PROTECCIÓN DE DATOS VS. TUTELA JUDICIAL EFECTIVA EN CASOS DE INFRACCIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL

Por Ignacio Garrote Fernández-Díez
Profesor Titular de Derecho Civil
Universidad Autónoma de Madrid

Resumen: El objeto fundamental de este trabajo es profundizar en las relaciones existentes entre la protección de datos personales y la tutela judicial efectiva de la propiedad intelectual en el caso del intercambio de archivos en redes *peer-to-peer*. Para ello examinaremos cómo se ha procedido para identificar y condenar a los usuarios de este tipo de redes en distintos países de nuestro entorno, prestando una especial atención a aquellos en los que las acciones se han planteado en la vía civil. A continuación estudiaremos las dificultades que existen en España para recopilar las direcciones IP de usuarios de redes P2P de cara a presentar una eventual demanda en el orden civil frente a dichos usuarios. Para superar estas dificultades defenderemos la idea de que una dirección IP debe ser considerada en nuestra legislación como un «dato de tráfico», no un «dato de carácter personal». Después señalaremos cómo la protección del derecho a la tutela judicial efectiva de la propiedad intelectual exige que la legislación española sea interpretada de modo que resulte posible solicitar al juez civil que ordene a los prestadores de acceso la revelación de la identidad de la persona que contrató el servicio de conexión a Internet desde el que se intercambiaron los archivos. Para ello analizaremos la regulación de las diligencias preliminares que prevé el art. 256.1.7.º de la Ley de Enjuiciamiento Civil a la luz del Derecho europeo y de nuestra propia Constitución, así como el régimen previsto en la Ley 25/2007, 18 de octubre, de Conservación de Datos en las Comunicaciones Electrónicas. También veremos cómo la nueva regulación del art. 8 de la LSSI (en la redacción de la D.A. 3ª de la Ley 2/2011, de Economía Sostenible) puede ayudar a acabar con este «puerto seguro» que supone España para los usuarios de redes P2P.

Palabras Clave: Protección de datos, tutela judicial efectiva, Derecho constitucional, propiedad intelectual, intercambio de archivos, redes

de pares, legislación española, Derecho comunitario, Derecho comparado.

SUMARIO:

TITLE:

DATA PROTECTION VS. ONLINE COPYRIGHT ENFORCEMENT

ABSTRACT:

The main object of this article is to go deep into the complex relationships between data protection regulations and copyright enforcement on infringements occurring in peer-to-peer

networks. To do so we will examine how legislation in different countries has been used to identify and condemn P2P user in civil proceedings. We will then turn into the difficulties currently existing in Spain to collect the IP addresses of the users in order to prepare a civil damages claim against those users. To overcome such difficulties we will defend the idea that an IP address should be considered in our legislation a «traffic data», not a «personal data». We will then analyze how effective copyright enforcement calls for an interpretation of Spanish legislation that allows civil claimants to ask the judge an injunction to discover the identity of the user that requested the access service to the Internet used to interchange the files. To allow such an interpretation we will examine the regulation of injunctions provided by art. 256.1.7º of the Spanish Civil Procedure Law (Ley de Enjuiciamiento Civil) in the light of European Law and our own Constitution. We will also examine the provisions of Law 25/2007, October 18th, of Data Retention in Electronic Communications and how the new legal regime of art. 8 of the LSSI (in the text provided by Law 2/2011, of Sustainable Economy) can help to avoid that «safe harbor» that Spain is right now for P2P users.

KEYWORDS: Data protection, Copyright enforcement, Constitutional Law, Copyright, File exchanges, peer-to-peer networks, Spanish legislation, Community Law, Comparative Law.

CONTENTS:

I. INTRODUCCIÓN

La disposición adicional cuadragésimo tercera de la Ley 2/2011, de 4 de marzo, de Economía Sostenible (mal llamada en medios periodísticos «Ley Sinde») ha introducido algunas reformas en nuestra legislación con el objetivo declarado de luchar contra la piratería en Internet.

Para ello, además de dar una nueva redacción al art. 158 de LPI, ha introducido una nueva letra e) en el primer apartado del art. 8 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información (LSSI) que incluye la propiedad intelectual en un elenco de bienes jurídicos especialmente protegidos en el ámbito de la prestación de servicios en Internet.

También se ha incluido un nuevo apartado 2 en dicho artículo 8 de la LSSI con el objetivo facilitar la correcta identificación de los «responsables del servicio de la sociedad de la información» que estén llevando a cabo conductas que, presuntamente, vulneran los derechos de propiedad intelectual (por ejemplo, una página web desde la que los usuarios se pueden descargar archivos que contienen obras y prestaciones protegidas por la propiedad intelectual).

Para poder llevar a cabo esta identificación los órganos competentes podrán requerir a los prestadores de servicios de la sociedad de la información los datos personales del (presunto) infractor a fin de que pueda comparecer en el procedimiento de suspensión del servicio de que se trate (por ejemplo, la retirada o bloqueo de contenidos en páginas web). Para realizar dicho requerimiento será necesaria una autorización judicial previa, de acuerdo con lo previsto en el apartado primero del nuevo art. 122 bis de la Ley reguladora de la jurisdicción contencioso-administrativa (norma introducida también por esta D.A. 43 de la Ley de Economía sostenible).

Respecto de esta cuestión, hay que tener en cuenta que aunque el nuevo art. 8.2 de la LSSI señala literalmente que los destinatarios de dicho requerimiento son en general los «prestadores de servicios de la sociedad de la información», sin hacer mayores distingos, seguramente habrá que entender que la norma se está refiriendo específicamente a quienes poseen la información que se pretende

obtener, esto es, los «prestadores de servicios de intermediación», y, en especial, a los prestadores de acceso y de alojamiento de página web según la definición de estos servicios de la letra b) del Anexo de LSSI. De este modo, cuando el requerimiento obtiene la pertinente autorización judicial, los intermediarios están obligados a facilitar los datos necesarios para llevar a cabo la identificación del infractor. Entre dichos datos habrá que incluir todos aquellos que sean necesarios y suficientes para lograr dicha identificación, en especial el nombre y el domicilio del presunto vulnerador de los derechos de propiedad intelectual.

Con esta regulación, la «Ley Sinde» permite facilitar la identificación de los responsables de páginas web que se utilizan como plataformas para vulnerar los derechos propiedad intelectual de los creadores, bien alojando directamente los contenidos (páginas web que actúan como repositorios de contenidos de obras y prestaciones protegidas pirateadas), bien suministrando enlaces a otras páginas web que cumplen esta función de «almacén» desde el que los usuarios se descargan los archivos.

A este mecanismo de identificación se le une un nuevo procedimiento híbrido, entre administrativo y judicial, que dota a la recién creada Sección Segunda de la Comisión de Propiedad Intelectual de legitimidad para proponer la retirada de contenidos de la Red. De esta manera, la «Ley Sinde» pretende atajar una de las principales vías de infracción de derechos de propiedad intelectual en Internet, la que se lleva a cabo a través de páginas web.

Sin embargo, existe una segunda forma de piratería masiva en Internet, la que hacen posible las redes de intercambio de archivos (redes P2P o *peer-to-peer*). Se trata de programas informáticos mediante los cuales los usuarios ponen en un «fondo común» un repertorio variopinto de obras y prestaciones protegidas por la propiedad intelectual (fonogramas, grabaciones audiovisuales, programas de ordenador, videojuegos, fotografías, etc.) para ser intercambiados de forma gratuita.

Este intercambio compite directamente con la explotación comercial de los objetos protegidos por la propiedad intelectual, y por ello ha sido fuertemente combatido por las industrias culturales (en especial, en los Estados Unidos), bien reclamando responsabilidad civil y/o penal a los creadores de estos programas P2P[1], bien dirigiendo su mirada directamente frente a los verdaderos «infractores directos» de la propiedad intelectual, los propios usuarios.

[1] El más importante de ellos es la sentencia del Tribunal Supremo de los EE.UU, el conocido como «caso Grokster», en el que las compañías de productores discográficos y cinematográficos demandaron a la compañía creadora del programa *Grokster* (*Grokster Ltd*), a los creadores de *KaZaA* (tanto a la filial norteamericana como a su matriz holandesa) y a los de *Morpheus* (*StreamCast Networks, Inc*), solicitando una indemnización por la violación masiva de los derechos de propiedad intelectual que los usuarios cometían usando estos programas. En la sentencia de la Corte de Apelación del Noveno Circuito de 19 de agosto de 2004 se señaló que los creadores de

Dentro de este combate contra los usuarios de redes *peer-to-peer*, se han ensayado fundamentalmente dos estrategias distintas, aunque compatibles. La primera consiste en interrumpir el servicio de acceso a Internet a los usuarios, para lo cual los derechohabientes deben contar con la colaboración de las empresas que dan servicios de conexión a estos usuarios que intercambian los archivos (los «prestadores de acceso»). El objetivo último de esta estrategia no es por tanto reclamar responsabilidad al usuario, sino instar la cesación de la conducta infractora mediante el expediente técnico de interrumpir el servicio de conexión a Internet que prestan las empresas de telecomunicaciones a sus abonados.

Así, en algunos países (entre los que se incluye España), es posible demandar al prestador de acceso ante la autoridad judicial para solicitar que se interrumpa el servicio de conexión a la red de de los usuarios infractores mediante la interposición de medidas cautelares o acciones de cesación (arts. 139.1 h) y 146 LPI). Para ello no es necesario ni siquiera conocer la identidad civil de los infractores, el legitimado pasivo de la acción es el propio intermediario y la restricción del acceso se realizará simplemente respecto de una o varias direcciones IP «infractoras»[2].

En otros países se ha optado por un mecanismo que se basa en una serie de advertencias sucesivas dirigidas a los usuarios infractores (el llamado sistema de «respuesta gradual» o «sistema de los tres avisos»). Dicho sistema consiste básicamente en encomendar a una autoridad administrativa la labor de pedir a los tribunales que ordenen la interrupción del servicio de conexión a Internet a los usuarios a los que reiteradamente (hasta tres veces) se les ha advertido que el intercambio de archivos es una conducta infractora, como ocurre en Francia tras la polémica Ley HADOPI[3].

