por esta vía, quién lo hizo.

> Conviene recordar que el PSL sólo puede conocer la identidad del titular de la cuenta de acceso a Internet a través de la cual se ha cometido la infracción, lo cual no quiere decir que esa persona sea necesariamente el infractor. Piénsese, por ejemplo, que una misma cuenta doméstica de acceso a Internet puede ser utilizada por todos los miembros de la familia para conectarse a la red. En estos casos, a falta de otras pruebas sobre quién puede haber sido el infractor, tendrá que recurrirse a la presunción judicial (art. 386 LEC) de que el titular de la cuenta de acceso es el infractor. En muchos casos, además, el titular de la cuenta de acceso será responsable indirecto de la infracción conforme al artículo 1.903 CC, bien porque los infractores están sometidos a su patria potestad o tutela, bien porque se trata de empleados suyos.

b) *La obligación de los PSL de retener los datos de conexión de los usuarios*

El éxito de las diligencias preliminares de revelación de la identidad de quien ha infringido derechos de propiedad intelectual a través de redes P2P depende de que el PSL a quien se dirige la orden judicial resultante conserve los datos de conexión correspondientes. Por consiguiente, de poco sirve reconocer a los titulares de derechos la facultad de requerir, por vía judicial, esta información, si no va acompañada de una obligación legal, dirigida a los PSL, de retención de esos datos de conexión durante cierto tiempo.

En teoría, es el artículo 12 LSSI el que establece el deber de los PSL de retener los datos de tráfico relativos a las comunicaciones electrónicas. De hecho, en su apartado 1 establece que «los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo» [137]. Precisa además, en su apartado 2, primer párrafo, que los datos que los proveedores de acceso han de conservar son únicamente

[137] La remisión a un posterior desarrollo reglamentario se completa en el apartado 4, según el cual se determinarán reglamentariamente las categorías de datos que deben conservarse según el tipo de servicio prestado, el plazo de retención de los datos, la forma de tratarlos y la forma de entregarlos a las autoridades que los soliciten.

los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información.

El problema es que el precepto remite, para algunas cuestiones esenciales, a un desarrollo reglamentario que todavía no se ha producido. Y así, resulta que, aunque se establece la obligación de retener los datos necesarios para localizar el equipo a través del cual se ha realizado la conexión, no se precisa por cuanto tiempo deben conservarse esos datos. Es cierto que se contempla el plazo máximo de conservación, que será de un año, pero no el plazo mínimo.

La Ley General de Telecomunicaciones no ha resuelto este problema. El artículo 38.3 de la misma reconoce el derecho de los abonados a que «se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación» y a que los datos de tráfico necesarios a efectos de la facturación y los pagos de las interconexiones sean tratados «únicamente hasta que haya expirado el plazo para la impugnación de la factura del servicio o para que el operador pueda exigir su pago», pero ello «sin perjuicio de lo dispuesto en el artículo 12 LSSI». El precepto, difícil de conjugar con el artículo 12 LSSI[138], se centra únicamente en el plazo máximo de conservación de esos datos, pero no en el plazo mínimo de retención obligatoria.

> Con respecto al tiempo que han de conservarse los datos de tráfico se han pronunciado tanto el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE como la AEPD, pero siempre desde la perspectiva de la facturación de los servicios, por lo que no son concluyentes a los efectos que aquí nos interesan. Así, el Grupo de Trabajo del Artículo 29, en su dictamen 1/2003, sobre almacenamiento de los datos de tráfico a efectos de facturación, adoptado el 29 de enero de 2003, señaló que los datos deberían poder conservarse durante un tiempo comprendido entre 3 y 6 meses, con posibilidad de ampliar el plazo en caso de litigio. La AEPD, por su parte, en su Informe sobre conservación de los datos de facturación telefónica, opina que el plazo de conservación debe ser de tres meses, si la factura se ha pagado, y cinco años, si no ha sido así.

Ante la falta de desarrollo reglamentario del artículo 12 LSSI, cabrían dos posibilidades. La primera, entender que el artículo 12.1 establece el plazo máximo de conservación de los datos de conexión y tráfico, que será de un año, y habilita al Gobierno para establecer, si lo estima pertinente, un plazo mínimo de retención de esos datos. Esto significaría que no existe un deber de mantenimiento de los datos, y que, por consiguiente, ante un requerimiento judicial de revelación de estos datos, el PSL podría alegar que no los conserva, porque no tenía tal obligación. Esta interpretación no encaja, sin embargo, con el título del artículo, que es muy claro en cuanto a la finalidad del mismo: establecer un deber de retención de datos.