---

programas P2P no eran responsables desde el punto de vista de la propiedad intelectual de las infracciones que cometen sus usuarios, pero dicha sentencia fue posteriormente rectificada por la Corte Suprema de los Estados Unidos, que se pronunció sobre la cuestión en su sentencia de 27 de junio de 2005 (*Metro-Goldwyin-Mayer Studios Inc., v. Grokster, Ltd, et alt.,* 75 U.S. P.Q.2d, 1001), en la que, por votación unánime, se declara responsables a los operadores de estas empresas por las violaciones de los derechos de propiedad intelectual que cometen a diario los usuarios de las redes P2P que ellos mismo crearon y operan. Posteriormente, ulteriores resoluciones judiciales han confirmado que los creadores de redes P2P son responsables por las infracciones que cometen los usuarios que utilizan dichos programas, como ocurrió por ejemplo en el auto de la Corte de Distrito de Nueva York de 11 de mayo de 2010, en el caso de *Arista Records y otros vs. LimeGroup LLC* y otros, respecto del programa de intercambio *Limewire*.

[2] Vid. Garrote Fernández-Díez, I., «La suspensión cautelar o cesación definitiva de los servicios a los usuarios infractores de derechos de propiedad intelectual», *pe.i (Revista de Propiedad Intelectual),* núm. 27, 2007, pp. 13-55.

[3] La Ley HADOPI (Ley 2009-669 de 2 de junio de 2009, para favorecer la difusión y la protección de la creación en Internet, publicada en el *Journal Officiel* de 13 de junio de 2009) contenía inicialmente un sistema que permitía a una Comisión administrativa recibir las denuncias de los titulares y trasladarlas a los prestadores de acceso, que tenían que enviar avisos a sus clientes. Si tras dos de esos avisos el usuario seguía intercambiando archivos, la Ley permitía a la Comisión desconectar al usuario de la Red por un plazo máximo de un año. Este sistema fue declarado inconstitucional por la Decisión del Consejo Constitucional núm. 2009-550, de 10 de junio de 2009,

Este sistema de respuesta gradual se ha implementado también en países como Irlanda sin una reforma legal expresa, utilizando únicamente acuerdos de colaboración entre los titulares de derechos de propiedad intelectual (o entidades que les representan) y los distintos prestadores de acceso a la Red, acuerdos que permiten la desconexión del usuario sin necesidad de interponer medidas cautelares o acciones de cesación por vía judicial[4].

La segunda estrategia para atajar el fenómeno de las redes *peer-to-peer* ha consistido en demandar directamente a los usuarios para reclamarles por vía penal o civil la responsabilidad que les corresponde por el intercambio ilícito de archivos. Puesto que es evidente que los usuarios son los infractores directos de los derechos, su procesamiento y ulterior condena no ha planteado especiales problemas en el Derecho comparado.

Sin embargo, en España esta segunda vía de protección de los derechos de propiedad intelectual en Internet se ha encontrado con dos poderosos obstáculos que, considerados de forma conjunta, han logrado situar a los usuarios españoles de redes P2P en un particular estado de impunidad que resulta extraordinariamente llamativo si lo comparamos con los países de nuestro entorno.

---

publicada en el J.O. el mismo día 13 de junio, con el argumento de que la desconexión a Internet del usuario necesitaba una intervención judicial, lo que provocó que la versión finalmente publicada de la norma contenga un sistema distinto, en el que la autoridad administrativa debe comunicar a una serie de tribunales especiales (hasta 9 en toda Francia) la información de que se dispone, siendo el Tribunal el encargado de imponer la sanción tras un proceso rápido, sin intervenciones orales e *inaudita parte*. El órgano administrativo (la HADOPI) es la responsable de la ejecución de la sanción al abonado, que no disfrutará de conexión a la red pero sí mantendrá los servicios de televisión y teléfono en el caso de paquetes vendidos de forma unitaria.

[4] Este sistema permite en esencia la desconexión del usuario de la Red sin una intervención judicial, lo que ha provocado polémica desde el punto de vista constitucional. Para intentar atajar esta cuestión, la Directiva 2009/140/CE, del Parlamento Europeo y del Consejo de 24 de noviembre de 2009 modificó la Directiva 2002/21/CE de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas para añadir un nuevo apartado 3 bis en el art. 1 con el siguiente tenor: «*Las medidas adoptadas por los Estados miembros relativas al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas respetarán los derechos y libertades fundamentales de las personas físicas, como queda garantizado en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y en los principios generales del Derecho comunitario. Cualquiera de esas medidas relativas al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas, que sea susceptible de restringir esos derechos y libertades fundamentales solo podrá imponerse si es adecuada, proporcionada y necesaria en una sociedad democrática, y su aplicación estará sujeta a las salvaguardias de procedimiento apropiadas de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y con los principios generales del Derecho comunitario, que incluyen una protección judicial efectiva y un procedimiento con las debidas garantías. Por lo tanto, dichas medidas solo podrán ser adoptadas respetando debidamente el principio de presunción de inocencia y el derecho a la vida privada. Se garantizará un procedimiento previo, justo e imparcial, que incluirá el derecho de los interesados a ser oídos, sin perjuicio de que concurran las condiciones y los arreglos procesales adecuados en los casos de urgencia debidamente justificados, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales. Se garantizará el derecho a la tutela judicial efectiva y en tiempo oportuno*».

Desde el punto de vista penal la persecución de los usuarios de redes P2P se ha visto bloqueada en la práctica por la postura de la Fiscalía General del Estado, que mediante su Circular 1/2006 señaló que el intercambio de archivos por particulares en redes de pares no era una conducta susceptible de ser encuadrada en el art. 270 del Código Penal como delito contra la propiedad intelectual por faltar ánimo del lucro en el usuario[5]. Con dicha Circular se ha cegado en la práctica la vía penal[6] para los titulares de derechos, en claro contraste[7] con lo que está sucediendo en la mayoría de los países de la Unión Europea y en los Estados Unidos[8].

Pero lo verdaderamente llamativo de nuestro país es que la posición de los derechohabientes no es mucho mejor a la hora de reclamar la responsabilidad en el ámbito civil. En este caso las dificultades emanan principalmente del hecho de que el usuario de las redes P2P casi siempre actúa de forma anónima o amparándose en un «nickname» o alias que esconde su verdadera identidad. Debido a ello, los titulares de derechos no pueden conocer por sí mismos la identidad del usuario que está utilizando una red P2P concreta para intercambiar archivos de forma ilícita. La única forma que tienen de conocer dicha identidad para

---

[5] Esta falta de protección penal de los derechos de propiedad intelectual en Internet no se ha extendido sin embargo al ámbito de la propiedad industrial, en donde generalmente se obliga a los prestadores de acceso a colaborar con los titulares en casos de que se detecte una infracción. Es el caso por ejemplo, del auto del Juzgado de Instrucción núm. 32 de Barcelona de 17 de diciembre de 2007 (ARP/2008/217), que obligó como medida cautelar a los prestadores de acceso que operan en España a bloquear el acceso a sus usuarios al dominio *nikebrother.com*, en donde se vendían prendas deportivas piratas.

[6] A este respecto, parece claro que la última reforma del Código Penal en relación con la tipificación de los delitos contra la propiedad intelectual, la aprobada mediante Ley Orgánica de 5/2010, de 22 de junio pretende insistir esa misma línea de «despenalización» de las conductas atentatorias contra los derechos de propiedad intelectual (en este caso, respecto del llamado «Top Manta»). La reforma añadió un segundo párrafo al art. 270.1 CP que, en esencia, permite imponer al juez reducir la pena a multa de tres a seis meses o trabajos en beneficio de la comunidad de treinta y uno a sesenta días en los supuestos en los que haya «distribución al por menor y reducida cuantía del beneficio económico», atendidas las «características del culpable». Además, en esos supuestos, cuando el beneficio no exceda de 400 euros, el hecho punible se rebaja a la calificación de falta del art. 623.5 CP.

[7] No parece ser ajeno a este proceso el hecho de que en los círculos políticos parece percibirse la propiedad intelectual como un obstáculo para el pleno desarrollo de Internet y de la propia Sociedad de la Información, como expresamente se menciona en las Conclusiones del Informe de la Subcomisión creada en el seno de la Comisión de Cultura sobre la Reforma de la Ley 23/2006, en donde expresamente se señala que «*La Subcomisión considera que la legislación sobre propiedad intelectual debe atender, especialmente, al desarrollo de la sociedad de la información, para lo cual es fundamental promover nuevos modelos de negocio*» (BOCG, Congreso, Serie D, núm. 345, de 1 de marzo).

[8] En Estados Unidos el Informe anual sobre la piratería en el mundo de 2010 (el conocido *Special 301 Report*) sigue insistiendo, como ya lo hizo en 2009, en que la derogación de dicha Circular supone un elemento imprescindible para la suficiente protección de las industrias culturales en nuestro país. El informe está disponible en <http://www.iipa.com/2010_SPEC301_TOC.htm>. Vid. reseña y anotación de este informe, a cargo de S. López Maza, P. Mariscal Garrido-Falla, G. Minero Alejandre, N. Moralejo Imbernón y R. Sánchez Aristi, en *pe.i (Revista de Propiedad Intelectual)*, núm. 35, 2010, pp. 103-127.

interponer una acción indemnizatoria ante los Juzgados de lo Mercantil es que le sea revelada por el único que la puede conocer con certeza, el prestador de acceso que suministra el servicio de conexión a Internet al usuario.

Sin embargo, llegados a este punto, los prestadores de acceso de nuestro país (fundamentalmente, grandes empresas de telecomunicaciones), se han refugiado en la legislación comunitaria y española sobre protección de datos para evitar tener que revelar la identidad del usuario infractor. Dicha negativa ha sido en lo fundamental avalada tanto por el Tribunal de Justicia de la UE como por los jueces y tribunales españoles, creando en la práctica una «bahía pirata» para los usuarios de redes P2P españoles, que pueden llevar a cabo libremente la actividad de intercambio de archivos sin temor a represalias ni en el ámbito penal ni en el civil.

A partir de este escenario, el objeto fundamental de este trabajo es profundizar en el análisis de las dificultades que existen en España para lograr una condena indemnizatoria en el orden civil frente a los usuarios de redes de pares[9]. Se trata de una cuestión delicada, en la que hay que equilibrar cuidadosamente los derechos constitucionales implicados (derechos de propiedad intelectual y tutela judicial efectiva, de un lado y protección de datos, de otro) pero que, sin embargo, apenas ha merecido atención por parte de nuestros operadores jurídicos tras la regulación de la Ley 25/2007, de 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas.

Para llevar a cabo nuestro estudio comenzaremos haciendo un breve resumen de cómo se ha procedido en los países de nuestro entorno para identificar y condenar a los usuarios que intercambian archivos en redes P2P, prestando una especial atención a aquellas jurisdicciones en las que la acción contra los usuarios ha venido fundamentalmente por la vía civil.

A continuación, explicaremos cómo de acuerdo con la legislación española el intercambio de archivos en redes P2P constituye una vulneración de los derechos previstos en la LPI.

En tercer lugar estudiaremos las dificultades que existen en España para recoger y «tratar» una serie de direcciones IP de usuarios de redes *peer-to-peer* de cara a presentar una eventual demanda en el orden civil frente a dichos usuarios. Para ello defenderemos la idea de que una dirección IP[10] no debe ser

---

[9] Este artículo pretende profundizar y actualizar el trabajo realizado en dos magníficos trabajos por A. González Gozalo, artículos que han sido publicados en esta misma *Revista de Propiedad Intelectual*: «La propiedad intelectual y la protección de datos de carácter personal en las redes P2P», publicado en el número 28 y «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», publicado en el núm. 20.

[10] La dirección IP es un código numérico que identifica necesariamente a toda máquina que intercambia (envía o recibe) información en Internet por medio del protocolo TCP/IP. De este

considerada como un «dato de carácter personal», sino como un mero «dato de tráfico» de los regulados en la Ley 25/2007. Esto implica que es posible solicitar al juez civil una autorización para recoger y almacenar direcciones IP en casos de presunta vulneración de derechos de propiedad intelectual sin necesidad de sujetarse a las reglas y casos previstos en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal y en su normativa de desarrollo.

Por último, señalaremos cómo, a la luz del derecho de tutela judicial efectiva previsto en nuestra Constitución y del Derecho comunitario, la legislación española debe ser interpretada de modo que resulte posible solicitar al juez civil que los prestadores de acceso revelen a los derechohabientes la identidad de la persona que contrató el servicio de conexión a Internet desde el que se intercambiaron los archivos. Para ello analizaremos la regulación de la Ley de Conservación de Datos de 2007 y las diligencias preliminares que, para la materia concreta de propiedad intelectual, prevé el art. 256.1.7.º de la Ley de Enjuiciamiento Civil. También veremos cómo la nueva regulación del art. 8 de la LSSI, en la redacción otorgada por la «Ley Sinde», puede ayudar, de forma modesta e indirecta, a acabar con este «puerto seguro» que la legislación española prevé para los usuarios de redes P2P.

II. INFRACCIÓN EN REDES P2P E IDENTIFICACIÓN DEL USUARIO EN EL ÁMBITO INTERNACIONAL

En los países de nuestro entorno tanto los legisladores como los tribunales desde un principio tuvieron claro que el principal responsable de la infracción de los derechos de propiedad intelectual en redes *peer-to-peer* es el usuario[11]. Y ello porque estamos ante auténticos actos de piratería, a pesar de que normalmente se lleven a cabo en la intimidad del hogar o en el puesto de trabajo[12].

En lógica consecuencia, y con el objetivo de atajar este tipo de intercambios, tanto en los Estados Unidos[13] como en la Unión Europea (Ita-

---

modo cada ordenador tiene una IP singular que permite la eficiente distribución de los datos (es la «dirección» a la que tienen que remitirse los paquetes de datos).

[11] En esto la doctrina en España y en Derecho Comparado es unánime. Vid., a modo de ejemplo, Ginsburg, J.,/Gaubiac, Y., «Contrefaçon, fourniture de moyens et faute: perspectives dans les systèmes de *Common Law* et civilistes à la suite des arrêts *Grokster* et *Kazaa*», *RIDA,* núm. 207, enero 2006, p.17.

[12] Así lo señalan Bercovitz Rodríguez-Cano, R., y Marín López, J.J., «El límite de copia privada y las redes de intercambio peer to peer», *Cuadernos de Derecho Judicial,* 2007-3, p. 153.

[13] En este país ya desde el año 2002 se plantearon diversas iniciativas legislativas en este sentido. La más conocida fue seguramente la *Author, Consumer, and Computer Owner Protection and Security Act 2003* (más conocida por sus iniciales, ACCOPS), que preveía por medio de su § 301 reformar la § 506 (a) de la *Copyright Act* para convertir en una infracción penal el hecho de «*introducir una obra protegida, sin la autorización de su titular, en una red de ordenadores accesible por miembros del público que sean capaces de copiar la obra mediante dicho acceso*». Existía por tanto una sanción penal directa para todo usuario que introdujera en una red P2P una obra o prestación protegida,

lia[14], Francia[15]) se han realizado mejoras legislativas para clarificar las normas existentes en materia de propiedad intelectual, tipificando como conducta ilícita el intercambio de archivos en redes P2P. En otros países sin embargo (como Alemania) no se ha considerado necesaria una reforma expresa de la legislación por entenderse que la conducta ilícita del usuario encaja en la normativa vigente mediante una sencilla labor interpretativa[16].

---

pero finalmente la ACCOPS no superó el trámite legislativo. Después, el debate en los Estados Unidos se trasladó de la sede parlamentaria a la judicial, quedando claro que la solución de la Corte Suprema del «caso Grokster» y las distintas demandas que se estaban planteando contra usuarios individuales concretos iban a hacer innecesaria una decisión legislativa concreta, evitando así el coste político que este tipo de norma podría tener para el legislador.

[14] En Italia la sentencia penal de la *Corte de Cassatione* de 9 de enero de 2007 señaló que no cabía condenar penalmente a unos estudiantes de la Universidad Politécnica de Turín que habían habilitado un servidor FTP para el intercambio de archivos que contenían, entre otros contenidos protegidos, programas de ordenador y videojuegos. Pero la sentencia aplica la legislación vigente en el momento de comisión de los hechos, es decir, 1999. Después, se promulgó en Italia el 12 de marzo de 2004 un Decreto Ley (el conocido como «Decreto Urbani»), que modificaba el art. 171-ter de la Ley italiana de Derecho de Autor de 22 de abril de 1941 para incluir como ilícito administrativo la difusión al público por vía telemática de obras cinematográficas o asimiladas protegidas por el derecho de autor, o de partes de estas, mediante redes o conexiones de cualquier género, incluyendo los programas de intercambio de archivos. Poco tiempo después la Ley núm. 128, de 21 de mayo de 2004 cambió las sanciones administrativas a los usuarios por sanciones penales, ampliando además el abanico de conductas delictivas al incluir en el art. 171-ter.2 de la LDA la conducta de quien, «*en violación del art. 16, y para obtener provecho, comunica al público, introduciendo en un sistema de redes telemáticas, mediante conexiones o de cualquier otro género, una obra protegida por el derecho de autor, o parte de esta*». La pena prevista en este caso puede oscilar entre uno y cuatro años de prisión, aunque, como en España, la exigencia del ánimo de lucro plantee la duda de si se está incluyendo en la norma a los usuarios de redes P2P.

[15] En Francia, el texto de la Ley núm. 2006-961 aprobado por la Asamblea Legislativa francesa contenía inicialmente una polémica reducción de las penas previstas para quienes intercambiaban contenidos en redes P2P mediante la redacción de un nuevo art. 335.11 PI, que convertía dicho delito en una mera falta (*contravention*). Sin embargo, dicha reducción fue considerada por el Consejo Constitucional como discriminatoria en relación con las infracciones que no se llevaban cabo a través de este tipo de redes (que deberían afrontar penas mayores), de manera que finalmente se mantuvieron para estos infractores las mismas penas que existen para el resto (hasta tres años de prisión y multa de hasta 30.000 euros). Posteriormente, y como antes mencionamos, la respuesta legislativa en Francia no se ha centrado tanto en la definición de la conducta ilícita o la gravedad de la pena como en un sistema de supervisión por un órgano administrativo (la HADOPI) que permite tras una serie de avisos previos desconectar de la red a un usuario infractor. Con todo, existen también sanciones penales si el usuario es reincidente en la infracción. Así, el art. 336-2 del *Code de Propriété Intellectuelle* impone a los prestadores de acceso la obligación de informar a los internautas de los peligros que implica el intercambio de archivos, mientras que el art. 331-2 obliga a que la conexión a Internet no sea utilizada para intercambios ilícitos de material protegido. Vid. Sobre esta cuestión Lucas-Schloetter, A., «La Loi Française relative au droit d'auteur dans la société de l'information», *pe.i (Revista de Propiedad Intelectual),* num. 25, 2007, p. 42.

[16] A nivel comunitario carecemos de una norma clara. El debate se centró en la fracasada Directiva del Parlamento europeo y del Consejo relativa a las medidas penales destinadas a garantizar el respeto de los derechos de propiedad intelectual, en cuyo trámite ante el Parlamento Europeo se introdujo una enmienda en el art. 2 de la norma al objeto de excluir la relevancia penal de los actos efectuados por los usuarios con fines personales y no lucrativos, lo que fue interpretado como un mensaje para despenalizar el intercambio de archivos en redes P2P. La propuesta inicial de Directiva tiene como referencia COM(2005) 276 final, y la Propuesta Modificada, COM(2006) 168 final, de 26 de abril de 2006.

A partir de esta consideración del intercambio de archivos como conducta ilícita se planteó en los países de nuestro entorno la cuestión previa de si los prestadores de servicios de acceso a Internet tenían o no la obligación de desvelar a los demandantes la identidad de la persona que se «esconde» tras una IP determinada desde la que se han detectado intercambios ilícitos. Pues bien, como veremos a continuación, en la práctica totalidad de los casos se ha entendido que dicho suministro de direcciones IP supone un paso necesario para la defensa de los derechos de propiedad intelectual, por lo que los prestadores de acceso no podían negarse a facilitarlos. Y ello incluso cuando las demandas a los usuarios se planteaban únicamente en el orden civil.

1. Estados Unidos: las *John Doe Actions*

Seguramente el primer lugar donde se plantearon demandas frente a usuarios individuales de redes *peer-to-peer* fue en los Estados Unidos. Pero tan pronto como los titulares de derechos emprendieron acciones legales, se encontraron con la reticencia de los prestadores de acceso a revelar la identidad de sus clientes en el marco de dichas acciones.

El punto de desacuerdo en un principio era que en la § 512 (h) de la *Digital Millenium Copyright Act* de 1998 se preveía la posibilidad de que los prestadores de servicios intermediarios comunicaran directamente a los interesados que se lo solicitaran a través de una petición autorizada por un oficial judicial (*subpoena*) las identidades de los abonados que infringieran derechos de propiedad intelectual. Así, aunque algunos prestadores de acceso sí facilitaron dichos datos voluntariamente a los titulares por esta vía (dando lugar a una batería de demandas en septiembre 2003 contra unos 250 usuarios) otros se negaron a ello, de manera que la cuestión acabó en los tribunales.