---

[138] Vid. GONZÁLEZ DE ALAIZA CARDONA, «La lucha de los titulares de derechos contra las redes "peer to peer" (P2P)», *cit.*, pág. 61, señalando que el artículo 38.3 ha derogado involuntariamente el plazo de un año previsto en el artículo 12.1 LSSI.

La segunda posibilidad, más razonable, es entender que el artículo 12.1 LSSI obliga a los PSL a retener los datos necesarios para localizar el ordenador utilizado por un usuario para conectarse a Internet, al mismo tiempo que habilita al Gobierno para fijar el plazo mínimo de mantenimiento de esos datos. Pero hasta que el Gobierno desarrolle reglamentariamente este artículo, no puede quedar vacío de contenido. Por ello, habrá que entender que los PSL tendrán que conservar los datos de conexión y tráfico durante un año.

VI. EL DERECHO DE INFORMACIÓN EN EL PROYECTO DE LEY POR LA QUE SE AMPLÍAN LOS MEDIOS DE TUTELA DE LOS DERECHOS DE PROPIEDAD INTELECTUAL E INDUSTRIAL Y SE ESTABLECEN NORMAS PROCESALES PARA FACILITAR LA APLICACIÓN DE DIVERSOS REGLAMENTOS COMUNITARIOS

En el apartado anterior hemos visto que hay argumentos en el derecho vigente para defender que los titulares de derechos de propiedad intelectual pueden solicitar a los tribunales civiles, por la vía de las diligencias preliminares, que requieran a los PSL para que revelen la identidad de quienes supuestamente han infringido sus derechos a través de redes P2P. Ello no es óbice, sin embargo, para que convenga aprovechar la transposición de la DRDPI para clarificar la situación, previendo expresamente un derecho de información como el del artículo 8 DRDPI, que hasta ahora no existe sino implícito en nuestra legislación.

Ya se han iniciado los trabajos para incorporar la DRDPI. En el BOCG de 28 de octubre de 2005 se publicó el Proyecto de Ley por la que se amplían los medios de tutela de los derechos de propiedad intelectual e industrial y se establecen normas procesales para facilitar la aplicación de diversos reglamentos comunitarios.

En lo que aquí nos interesa, el Proyecto prevé la modificación de la Ley de Enjuiciamiento Civil a fin de incorporar entre las diligencias preliminares del artículo 256 el derecho de información del artículo 8 DRDPI[139]. El texto propuesto en el artículo primero del Proyecto es el siguiente[140]:

---

[139] La Exposición de Motivos del Proyecto lo explica de la siguiente manera: «Bajo la denominación de derecho de información, la directiva considera necesario poder ofrecer, en el ámbito del proceso civil, cauces para obtener información sobre el origen y las redes de distribución de las mercancías o servicios en los que se concrete la infracción de los derechos de propiedad intelectual o industrial. La ley encauza la posibilidad de instar de un órgano jurisdiccional civil el requerimiento de esta información a través de una nueva diligencia preliminar dentro del artículo 256 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, si bien limita su posibilidad a la preparación de un juicio por una infracción de un derecho de propiedad intelectual o de propiedad industrial cometida mediante actos desarrollados con fines comerciales.
(...)
»La regulación de la práctica de estas nuevas diligencias está presidida por la doble cautela de garantizar la confidencialidad de la información requerida y de evitar que los datos obtenidos puedan utilizarse para fines distintos a la preparación del juicio».

[140] Se reproducen exclusivamente aquellos apartados que inciden sobre el tema que aquí nos ocupa.

«Uno. En el apartado 1 del artículo 256 se introduce un número 5.º bis, el actual número 7.º pasa a ser el 9.º y se introducen dos nuevos números, el 7.º y el 8.º, con la siguiente redacción:

(...)