La resolución de este asunto tuvo lugar mediante la sentencia de la Corte de Apelación del Distrito de Columbia de 19 de diciembre de 2003[17], que señaló que la § 512 (h) de la *Digital Millenium Copyright Act* no se aplicaba a los prestadores de acceso a la red (en el caso, la empresa *Verizon*), con el argumento de que la norma estaba pensada únicamente para los prestadores de alojamiento respecto de los datos de los operadores de páginas web. Esta doctrina del caso *Verizon* fue después confirmada por otras Cortes de Apelación (por ejemplo, la del Octavo Circuito de 4 de enero de 2005[18]) convirtiéndose así en doctrina consolidada.

---

[17] *Recording Industry Association of America Inc., v. Verizon Internet Services, Inc*, sentencia de 19 de diciembre de 2003, 341 F.3d, 1299.

[18] *Charter Communications Inc, y otros v. RIIA y otros,* 2005 WL 15416. En este caso la *RIAA* demanda a un prestador de acceso (*Charter*) solicitando que revele las identidades de algunos de sus clientes, que están intercambiando ilícitamente fonogramas a través de sistemas P2P. El juez

Ante este hecho, la estrategia de las industrias culturales norteamericanas se centró en presentar demandas individuales contra usuarios desconocidos (*John Does*), de modo que fuera el propio juez el que requiriera mediante diligencia a los prestadores de acceso la información sobre los usuarios que actúan bajo al aparente anonimato de una dirección IP.

Y esta estrategia ha tenido éxito en prácticamente todos los tribunales de los Estados Unidos, en donde a partir un auto pionero de 2005[19] los jueces obligan a los prestadores de acceso a desvelarles la IP de los usuarios infractores ante la simple presentación de un principio de prueba razonable (*fumus boni iuris*) por parte de los derechohabientes.

Con este método, los titulares de derechos norteamericanos han logrado desde el año 2006[20] numerosísimas condenas contra usuarios de redes P2P[21] por infracción de la Sección 506 (a) (1) (A) de la *Copyright Act*[22]. Algunas de ellas

---

de primera instancia obliga a *Charter* a revelar la identidad de los clientes que están detrás de las IP solicitadas. *Charter* apela. La Corte de Apelación

[19] La primera de ellas fue la del auto de la Corte de Distrito de Columbia de 2 diciembre de 2005, en el caso de *Paramount Pictures Corp. v. John Davis (*235 F.R.D. 102). En este caso, es una productora audiovisual (*Paramount*) la que demanda a un usuario de *eDonkey*, que había ofrecido en dicha red P2P una copia de una película producida por ella. *Paramount* demuestra que apenas una semana después de su estreno en las salas de cine la película ya había sido puesta en *eDonkey* por una persona que utilizó para dicha puesta a disposición del público una dirección IP determinada. Tras interponer la correspondiente *John Doe action*, *Paramount* solicita al prestador de acceso al que pertenece la IP, *Comcast;* que le comunique la identidad civil del infractor. Ante la negativa de *Comcast*, *Paramount* recurrió ante la Corte del Distrito de Columbia, quien, por medio de auto de 3 de marzo de 2005, obligó a *Comcast* a desvelar quién había utilizado la IP y el día y hora de la puesta a disposición ilícita. Descubierta de este modo la identidad del ahora demandado, John Davis, *Paramount* reclamó daños y perjuicios por la puesta a disposición ilícita de la película en *eDonkey*.

[20] Seguramente la primera de dichas acciones que acaba con una condena al usuario, y no con una transacción es la sentencia de 10 de abril de 2006 (*Disney Enterprises, Inc., v. Kathy Farmer*), en la que se condena a la demandada, la señora Farmer, a una indemnización de 1.200 dólares por cada una de las películas de Disney que la señora había intercambiado gracias a una aplicación P2P. En este caso, las compañías acuden a la *John Doe action*, solicitando a la Corte de Distrito de Georgia (donde reside el prestador de acceso, *BellSouth*) que ordene a dicho prestador la identificación del infractor que actúa tras el apodo de «Farmer». Obedeciendo la orden de la Corte de Georgia, *BellSouth* identifica a la infractora como Kathy Farmer, residente en Tennessee. Una vez que ha logrado identificar al infractor, *Disney* demanda a la señora Farmer en Tennesse, obteniendo en un juicio en rebeldía (*default*) un auto de medidas cautelares que condena a la cesación de la actividad infractora. La señora Farmer recurre el auto de medidas cautelares, pero la Corte de Distrito de Tennessee lo confirma, ordenando la cesación definitiva de la conducta (*permanent injuction*) y la prohibición de reanudar la actividad infractora. Además, condena a la demandada a una indemnización de 1.200 dólares por cada una de las películas que puso a disposición del público, y a abonar las costas del proceso (*attorney's feees*), puesto que la infracción ha sido dolosa.

[21] Así ha ocurrido por ejemplo con la actividad de los productores discográficos norteamericanos (RIAA), que desembocó en una oleada de demandas que, a lo largo de casi seis años, alcanzó a casi 30.000 usuarios (aunque en la gran mayoría de los casos se llega a un acuerdo extrajudicial que resolvió el caso).

[22] Vid, por ejemplo, *Tanya Andersen v. Atlantic Recording Corporation y otros*, auto de U.S. District Court, D. Oregon, de 12 de noviembre de 2009, (93 U.S.P.Q. 2d 1047), rechazando el recurso de la condenada por el intercambio; o el caso contra uno de los líderes del grupo «Elite Torrents»,

han sido además especialmente rigurosas, como ocurre por ejemplo con la famosa resolución de la Corte de Distrito de Massachusetts de 9 de julio de 2010[23], que condenó a un usuario a abonar una indemnización de 2.250 dólares *por cada una* de las treinta canciones que compartió utilizando programas de intercambio de archivos.

2. Países de la Unión Europea

En distintos países europeos también se han iniciado acciones judiciales, tanto en el orden penal como en el civil, contra usuarios individuales de redes *peer-to-peer*, fundamentalmente a iniciativa de los productores musicales y audiovisuales. Para ello los titulares han acudido a los jueces para que estos requirieran a los prestadores de acceso la identidad de los infractores, procediendo inmediatamente contra dichos usuarios una vez que habían sido identificados.

Y en estos casos, los Tribunales de los distintos Estados miembros de la UE generalmente han entendido que los prestadores de acceso están obligados a comunicar al juez dichos datos de acuerdo con la legislación comunitaria y nacional aplicable.

Ello es desde luego así en los países en los que el intercambio de archivos está considerado como una infracción penal contra los derechos de propiedad intelectual. Así ocurre por ejemplo en Bélgica desde el año 2003[24] o en Francia[25] y

---

Daniel Dove, condenado a dieciocho meses de prisión por este tipo de intercambios (*Arista Records y otros vs. Daniel Dove*, sentencia de U.S. District Court, W.D., Virginia, de 7 de noviembre de 2008-585 F. Supp.2d 865).

[23] 721 F. Supp. 2d 85. Aunque la sentencia puede parecer rigurosa desde el punto de vista europeo, en realidad, redujo la indemnización fijada en un principio, que era de 675.00 dólares en concepto de «daños estatutarios» por infracción dolosa de los derechos de propiedad intelectual de las compañías discográficas actoras.

[24] Creo que la primera sentencia en este sentido es la del *Tribunal de Premiére Instance de Bruxelles (Penal)* de 28 de abril de 2003, en la que un joven que intercambia por Internet miles de ficheros Mp3 mediante el sistema FTP es declarado penalmente responsable, aunque la condena es suave por la juventud del infractor (25 euros y tres años de prisión, que quedan en suspenso).

[25] En Francia en realidad se resuelve simultáneamente la cuestión en la vía penal y en la vía civil, pero en todo caso se han producido numerosas condenas penales a usuarios individuales por intercambiar ficheros musicales o audiovisuales en redes P2P. Es el caso, por ejemplo, de la sentencia del *Tribunal de Grande Instance de Vannes* de 29 de abril de 2004. Los actores (algunos productores audiovisuales franceses, la asociación que les agrupa —FNDF— y la entidad de gestión SACEM) demandan a seis usuarios que se ponen en contacto por medio de un sitio web (*www.echange-cd.fr.st*) y que posteriormente, gracias al programa *KaZaA,* intercambiaban ficheros audiovisuales en formado *DivX que contienen grabaciones audiovisuales del repertorio de los actores. Para ello presentan como prueba las «capturas» de pantalla realizadas por la gendarmería francesa, en las que se «documentaba» cómo se perfeccionó la transacción. Un registro domiciliario confirma que el disco duro del ordenador de uno de los usuarios tiene 198 CD en formato *DivX puestos en la «carpeta compartida» de *KaZaA*. El Tribunal condena a cinco de los usuarios por un delito de reproducción ilícita a penas que van entre los 2000 y 5.800 euros y al que compartía en *KaZaA* las 198 películas en *DivX a tres meses de prisión. Desde ese momento de 2004, la jurisprudencia

Alemania[26] desde el año 2004, en los que el propio juez instructor de la causa o, en su caso, el Fiscal, solicita a los prestadores de acceso la identificación del infractor, procediendo después al correspondiente procesamiento penal.

Pero incluso en algunos países en los que la presión judicial contra los usuarios se ha centrado fundamentalmente en la vía civil los jueces no han dudado en obligar a los prestadores de acceso a que faciliten la identidad de los usuarios infractores[27].

Así ocurre por ejemplo en el *Reino Unido*[28], en donde se ha considerado aplicable al caso de las redes P2P la doctrina de la *Norwich Pharmacal order*[29], que en esencia implica que quien asiste a otro a cometer un acto ilícito sin conocimiento de dicha ilicitud no resulta responsable de la misma, pero deviene obligado a facilitar toda la información de la que disponga, incluido el nombre del infractor.

---

penal ha sido constante, como ocurre en los tempranos ejemplos de la sentencia del Tribunal de *Grande Instance de Rodez* de 13 de octubre de 2004 (sobre grabaciones audiovisuales) y la sentencia del *Tribunal de Grande Instance de Pontoise* de 2 de febrero de 2005, en la que se condena a un usuario por haber intercambiado en una red P2P archivos musicales a una multa de 3.000 euros. Y lo mismo ocurre con las resoluciones dictadas en procesos de apelación, como la de la *Cour de Appel de Aix-en-Provence* de 5 de septiembre de 2007, que condena al pago de una multa de 15.000 euros, o la de la *Cour de Appel de Versailles* de 16 de marzo de 2007, que impone una pena de prisión de tres meses.