7.º Mediante la solicitud, formulada por quien pretenda ejercitar una acción por infracción de un derecho de propiedad industrial o de un derecho de propiedad intelectual cometida mediante actos desarrollados a escala comercial, de diligencias de obtención de datos sobre el origen y redes de distribución de las mercancías o servicios que infringen un derecho de propiedad intelectual o de propiedad industrial y, en particular, los siguientes:

a) Los nombres y direcciones de los productores, fabricantes, distribuidores, suministradores y prestadores de las mercancías y servicios, así como de quienes, con fines comerciales, hubieran estado en posesión de las mercancías.

b) Los nombres y direcciones de los mayoristas y minoristas a quienes se hubieren distribuido las mercancías o servicios.

c) Las cantidades producidas, fabricadas, entregadas, recibidas o encargadas, y las cantidades satisfechas como precio por las mercancías o servicios de que se trate y los modelos y características técnicas de las mercancías.

Las diligencias consistirán en el interrogatorio de:

a) Quien el solicitante considere autor de la violación.

b) Quien, a escala comercial, haya prestado o utilizado servicios o haya estado en posesión de mercancías que pudieran haber lesionado los derechos de propiedad industrial o intelectual.

c) Aquel a quien los anteriores hubieren atribuido intervención en los procesos de producción, fabricación, distribución o prestación de aquellas mercancías y servicios.

La solicitud de estas diligencias podrá extenderse al requerimiento de exhibición de todos aquellos documentos que acrediten los datos sobre los que el interrogatorio verse.

8.º (...)

A los efectos de los números 7.º y 8.º de este apartado, se entiende por actos desarrollados a escala comercial aquellos que son realizados para obtener beneficios económicos o comerciales directos o indirectos.

Dos. El apartado 1 del artículo 257 queda redactado del siguiente modo:

1. (...)

En los casos de los números 6.º, 7.º, 8.º y 9.º del apartado 1 del artículo anterior, será competente el tribunal ante el que haya de presentarse la demanda determinada. Si, en estos casos, se solicitasen nuevas diligencias, a raíz del resultado de las hasta entonces practicadas, podrán instarse del mismo tribunal o bien del que, a raíz de los hechos averiguados en la anterior diligencia,

resultaría competente para conocer de la misma pretensión o de nuevas pretensiones que pudieran eventualmente acumularse.

Tres. Se adicionan dos nuevos apartados, el 3 y el 4, al artículo 259, con la siguiente redacción:

3. En el caso de las diligencias del artículo 256.1.7.º, para garantizar la confidencialidad de la información requerida, el tribunal podrá ordenar que la práctica del interrogatorio se celebre a puerta cerrada. Esta decisión se adoptará en la forma establecida en el artículo 138.3 y a solicitud de cualquiera que acredite interés legítimo.

4. La información obtenida mediante las diligencias de los números 7.º y 8.º del apartado 1 del artículo 256 se utilizará exclusivamente para la tutela jurisdiccional de los derechos de propiedad industrial o de propiedad intelectual del solicitante de las medidas, con prohibición de divulgarla o comunicarla a terceros. A instancia de cualquier interesado, el tribunal podrá atribuir carácter reservado a las actuaciones, para garantizar la protección de los datos e información que tuvieran carácter confidencial».

Cuatro. El artículo 261 queda redactado del siguiente modo:

Artículo 261. Negativa a llevar a cabo las diligencias.

Si la persona citada y requerida no atendiese el requerimiento ni formulare oposición, el tribunal acordará, cuando resulta proporcionado, las siguientes medidas, por medio de un auto, en el que expresará las razones que las exigen:

(...)

5.ª Tratándose de las diligencias previstas en el artículo 256.1.6.º, ante la negativa del requerido o de cualquier otra persona que pudiera colaborar en la determinación de los integrantes del grupo, el tribunal ordenará que se acuerden las medidas de intervención necesarias, incluida la de entrada y registro, para encontrar los documentos o datos precisos, sin perjuicio de la responsabilidad penal en que pudiera incurrir por desobediencia a la autoridad judicial. Iguales medidas ordenará el tribunal en los casos de los números 5 bis, 7.º y 8.º del apartado 1 del artículo 256, ante la negativa del requerido a la exhibición de documentos.»