[26] En Alemania la jurisprudencia ha considerado que la conducta de los usuarios de este tipo de redes es un ilícito penal que debe llevar aparejada una pena de multa de hasta 10.000 euros, toda vez que durante el trámite parlamentario de la segunda Ley de Reforma de 2007 se eliminó una propuesta que hubiera eximido de responsabilidad penal a quienes intercambien copias para uso privado «en un número limitado». Ello ha provocado que las condenas a los usuarios individuales de redes P2P se hayan sucedido en la jurisprudencia germana desde la sentencia del *Amtgericht Cottbus* de 6 de mayo de 2004, en la que se condena a un usuario de *KaZaA* a pena de multa de 400 euros por haber puesto a disposición del público 272 archivos musicales.

[27] Resulta peculiar la situación en Italia, en donde se ha entendido que los prestadores de acceso no tenían la obligación ni de comunicar los datos de sus usuarios a los derechohabientes, ni de monitorizar a los usuarios para detectar cuáles de ellos estaban usando la red para intercambiar archivos y bloquear las páginas web que suministran enlaces a redes P2P. Así ha ocurrido en el caso *FAPAV vs. Telecom Italia,* auto de 15 de abril de 2010, en una demanda promovida por la *Federación contra la Piratería Audiovisual* italiana contra el mayor prestador de acceso italiano, *Telecom Italia*. Con todo, el Tribunal sí ha afirmado que es la autoridad judicial la competente para solicitar los datos personales de los usuarios, de conformidad con lo establecido por la Ley, lo que abre la puerta a posibles demandas en el orden civil. La decisión contrasta con otra anterior en el caso *Techland Sp. Z O.O. e Peppermint Jam Records GmbH vs Wind Telecommunicazione*, auto del Tribunal de Roma (Sección IX, Civil), de 14 de julio de 2007, en el que una discográfica alemana pretendía demandar a más de 3.000 usuarios que habían sido detectados intercambiando fonogramas en redes P2P. El Tribunal Civil de Roma afirmó que el tratamiento de direcciones IP por parte de una empresa contratada por la productora al efecto había sido ilícito por no contar con el consentimiento de los interesados, posición que fue poco después adoptada también por la Autoridad nacional italiana en materia de protección de datos.

[28] En realidad en el Reino Unido, como en Francia, se utiliza una diversidad de sanciones civiles o penales, dependiendo de la gravedad de la conducta infractora.

[29] La sentencia que la estableció originariamente fue *Norwich Pharmacal Co v. Customs and Excise Comrs,* 1974, A.C. 133 [H.L].

La doctrina fue aplicada por primera vez en supuestos de usuarios de redes *peer-to-peer* en el caso *Universal Island Records Ltd. y otras contra NTL Group Ltd y otro*s (auto de la *High Court of Justice [Chancery Division*], de 14 de octubre de 2004[30]), decisión a la que luego siguieron muchas otras tanto en Inglaterra como en Irlanda del Norte.

Posteriormente, el debate sobre el posible «tratamiento» de direcciones IP como cuestión relacionada con la protección de datos hizo necesaria la intervención del legislador, que reguló específicamente la cuestión en las secciones 124 A a 124 N de la *UK Digital Economy Act 2010,* aprobada el 8 de abril de 2010[31].

Dicha Ley prevé que el proceso de identificación del usuario se inicie con una labor investigadora de los titulares, que envían al prestador de acceso una serie de direcciones IP desde las que se han detectado actividades de intercambio de archivos que presuntamente vulneran los derechos de propiedad intelectual, solicitando la identificación de los usuarios que utilizaron dichas IP en un día y a una hora determinada.

El prestador de acceso debe verificar si la solicitud cumple con los requisitos formales que la ley señala y si los datos de conexión que proporcionan los titulares coinciden con los que ellos mismos tienen registrados. De ser así, el prestador de acceso envía una carta de aviso a los usuarios que están llevando a cabo las presuntas conductas infractoras. Dicha notificación consiste en un simple aviso de que la dirección IP que se les asignó ha sido utilizada para el intercambio ilegal de materiales protegidos por los derechos de propiedad intelectual, especificando cuáles son las normas jurídicas implicadas[32].

El prestador de acceso también tiene la obligación de guardar y mantener un archivo con el número de avisos enviado a cada uno de sus abonados, puesto que puede ser requerido por los titulares para que les envíe una lista en la que consten los usuarios así notificados y el número de avisos que ha recibido cada uno. En dicha lista no consta aún el nombre y la dirección de los usuarios, solo su *username* o apodo (*nickname*).

Gracias a esta lista, los titulares pueden identificar a los usuarios reincidentes (que siguen intercambiando archivos pese a las advertencias) y luego llevarla al juez civil para que emita un auto en el que condene al prestador de acceso a revelar la identidad de aquellos que, pese a los avisos, continúan con la

---

[30] Vid. el resumen que hace de esta cuestión González Gozalo, «El conflicto entre la propiedad intelectual y el derecho a la protección de datos de carácter personal en las redes P2P», cit., p. 43, nota al pie 52.

[31] La norma está en vigor desde el 12 de junio de 2010.

[32] Vid. Ryan, J, en «Internet Access Controls: Three Strike's Graduated Response' Initiatives», cit, p. 12.

conducta infractora. Si el prestador de acceso se niega a cumplir sus obligaciones tras la orden judicial, la multa que se le impone puede ascender hasta las 250.00 libras.

Una vez que el juez ordena que se desvele dicha identidad y el prestador de acceso contesta, el juzgado remite dicha respuesta a los titulares, que deben mandar un «aviso final» al usuario en el que le solicite la cesación total de la conducta infractora y se le deje claro que el siguiente paso, si este aviso final es ignorado, será una acción judicial. Si aún así, el usuario no interrumpe la conducta infractora, los titulares de derechos pueden proceder por vía judicial contra el usuario.

En la práctica la puesta en vigor de este sistema se ha condicionado a que la autoridad reguladora del mercado de las telecomunicaciones, OFCOM, apruebe un procedimiento técnico que aclare cómo deben llevarse a cabo las labores de detección de direcciones IP, qué pruebas deben aportarse al prestador de acceso para demostrar que ha existido *prima facie* una infracción, cómo puede el usuario oponerse al proceso y los formularios de las distintas notificaciones que se utilizarán en el proceso. Dicho procedimiento tiene que ser en principio consensuado entre los titulares de derechos, los prestadores de acceso y las organizaciones de consumidores, pero, a falta de acuerdo, será redactado por la propia OFCOM[33].

Además, la Ley ha sido combatida desde el punto de vista de la protección de datos personales de los usuarios, pero las alegaciones en este sentido han sido descartadas por la sentencia de la High Court de 20 de abril de 2011, que resuelve un recurso de dos de los principales prestadores de acceso del Reino Unido, *British Telecom* y *Talk Talk*.

En *Irlanda*, la tensa relación entre la protección de los datos personales y los derechos de propiedad intelectual se ha dirimido en una larga batalla judicial entre los productores de fonogramas irlandeses y el mayor prestador de acceso de Internet del país, *Eircom*, que comienza con el auto de *Emi Records y otros v. Eircom Ltd. y BT Communications Ireland Ltd*[34].

---

[33] En un principio la Ley no prevé la posibilidad de interrumpir el servicio a los usuarios infractores, aunque la Sección 124G de la Ley prevé que pasado un año desde que el reglamento redactado por OFCOM entre en vigor, el Secretario de Estado pueda emitir resoluciones administrativas para imponer «Obligaciones técnicas» a los prestadores de acceso, lo que puede incluir la desconexión del servicio a los usuarios infractores o la atribución de un ancho de banda limitado, que les pueda permitir enviar o recibir correos y navegar por la Red, pero no intercambiar archivos. Con todo, estas futuribles «obligaciones técnicas» deberán ser aprobadas de nuevo por las dos cámaras del Parlamento británico, e implementadas conforme a un nuevo código que debe ser redactado por OFCOM (vid. RYAN, J, en «Internet access controls: Three Strike's graduated response' initiatives», p. 13).

[34] Auto del *High Court of Justice (Commercial),* de 8 de julio de 2005, [2006] E.C.D.R.5.

En el caso los titulares de derechos solicitaron al juez que obligara a *Eircom* a descubrir la identidad de diecisiete usuarios que habían utilizado redes P2P para intercambiar archivos que contenían fonogramas cuyos derechos pertenecían a las compañías demandantes. Aunque no existían en aquel momento precedentes en el Derecho irlandés ni jurisprudencia al respecto (más allá de la *Norwich Pharmacal order* inglesa), el juez señaló que los demandantes tienen derecho a que los prestadores de acceso revelen la identidad de sus abonados si se cumplen ciertos requisitos que el juez cree que se dan en el caso de autos.

El primero es que exista una apariencia de buen derecho para la petición, que consiste en una demostración *prima facie* de que ha habido infracción de derechos de propiedad intelectual. El segundo, que no haya otro medio razonable para obtener la identidad de los presuntos infractores, como ocurre en el caso de la infracción a través de redes *peer-to-peer*. Y el tercero y último, que la información obtenida únicamente sea utilizada para la preparación de una eventual acción judicial contra estos infractores, respetando su derecho a la intimidad y sin comunicar dicha identidad a terceros no interesados.

Dicho auto fue recurrido, y tras casi cuatro años de disputas, las partes alcanzaron un acuerdo extrajudicial el 28 de enero de 2009 por el cual *Eircom* se comprometía en el futuro a informar a sus subscriptores de que la IP que se les había asignado había sido detectada como una IP desde la que se infringían derechos de propiedad intelectual. La compañía de telecomunicaciones se comprometió además a avisar al usuario de que a menos que cesara en su conducta infractora sería desconectado de la red y a desconectar efectivamente al usuario que hiciera caso omiso de la advertencia.

Dicho acuerdo fue recurrido ante la *High Court of Justice* por la autoridad administrativa de protección de datos (el *Data Comissioner*), por entender que implicaba por parte de *Eircom* un «tratamiento» de direcciones IP, direcciones que debían ser consideradas como datos personales protegidos por la legislación irlandesa y comunitaria.

Sin embargo, la sentencia de la *High Court of Justice* de 16 de abril de 2010[35] rechaza dicha pretensión y aprueba en lo sustancial el acuerdo, con el argumento ciertamente revelador de que «*ni DtecNet* [la empresa encargada por los productores para compilar las IP infractoras]... *ni ninguno de los demandantes cuyos derechos de autor han sido infringidos podría saber a partir de dicho proceso que el infractor es una persona determinada con un domicilio determinado en Irlanda*. *Lo que sí saben es que esa dirección IP concreta ha estado involucrada en la descarga* (la traducción es mía)».

[35] [2010] IEHC 108.

El argumento principal de la sentencia es por tanto evidente: la dirección IP no hace por sí misma a una persona identificable, únicamente indica a los derechohabientes (o a cualquier persona que forme parte de la red *peer-to-peer*) desde qué ordenador se están intercambiando contenidos. Sólo el prestador de acceso (*Eircom*) puede saber a partir de dicha dirección IP quién contrató el acceso a Internet de la máquina.

En un caso similar, *Emi Records (Ireland) y otros vs. UPC Communications Ireland Ltd.,* otra sentencia de la *High Court* de 11 de octubre de 2010[36] ha reiterado en el marco de unas medidas cautelares de cesación la obligación de identificar a los usuarios que intercambian archivos en redes P2P por medio de las *Norwich orders*, aclarando también que el acuerdo entre *Eircom* y las discográficas únicamente vincula a las partes que lo suscribieron, y no al resto de prestadores de acceso[37].

Observamos por consiguiente que tanto en el Reino Unido como en Irlanda se han arbitrado mecanismos (legislativos en un caso, judiciales en otro) para obligar a los prestadores de acceso a desvelar la identidad de usuarios de Internet que intercambian contenidos protegidos por la propiedad intelectual en redes P2P en el marco de procedimientos civiles.

Pero la imposición de dicha obligación no sólo se ha producido en países de la tradición del *Common Law*, sino también en países europeos en los que ni siquiera se discute que las direcciones IP deban de consideradas como «datos de carácter personal» de acuerdo con la legislación nacional aplicable.

Así ocurre por ejemplo en *Holanda,* en donde su Tribunal Supremo (*Hoge Raad*) declaró en su sentencia sobre el asunto *Lycos/Pessers* de 25 de noviembre de 2005 que las leyes holandesas de protección de datos personales no impedían que se revelara la identidad de los usuarios en el marco de un proceso civil sobre infracción de derechos de propiedad intelectual siempre que se dieran tres condiciones que el propio Tribunal establece en su sentencia.

En primer lugar, que haya una presunción razonable de que el usuario ha llevado a cabo una conducta ilícita que perjudica al demandante. En segundo lugar, que el solicitante de la información demuestre tener un interés legítimo en obtener el nombre y la dirección del usuario. Y, en tercer lugar, que no debe haber un medio menos intrusivo para obtener los datos que el requerimiento al prestador de acceso[38].

---

[36] La sentencia está disponible en <http://es.scribd.com/doc/39104491/EMI-v-UPC>.

[37] Vid. el parágrafo 60 de la sentencia.

[38] Así se resume la sentencia en el Estudio encargado por la Comisión titulado «Study on Online Copyright Enforcement and Data Protection in Selected Member States», disponible en <http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_042010_en.pdf>. La doctrina de esta sentencia ha sido luego aplicada en, al menos, otros dos casos resueltos por

Es importante señalar que en el caso *Lycos/Pessers* los datos solicitados eran los de un operador de un sitio web, no los de un usuario de una red *peer-to-peer*. Sin embargo, en un Estudio publicado por la Comisión de la UE en 2010 se afirma que el Ministerio de Justicia holandés entiende que la doctrina de *Lycos/Pessers* es conforme con la sentencia del TJCE en el asunto *Promusicae* (a la que luego nos referiremos), lo que conduce al Estudio a afirmar que es probable que los jueces holandeses ordenen que se desvelen los datos personales también en el caso de usuarios de redes P2P si se cumplen en el supuesto enjuiciado los criterios sentados por el *Hoge Raad*.

Algo similar ocurre en *Suecia,* en donde es posible solicitar a los prestadores de acceso que revelen la identidad de los usuarios de redes P2P en el marco de procesos civiles de infracción de derechos de propiedad intelectual, previa autorización judicial, de acuerdo con el art. 53 c) de la Ley de Derecho de Autor sueca (modificada a tal efecto el 1 de abril de 2009)[39].

Dicha autorización judicial sólo se concede si el solicitante demuestra con un principio de prueba razonable que se ha cometido una violación de sus derechos exclusivos y se puede presumir razonablemente que la información va a servir para facilitar la investigación de la infracción. También deberá superarse un test de proporcionalidad, de modo que la finalidad legítima de protección debe prevalecer sobre los inconvenientes que supone que se tome esta medida.

El último ejemplo que podemos citar a nivel europeo es el de *Polonia*, en donde los prestadores de acceso tienen la obligación de revelar la identidad de los usuarios que han utilizado determinadas direcciones IP para intercambiar archivos como paso previo a una eventual demanda en el orden civil a partir de una decisión de la Autoridad nacional polaca de protección de datos de 2004 que entendió que la tutela judicial civil de los derechos era un «interés legítimo suficiente» para establecer dicho deber[40].

Por tanto, resumiendo lo visto hasta ahora, en la práctica totalidad de los países europeos el intercambio de archivos protegidos se configura como una conducta ilícita. Si la conducta se considera delito, el propio Juez penal puede autorizar la recogida y tratamiento de direcciones IP y solicitar a los presta-

---

tribunales inferiores, el de *Stitching BREIN vs. KPN* (sentencia de *Rechtbank* de La Haya de 5 de enero de 2007) y el de *Stitching BREIN vs. Leaseweb* (sentencia de *Hof Amsterdam* de 3 de julio de 2008). Hay que señalar sin embargo, que, en ambos casos, se solicitaban los datos de operadores de sitios web, no de usuarios individuales de redes P2P.

[39] Vid. el Informe de la Comisión de septiembre de 2009 titulado «Study on Online Copyright Enforcement and Data Protection in Selected Member States», disponible en la dirección de Internet <http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf>, p. 48.

[40] Así se señala en el Informe de la Comisión de abril de 2010 titulado «Study on Online Copyright Enforcement and Data Protection in Selected Member States», disponible en la dirección de Internet <http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_042010_en.pdf >, p. 17.

dores de acceso que revelen la identidad de los usuarios que utilizan redes P2P para infringir derechos de propiedad intelectual. Ello ha conducido a numerosas condenas a estos usuarios en países como Estados Unidos, Bélgica, Francia o Alemania.

Y si la demanda se plantea únicamente en el orden civil, hay algunos países europeos (Reino Unido, Irlanda, Holanda, Suecia, Polonia) en donde se considera lícita la recogida y tratamiento de las direcciones IP de los usuarios para preparar la correspondiente demanda, pudiéndose luego requerir al prestador de acceso por parte del juez civil para que revele a los titulares de derechos de propiedad intelectual el nombre y dirección de los presuntos infractores. Ello permite identificar a los usuarios también en estos supuestos en los que la conducta del usuario no se tipifica como delito.

III. LA SITUACIÓN EN ESPAÑA. EL INTERCAMBIO DE ARCHIVOS COMO CONDUCTA INFRACTORA

Con nuestra Ley de Propiedad Intelectual en la mano resulta indiscutible que los usuarios de programas de intercambio de archivos son responsables por violar los derechos de propiedad intelectual de los titulares de obras o prestaciones protegidas que se contienen en dichos archivos.

En concreto, respecto del derecho de autor, la introducción de una obra en la «carpeta compartida» de una aplicación P2P (como *Bittorrent*, *Emule*, o similares), implica la confección de reproducción no autorizada de acuerdo con el art. 18 LPI.

En el caso de los titulares de derechos afines, esta misma conducta infringe de forma directa el derecho de reproducción que otorgan los arts. 107.1 LPI (a los artistas, intérpretes y ejecutantes), 115.1 LPI (a los productores de fonogramas) y 121.1 LPI (a los productores de grabaciones audiovisuales). El «uploading» de contenidos en este tipo de redes no puede quedar además nunca amparado por el límite de copia privada del art. 31.2 LPI[41], pues se está haciendo un uso colectivo de la copia incompatible con esta excepción.

Además, la subida de contenidos a una red de intercambio de archivos no sólo supone una infracción del derecho de reproducción, también implica una puesta a disposición al público de los contenidos protegidos (que quedan en una «carpeta compartida, al alcance de los demás usuarios de la red de intercambio) que

---

[41] En el mismo sentido, Bercovitz Rodríguez-Cano, R., y Marín López, J.J., «El límite de copia privada y las redes de intercambio peer to peer», cit., p. 176, González de Alaiza, J.J., «La lucha de los titulares contra las redes «peer-to-peer»», cit., p. 53 y Aparicio Vaquero, J.P., «El intercambio de archivos en redes de pares a la luz del derecho vigente», cit., p. 69.

tiene que estar autorizada por los titulares de derechos en virtud de los arts. 20.2 i), 108.1 b), 116.1 y 122.1, todos ellos de la Ley de Propiedad Intelectual.

Así lo señala la doctrina de forma unánime[42], y así lo han afirmado en alguna ocasión nuestros Tribunales[43] *obiter dicta* en supuestos en los que se demandaba a los administradores de páginas web que contiene enlaces que activan las aplicaciones de intercambio de archivos que funcionan con protocolos «torrent», o similares[44].

Con estas premisas, es claro que la dificultad principal con que se encuentran en este ámbito los derechohabientes no es argumentar por qué los usuarios de las redes P2P infringen sus derechos de propiedad intelectual, sino cómo localizar a quienes llevan a cabo la actividad de intercambio de forma aparentemente anónima gracias a la utilización de un alias, apodo o «nickname».

Pues bien, para lograr dicha identificación, los titulares deben realizar una operación que consta de dos pasos. El primero consiste en averiguar y anotar la dirección del Protocolo de Internet (dirección IP) desde la cual se han puesto a disposición del público los archivos, lo que plantea la cuestión previa de si una dirección IP puede ser considerada como un «dato de carácter personal» a efectos de esta recogida y tratamiento.

Una vez recogidas y anotadas las IP desde las que se han producido los intercambios ilícitos de archivos, y la fecha y la hora en la que se produjeron dichos intercambios, los derechohabientes deberán solicitar al juez civil que ordene a los prestadores de acceso que desvelen la identidad de la persona a

---

[42] Vid. Bercovitz Rodríguez-Cano, R., y Marín López, J.J., «El límite de copia privada y las redes de intercambio peer to peer», cit., p. 164, González de Alaiza Cardona, J.J., «Napster «Copias robadas», responsabilidad de los intermediarios y otros interrogantes para el derecho de autor en Internet», cit., p. 74 y también en «La sentencia de la Corte Suprema estadounidense en el caso Grokster: La matizada condena a los operadores P2P», cit., p. 146, Plaza Penadés, J., *Propiedad Intelectual y Sociedad de la Información*, Aranzadi, 2001, p. 211, Bouza, M.A., y Castro Marques, M., «El caso Napster», en *Actas de Derecho Industrial y Derecho de Autor*, Tomo XXI-2000, Santiago de Compostela, 2001, p. 442.