El Proyecto ha venido a corregir algunas deficiencias importantes que presentaba el primer Anteproyecto procedente del Ministerio de Justicia, que en el tema objeto de este estudio contradecía abiertamente lo dispuesto por el artículo 8 DRDPI. En efecto, bastaba con fijarse en el elenco de sujetos a quienes, de acuerdo con el Anteproyecto, podría requerirse la información[141], y compararlo con el que contiene la Directiva, para apreciar que faltaba justamente el supuesto que aquí nos ocupa: el de quienes prestan a escala

[141] Establecía el Anteproyecto a este respecto:
«Las diligencias consistirán en el interrogatorio de:
a) quien el solicitante considere autor de la violación;
b) quien, con fines comerciales, haya utilizado servicios o haya estado en posesión de mercancías que pudieran haber lesionado los derechos de propiedad industrial o intelectual;
c) aquél a quien los anteriores hubieren atribuido intervención en los procesos de producción, fabricación, distribución o prestación de aquellas mercancías y servicios».

> comercial los servicios de los que se vale el infractor para cometer la infracción. Es posible que la omisión se debiera a un lapsus del Ministerio; pero también que fuera consciente. Podría, en efecto, responder al propósito de evitar la adopción de una medida sin duda impopular dentro del cada vez más nutrido colectivo de internautas. O, todo lo contrario, podría deberse a la intención de evitar reiteraciones, si se entiende, como se ha defendido más arriba, que el deber de información de los prestadores de servicios de la sociedad de la información, también en el ámbito civil, se encuentra ya recogido en el artículo 12 LSSI. Sea como fuere, la omisión era censurable, pues obligaba a los titulares de derechos de propiedad intelectual a justificar ante los tribunales que esa facultad que les reconoce el artículo 8 DRDPI está ya implícita en nuestro ordenamiento, como única vía para obtener las diligencias preliminares necesarias para preparar los juicios por infracción de sus derechos, y les dejaba a expensas de la interpretación que el juez en cuestión hiciera de nuestra legislación. Por ello, hay que aplaudir que, finalmente, en el Proyecto se haya incluido la posibilidad de solicitar como diligencias preliminares el interrogatorio de quienes prestan a escala comercial los servicios de los que se ha servido el supuesto infractor para violar los derechos de propiedad intelectual.

Entrando ya en el análisis somero del Proyecto, lo primero que hay que señalar es que ha optado por incorporar el artículo 8 DRDPI mediante el añadido de nuevas diligencias preliminares. Dicha vía no es contraria a la Directiva, por más que el derecho de información regulado en ésta se enmarque en procesos ya iniciados. Debe recordarse que la Directiva es de mínimos (art. 2 DRDPI), lo que permite a los Estados miembros incorporar o mantener medidas judiciales más beneficiosas para los titulares de derechos. Dado que es más beneficioso para los titulares de derechos poder averiguar la identidad de los supuestos infractores antes de iniciar el proceso con la correspondiente demanda o con la solicitud de medidas cautelares, hay que entender que la opción del Proyecto es válida.

La inclusión de nuevas diligencias preliminares en el listado del artículo 256.1 LEC conlleva la modificación de algunos otros preceptos del Capítulo II del Título Primero del Libro II de la LEC. Como es sabido, el régimen de todas las diligencias preliminares de la LEC es común, excepción hecha de algunas especialidades previstas en función de los supuestos concretos regulados. Por esta razón, el régimen de las diligencias de obtención de datos sobre el supuesto infractor de derechos de propiedad intelectual que actúa a través de redes P2P será el general de este Capítulo II, con las singularidades que pretende introducir el Proyecto. Ello justifica que aquí sólo se aluda a esas especificidades que presentan las diligencias de obtención de datos en el caso que nos ocupa.

Para empezar, el supuesto de hecho que permite la solicitud de diligencias de obtención de datos sobre el origen de la infracción es más restringido que el contemplado por el artículo 8 DRDPI. Según el Proyecto, procederá el interrogatorio de quienes presten a escala comercial servicios intermediarios, a fin de averiguar la identidad del supuesto infractor, cuando los actos que constituyen la alegada violación del derecho de propiedad intelectual se hayan

cometido también a escala comercial. A *sensu contrario*, si la infracción no se ha cometido a escala comercial, no será posible recurrir a la vía prevista por el proyectado artículo 256.1.7.º LEC. Sin embargo, no es eso lo que establece la Directiva. El artículo 8 DRDPI obliga a los prestadores de servicios a escala comercial a identificar a los destinatarios de sus servicios que supuestamente infringen derechos de propiedad intelectual o industrial, sin exigir que la infracción se haya cometido también a escala comercial. Es el servicio a través del cual se comete la infracción, y no la propia infracción, lo que tiene que desarrollarse a escala comercial. Por consiguiente, de acuerdo con la Directiva, en todo caso podrá pedirse al proveedor de acceso a Internet que identifique al usuario que intercambia sin autorización obras o prestaciones protegidas, aunque no lo haga con objeto de obtener beneficios económicos o comerciales directos o indirectos. Este matiz no se encuentra en el propuesto artículo 256.1.7.º LEC, que, por lo tanto, contradice lo dispuesto en la Directiva. Es cierto, sin embargo, que la amplitud del concepto «escala comercial» es tal, sobre todo a la vista de sus antecedentes en el ámbito comunitario, que potencialmente permite adoptar estas diligencias preliminares siempre que la infracción le ahorre al presunto infractor los costes de adquisición de la obra o prestación protegida. Pero no es menos cierto que constituye éste un argumento más teórico que práctico[142] y que, en todo caso, al menos en abstracto, se trata de una exigencia que empeora la posición de los titulares de derechos en España con respecto a lo dispuesto por el artículo 8 DRDPI[143], por lo que su definitiva adopción supondría un incumplimiento del las obligaciones de transposición de la DRDPI.

Una segunda especialidad que presenta la regulación propuesta es la relativa a la competencia judicial para resolver sobre estas diligencias preliminares. De acuerdo con el proyectado artículo 257.1 LEC, el órgano jurisdiccional competente para resolver sobre la solicitud de interrogatorio del proveedor de acceso a través del cual se han infringido los derechos de propiedad intelectual será el tribunal ante el que haya de presentarse la demanda determinada. Ello obliga a que sea necesariamente un Juzgado de lo Mercantil, que es el órgano competente por razón de la materia. Ahora bien, en cuanto a la competencia territorial, el Proyecto se está remitiendo implícitamente al artículo 52.1.11.º LEC, según el cual «en los procesos en los que se ejerciten demandas sobre infracciones de la propiedad intelectual, será competente el tribunal del lugar en que la infracción se haya cometido o existan indicios de su comisión o en que se encuentren ejemplares ilícitos, a elección del demandante». Esto plantea problemas en el ámbito en el que nos movemos, dado que, como siempre que nos enfrentamos ante violaciones de derechos de propiedad intelectual cometidas a través de Internet, es difícil determinar cuál es el lugar de comisión de la infracción. Puede entenderse que es el lugar desde el que se pone ilícitamente en

[142] Habrá que ver si los tribunales españoles consideran que un usuario de Internet que intercambia obras o prestaciones protegidas es un infractor a escala comercial.
[143] Es peor para los titulares de derechos tener que probar que la infracción se ha cometido a escala comercial, por amplio que pueda resultar este concepto, que no tener tal carga.

línea la obra o prestación protegida, o también que es el lugar desde el que la obra o prestación protegida puede descargarse. La segunda alternativa hace competente a cualquier tribunal de España, en la medida en que un archivo puesto a disposición del público a través de redes P2P puede descargarse, en principio, desde cualquier ordenador no sólo de España, sino del mundo. Por ello, a efectos de acotar la competencia territorial de alguna manera en el ámbito que nos ocupa [144], sería preferible la primera opción, que por otra parte es respetuosa con el segundo inciso del artículo 52.1.11.º, ya que el ordenador-servidor a través del cual se pone una obra o prestación protegida a disposición del público puede asimilarse al «lugar donde se encuentr[e]n ejemplares ilícitos». Ahora bien, sin conocer la identidad del supuesto infractor, tampoco podemos precisar desde dónde se comete la infracción. Lo más cercano al lugar de comisión de la infracción es el lugar donde esté establecido el PSL que proporciona acceso a Internet al supuesto infractor, que no tiene por qué coincidir con aquél [145]. Por ello, para el supuesto que nos ocupa, habría sido preferible mantener como criterio de competencia territorial el del domicilio del interrogado, que no presenta dudas.