[43] Así ocurre por ejemplo, en el Auto de la AP de Murcia de 16 de septiembre de 2009, en el caso de *elitedivx.com*, en donde la AP señala expresamente que la conducta de los usuarios supone no sólo un acto de reproducción no autorizado, sino también un acto de comunicación pública que infringe los derechos de los titulares. Algo similar ocurre con la sentencia de la AP de Barcelona de 24 de febrero de 2011 (caso *El Rincón de Jesús*), que puede encontrarse reseñada en este mismo número por S. López Maza.

[44] Los creadores de este tipo de páginas lo que hacen es «colgar» en la web una lista de enlaces (en realidad, una base de datos de enlaces) que los usuarios «cortan y pegan» en sus programas P2P para iniciar el proceso de descarga de los archivos en redes como *edk2* (la utilizada por aplicaciones como *Emule*) y las que utilizan la tecnología del protocolo *bitorrent* (como el cliente del mismo nombre). Estos sitios *web* de provisión de enlaces son especialmente útiles en programas P2P que no cuentan con un servicio de búsqueda de archivos (como suele ocurrir en las aplicaciones que intercambian ficheros *torrent*) o simplemente para localizar el archivo concreto que interesa al usuario a partir de un buscador de Internet como *Google*.

la que está vinculada dicha IP (quien contrató la cuenta de acceso a Internet a la que se asignó la IP utilizada para el intercambio de archivos), lo que abriría el camino a una demanda indemnizatoria contra un usuario identificado con nombre y apellidos, como el exige el art. 399.1 LEC.

En esta segunda fase del proceso el problema estriba fundamentalmente en determinar si en la legislación española el prestador de acceso tiene que revelar al juez dentro del marco de un proceso civil la identidad de un usuario que utilizó una IP un día y a una hora determinada para intercambiar archivos protegidos por la propiedad intelectual. Veamos ahora ambas cuestiones por separado.

IV. RECOPILACIÓN DE DIRECCIONES IP PARA PREPARAR UNA DEMANDA EN EL ORDEN CIVIL CONTRA USUARIOS DE REDES P2P

Los problemas fundamentales que plantean la recogida y tratamiento de direcciones IP durante la preparación de procesos civiles de defensa de los derechos de propiedad intelectual son dos. Por un lado, si con dicha recogida se está respetando el derecho al secreto de las comunicaciones de los usuarios. Y, por otro, si es necesario el consentimiento del usuario (o, en su defecto, la correspondiente exención administrativa o autorización judicial) para recoger y tratar esas direcciones IP por estar ante un «dato de carácter personal».

1. El proceso técnico de obtención de direcciones IP y el secreto de las comunicaciones

Debido al modo en el que funcionan este tipo de redes, todos los usuarios de un programa P2P deben «descubrir» su dirección IP durante el proceso de intercambio de los archivos. Esta dirección IP es la que individualiza a cada ordenador que está conectado a la Red, de manera que si conocemos una IP, sabemos desde qué ordenador se han transmitido una serie de archivos en un día y a una hora concreta.

En realidad, el proceso para averiguar desde qué IP se ha transmitido un archivo concreto es técnicamente muy sencillo: las más de las veces no hay más que echar un vistazo a la propia pantalla del ordenador, pues la mayoría de aplicaciones P2P nos suministran este dato por defecto.

Por tanto, para obtener un listado de direcciones IP «infractoras» (direcciones que han sido utilizadas para intercambiar archivos ilícitos) los derechohabientes (o un tercero contratado a tal efecto) únicamente tienen que buscar a través de una aplicación P2P concreta (un programa como *Ares*

o *Emule*) un archivo que contenga una obra o prestación protegida sobre la que ostenten derechos. Viendo los resultados de esta búsqueda se puede fácilmente obtener una lista de todas las IP desde las que se está poniendo a disposición del público ese archivo concreto, así como el seudónimo o *nickname* que se está utilizando para el intercambio (por ejemplo, *anonimo@ares.com*).

Una vez localizadas las direcciones IP de los usuarios que ofrecen un archivo concreto, los derechohabientes pueden perfeccionar el acto de descarga para comprobar que el archivo está efectivamente disponible en la carpeta compartida (asegurándose así, por ejemplo, de que no se trata de un error en el sistema de búsqueda) y que el archivo contiene una obra o prestación protegida por la propiedad intelectual.

Naturalmente, el proceso ulterior de identificación del usuario sería mucho más sencillo si cada IP se correspondiera con un ordenador concreto conectado a Internet. Sería como la matricula de un coche, que siempre identifica al mismo vehículo. Sin embargo, dado que el número de direcciones IP que tiene un prestador de acceso está limitado (suele haber más usuarios que direcciones IP disponibles), la mayoría de las IP que existen actualmente son dinámicas, es decir, se asignan al usuario cada vez que éste se conecta a Internet y únicamente durante el tiempo que dure la conexión.

De ahí que en este proceso de recogida de información previo a cualquier demanda por intercambio de archivos en redes P2P sea necesario que los titulares recolecten además del alias del usuario y su dirección IP, el día y la hora de conexión. Sólo así puede saberse con toda precisión a qué máquina se había asignado una IP dinámica en un intervalo de tiempo concreto.

En todo caso, resulta evidente que este proceso de recolección de direcciones IP por parte de los titulares en modo alguno vulnera el secreto de las comunicaciones del art. 18.3 de la Constitución española.

El motivo es que quien anota las direcciones IP (sea un derechohabiente, sea un tercero por su cuenta) es parte activa en el proceso de comunicación, forma parte de ella, y por tanto no está interceptando una comunicación ajena[45]. Así lo ha declarado de forma clara la jurisprudencia de la Sala 2ª del Tribunal Supremo (SSTS de 28 de mayo de 2008[46] y 14 de julio de 2010[47]), que señalan que la garantía constitucional del art. 18.3 CE no es aplicable a la comunicación que ocurre a través de programas P2P.

---

[45] Así lo entiende también, creo que con acierto, González de Alaiza, J.J., «La lucha de los titulares contra las redes «peer-to-peer»», cit., p. 601.
[46] RJ 2008/3441.
[47] RJ 2010/3509.

A esta misma conclusión debemos llegar aplicando el Derecho comunitario y, en especial, la regulación del art. 2 b) de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (en adelante Directiva sobre la Intimidad en las Comunicaciones Electrónicas o DICE).

A la vista de dicha norma, es indiscutible que la dirección IP y el día y la hora de la conexión son «datos de tráfico» en el sentido de la Directiva[48], pero estos datos de tráfico no están amparados por el principio de confidencialidad de las comunicaciones que sienta la Directiva (art. 5.1)[49]. El principio de confidencialidad respecto de los datos de tráfico se refiere por tanto a los intermediarios que hacen posible la comunicación de dichos datos, y a cualquier tercero que quiera conocerlos, pero no a los propios protagonistas de la comunicación (en nuestro caso, todos los usuarios de una red P2P).

2. Discusión sobre la dirección IP como «dato de carácter personal»

Aunque, como acabamos de ver, los derechohabientes que recogen direcciones IP para preparar demandas en el orden civil no están infringiendo con dicha conducta el secreto de las comunicaciones, existe un fuerte debate a nivel europeo sobre si pueden llevar a cabo dicha actividad a la luz de la regulación sobre la protección de datos de carácter personal.

1. *Postura mayoritaria: las direcciones IP son un «dato de carácter personal»*

a) La cuestión a nivel europeo y en España

La idea de que una dirección IP (incluso si es una IP dinámica, que se va a asignando a ordenadores personales de forma sucesiva) es un «dato de carácter personal» cuajó desde muy pronto tanto a nivel europeo como español.

Seguramente el origen de esta postura es un Informe del *Grupo de Trabajo sobre Protección de datos del art. 29* titulado «Intimidad e Internet (enfoque comu-

---

[48] Lo mismo ocurre en nuestra legislación a la vista del art. 64 a) del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios. Dicha norma prevé que *a los efectos de este título* son datos de tráfico cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas, o a efectos de su facturación, definición en la que encajan la dirección IP, el día y la hora de la conexión.

[49] Así lo señala, a mi juicio correctamente, González Gozalo, A., «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», cit., p. 97.

nitario integrado del tratamiento de datos en línea)» de 21 de noviembre de 2000[50], en el que se señalaba que una IP es un dato personal porque, conforme al art. 2 a) de la Directiva 95/46/CE, sobre Protección de Datos de Carácter Personal, permite identificar a una persona *de una forma razonable* a la luz del Considerando 26 de la precitada Directiva, que aclara que «*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*».

Dicha conclusión se vio reforzada por el Dictamen 4/2007 de dicho Grupo de Trabajo, de 20 de junio de 2007[51], que vuelve a reflejar la convicción de este grupo de expertos de que las direcciones IP deben ser consideradas como datos de carácter personal[52], aunque el propio Informe señaló con carácter preventivo que el alcance de las normas de protección de datos «no deben llevarse hasta sus extremos» ni aplicarse a «situaciones para las que no fueron concebidas por el legislador».

A partir de ambos trabajos, se produjo después un refuerzo a nivel comunitario de la protección de la IP como un «dato protegido» gracias a dos normas distintas. Por un lado, por la regulación del art. 6 de la Directiva sobre la Intimidad en las Comunicaciones Electrónicas. Por otra, por la regulación de los «datos de tráfico» de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas (en adelante, Directiva de Conservación de Datos en las Comunicaciones Electrónicas o DCDCE).

En efecto, el art. 6 DICE estableció el principio general de que los llamados «datos de tráfico» (entre los que se incluyen las direcciones IP) sólo pueden ser conservados y tratados para los fines que la propia Directiva (o cualquiera otra norma comunitaria prevea). La regla general será entonces la protección de estos datos a nivel comunitario, que sólo podrán ser utilizados en ciertas condiciones (por ejemplo, para facturar, *ex* art. 6.2 DICE). De este modo, el principio básico quedaba fijado: la dirección IP es un «dato de tráfico», que sólo puede ser tratado en circunstancias excepcionales y previa habilitación normativa.