Es posible que la información suministrada por el PSL sea por sí sola insuficiente para averiguar la identidad del supuesto infractor, porque nos lleve hasta la puerta de entrada a una red de área local o una *Intranet*. En este caso, para identificar al presunto infractor pueden ser necesarias, como antes vimos, nuevas diligencias preliminares, dirigidas esta vez contra quien controla esa red de área local integrada por múltiples usuarios que acceden a Internet a través de una única IP pública. De acuerdo con el proyectado artículo 257.1 LEC, en este caso las nuevas diligencias de obtención de datos podrán instarse ante el mismo tribunal que conoció las primeras, o ante el tribunal «que resultaría competente para conocer de la misma pretensión o de nuevas pretensiones que pudieran eventualmente acumularse». En este caso, este nuevo tribunal está territorialmente acotado, ya que ubicación de la red de área local desde la que se ha cometido la infracción puede precisarse.

El uso que el titular de los derechos puede hacer de la información obtenida a través de diligencias de obtención de datos es restringido. Como señala el artículo 259.4 LEC, según la redacción sugerida por el Proyecto, tales datos sólo podrán utilizarse para la tutela jurisdiccional de los derechos de propiedad intelectual del propio solicitante de las medidas. Por lo tanto, no podrá ceder esa información a terceros. Ello excluye la comunicación de los datos del supuesto

---

[144] Acotar la competencia territorial es razonable cuando la única relación del sujeto pasivo de las diligencias preliminares con la supuesta infracción es que sus servicios fueron utilizados por el presunto infractor para violar los derechos de propiedad intelectual. No lo es tanto, en cambio, cuando se trata de determinar el tribunal competente para conocer sobre la medidas cautelares solicitadas, o para resolver sobre el fondo del asunto, y ello porque quien comete una infracción a través de Internet asume que esa infracción surtirá efectos en cualquier lugar de España y, en consecuencia, asume también el riesgo de que se presente la demanda ante cualquier tribunal de España.

[145] Téngase en cuenta que en el intercambio de archivos a través de redes P2P descentralizadas, el más habitual hoy en día, la obra o prestación protegida se pone en línea a través del propio ordenador del infractor, y desde ahí la descargan directamente los demás usuarios.

infractor a otros titulares de derechos que puedan haberse visto perjudicados por la infracción. En cambio, en mi opinión no excluye a los representados del solicitante, en la medida en que éste actúe en nombre y por cuenta de aquéllos. Por consiguiente, una entidad de gestión que tiene encomendada por sus socios la defensa de sus derechos de propiedad intelectual y solicita diligencias preliminares para averiguar la identidad de los supuestos infractores, podrá comunicar a aquéllos la información obtenida, a los solos efectos de que éstos, en su caso, puedan también interponer la correspondiente demanda.

Por otra parte, y como es lógico, el que el uso de esta información sea restringido no quiere decir que el solicitante esté obligado a interponer una demanda contra el supuesto infractor. Puede tratar de solventar el problema extrajudicialmente, o simplemente optar, a la vista, por ejemplo, de un estudio prejudicial, por dejarlo estar. Igualmente, puede acumular a su acción por infracción de sus derechos de propiedad intelectual cualesquiera otras acciones conexas. Así, por ejemplo, la demanda podría ser por infracción de derechos de propiedad intelectual y competencia desleal. Lo que no cabría, entiendo, es aprovechar la información obtenida para interponer una demanda que no se fundara en la vulneración de sus derechos de propiedad intelectual.

Para terminar, hay que hacer referencia a una última cuestión. ¿Qué ocurre si el proveedor de acceso se niega a proporcionar la identidad del supuesto infractor? El artículo 261.5.ª de la LEC, según redacción prevista por el Proyecto, no contempla este supuesto, pero sí el de la negativa del obligado a informar sobre la supuesta infracción de derechos de propiedad intelectual cometida por medio de sus servicios a exhibir los documentos relacionados con la supuesta infracción, siempre que no medie oposición formal. Para este supuesto, el Proyecto permite que el tribunal ordene las medidas de intervención necesarias, incluida la de entrada y registro, sin perjuicio de la responsabilidad penal que pudiera derivarse de tal negativa. Creo que estas medidas son aplicables también en nuestro caso, en la medida en que la información que el PSL puede suministrar se encuentra en sus propias bases de datos. Aunque no se pida la exhibición de los documentos internos del proveedor de acceso, a partir de los cuales puede conocerse la identidad del supuesto infractor, lo que se solicita es que se dé testimonio de lo que figura en dichos documentos internos. Por consiguiente, si no lo hace voluntariamente, podrá la autoridad judicial ordenar la correspondiente intervención.