Posteriormente, la Directiva de Conservación de Datos en las Comunicaciones Electrónicas abundó en dicha tendencia. Así, cuando la Directiva define en el

---

[50] Documento 5063/00/ES/FINAL, disponible en formato PDF en la dirección de Internet <http// www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37es.pdf>.

[51] Dictamen 4/2007 sobre el concepto de datos personales, disponible en formato PDF a partir de la dirección <ec.europa.eu/justice_home/fsj/privacy/docs/.../wp136_es.pdf>.

[52] Se señala expresamente en la página 18 de dicho informe que cuando se pretende identificar a los usuarios de un ordenador para demandarle por violación de los derechos de propiedad intelectual, dicha información debe ser considerada como «datos personales».

art. 5 los datos a los que resulta de aplicación (los datos que los operadores de telecomunicaciones deberán conservar de acuerdo con el deber general previsto en el art. 3) se menciona expresamente «*el nombre y la dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo Internet (IP), una identificación de usuario o un número de teléfono*» (art. 5.1 a) 2) iii) de la Directiva).

De este modo, el reforzamiento de la IP como un «dato de tráfico» con una protección similar a la de los datos personales es evidente, aunque indirecto. Se produce de forma fundamental porque una dirección IP (que es un mero «dato de tráfico»), se coloca al mismo nivel que la propia identificación del usuario (que está mencionado en el apartado i) de este art. 5.1 a) 2), que es sin duda un dato de carácter personal.

Es claro por tanto que en esta DCDCE late la idea de que las reglas de protección de datos de carácter personal son también aplicables, *mutatis mutandis*, a los meros «datos de tráfico». Así se desprende especialmente del Considerando 15 de la DCDCE, que expresamente señala que tanto la Directiva 95/46/CE, sobre Protección de Datos Personales, como la DICE son plenamente aplicables a los datos conservados de conformidad con esta Directiva.

A partir de esta base legislativa, existe un buen número de países comunitarios (Alemania, Austria, Suecia) en donde las autoridades nacionales de protección de datos y los tribunales entienden que las direcciones IP son datos de carácter personal porque permiten identificar a una persona por medios razonables[53].

En el Derecho español, la definición más aproximada de lo que es una dirección IP es la del art. 3.2 i) de la Ley de Conservación de Datos, que es la norma que implementa en España la DCDCE.

En concreto, esta LCDCE obliga a los prestadores de servicios de acceso a Internet a conservar «la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación». El concepto de dirección IP se maneja por tanto fundamentalmente, como en el Derecho comunitario, para definir las obligaciones de los prestadores de acceso a Internet en cuanto a la retención de datos, asumiendo como dato previo que estamos ante un código numérico que se asigna a una comunicación. Pero no hay ni una definición técnica de lo que debe ser una «dirección IP», ni, por supuesto, una mención expresa a que las direcciones IP deben ser consideradas en nuestro Derecho como «datos de carácter personal».

---

[53] Vid. el Informe de la Comisión de septiembre de 2009 titulado «Study on Online Copyright Enforcement and Data Protection in Selected Member States», disponible en <http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf>, pgs, 10, 30 y 44.

A falta de esta previsión expresa de nuestro legislador, la idea de que una dirección IP es un «dato personal» que goza de la protección otorgada por la LOPD ha sido obra fundamentalmente de la Agencia Española de Protección de Datos (AEPD), que a partir de los trabajos y normas comunitarias antes citadas ha afirmado en reiteradas ocasiones el carácter de «dato personal» de la dirección IP desde un primer informe del año 2003[54]. Dicho informe fijó una posición inicial que se ha mantenido inalterable desde entonces pese a los numerosos cambios legislativos producidos a nivel nacional y comunitario, y que ha sido aceptada por la generalidad de nuestra doctrina[55], aunque nunca haya sido confirmada a nivel jurisprudencial.

b) Recopilación y tratamiento de direcciones IP si aceptamos que son «datos de carácter personal»

Admitir que una dirección IP es un dato de carácter personal no implica sin embargo renunciar a su recogida y tratamiento en la preparación de pleitos civiles. Y ello porque un análisis de la legislación en la materia (como ha hecho entre nosotros González Gozalo) demuestra que cuando los titulares recopilan direcciones IP para preparar una eventual demanda frente a usuarios de redes P2P no están infringiendo la regulación de la LOPD, tanto si el proceso se hace forma manual como si se realiza de forma automatizada.

En efecto, es claro que incluso asumiendo que las direcciones IP son datos de carácter personal resulta muy dudoso que una lista de direcciones IP utilizada para preparar una eventual demanda contra un usuario de redes P2P (sobre todo si está confeccionada a mano) pueda ser considerada como un «fichero de datos de carácter personal» en el sentido de la LOPD.

El motivo es que la Ley (art. 3 b) LOPD) exige que haya un «conjunto *organizado* de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso», y no parece que una mera lista de direcciones IP tenga dicha organización (imaginemos, por ejemplo, que se han anotado en un papel escrito a ordenador una serie de direcciones IP, junto con el día y la hora en la que se realizó la conexión).

A estos efectos, la doctrina ha señalado[56] que no sólo ha de atenderse al hecho cualitativo de que los «datos» no tengan criterios para su ordenación y sistema-

[54] Informe 327/03, disponible en la dirección <https://www.agpd.es/index.php?idSeccion=150>.

[55] Vid. en ese sentido González Gozalo, A., «La propiedad intelectual y la protección de datos de carácter personal en las redes P2P», *pe.i, (Revista de Propiedad Intelectual),* núm. 28, 2008, p. 17 y la explicación detallada de la postura de este autor en «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», cit, pp. 94-96 y 11-112.

[56] González Gozalo, A., «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», cit., p. 114.

tización, sino también a un criterio cuantitativo, señalando que, por ejemplo, resulta difícil pensar en que una mera lista de diez direcciones IP sea un fichero en el sentido de la LOPD. Ello naturalmente implica que en estos supuestos no sea de aplicación lo dispuesto en el art. 4 del Real Decreto de Medidas de Seguridad ni el resto de la normativa de la LOPD (especialmente respecto de la notificación previa a la Agencia del art. 26.1 LOPD), normas que habría que cumplir si entendiéramos que una lista de direcciones IP es un «fichero» sometido a tratamiento en el sentido de la LOPD.

Cuando los titulares de derechos de propiedad intelectual utilizan por sí mismos o con la ayuda de terceros programas informáticos inteligentes para rastrear de forma automatizada las redes P2P y configurar (ahora sí), auténticos ficheros de direcciones IP, resulta evidente que procede la aplicación de la LODP si pensamos (en contra de lo que se mantiene en el presente trabajo) que una IP es un «dato de carácter personal».

Esto implicará plantearse si es necesario requerir del usuario el consentimiento para obtener dicho «dato», de acuerdo el principio general del art. 6.1 LOPD, y si es necesario informar de la recogida al afectado, *ex* art. 5.4 LOPD. Además, una vez recogidos, los «datos» deberán ser tratados por los titulares de derechos en sucesivas ocasiones a lo largo del proceso previo a la demanda civil, tanto para comunicarlos al juez y al propio prestador de acceso como para que éste busque en sus archivos al infractor. Ello nos llevará a plantearnos si hay alguna habilitación legal para dicho «tratamiento».

Para afrontar esta cuestión, existen básicamente dos opciones. La primera consiste en acudir a la idea de que estamos ante datos que figuran en «fuentes accesibles al público» y su tratamiento es necesario para la satisfacción de un interés legítimo (art. 6.2 *in fine* LOPD). La segunda es entender que hay una autorización expresa o tácita de la Ley para este caso (art. 6.1 LOPD).

A este respecto, la doctrina[57] ha apuntado en primer lugar si este art. 6.2 *in fine* de la LOPD no supone una incorporación indebidamente restrictiva del art. 7 f) de la Directiva 95/46, sobre Protección de Datos Personales, que exceptúa el consentimiento previo del afectado por el tratamiento si es necesario para la satisfacción de un interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, sin añadir el requisito de que los datos se hayan obtenido de una fuente accesible al público.

Se trata de una posibilidad que ha barajado también respecto del art. 10.2 b) del Reglamento la Sentencia del Tribunal Supremo (Sala Tercera) de 15 de julio

[57] Vid. a ese respecto, González Gozalo, A., «El conflicto entre la propiedad intelectual y el derecho a la protección de datos de carácter personal en las redes P2P», cit., p. 51.

de 2010[58], que plantea una cuestión prejudicial al Tribunal de Justicia preguntando si es admisible que en el Derecho nacional de un Estado miembro (en este caso, en el art. 10.2 b) del Reglamento, que replica en esto la regulación legal) se introduzca este requisito adicional de que los datos deban haberse obtenido de una fuente accesible al público.

En cualquier caso, me parece evidente que una red *peer-to-peer* puede ser usada como canal adecuado para comunicar informaciones de cualquier tipo al público, lo que no hace descabellado calificarla como una «fuente accesible al público» o incluso un «medio de comunicación social» (al igual que lo puede ser, por ejemplo, una red social, o una página web, caso de la sentencia de la Audiencia Nacional de 24 de abril de 2007, que apunta en este caso el carácter de la página web como «medio de comunicación»[59]).

La segunda posibilidad que antes apuntamos para eximir de la necesidad del consentimiento del usuario para recopilar y «tratar» direcciones IP, la de la habilitación legal del art. 6.1 LOPD, la vemos claramente en materia de propiedad intelectual en los arts. 138 III, 139.1 h) y 141.6 de la LPI, que permiten solicitar al prestador de acceso la suspensión del servicio a los usuarios infractores, solicitud que no puede llevar a cabo sin realizar un «tratamiento» de las direcciones IP como el que hemos descrito antes. Parece por tanto razonable pensar que el legislador de la Ley 19/2006 ha realizado una habilitación legal (siquiera implícita) que permita a los derechohabientes solicitar las medidas cautelares y definitivas de cesación del servicio a las que se refiere la LPI[60].

Y si eso es así respecto de las medidas cautelares y definitivas de cesación, carecería de sentido a mi juicio que no se pudiera realizar este «tratamiento» sin recabar el consentimiento previo del afectado en el caso del art. 140 LPI, respecto de la acción de indemnización. Dicho tratamiento resulta imprescindible para articular una demanda posterior, de manera que es necesario entender que el titular puede actuar sin contar con el consentimiento previo del (futuro) demandado.

En resumen, incluso si consideramos que una dirección IP es un «dato de carácter personal» a los efectos de la LOPD y de su Reglamento, es posible su recogida y tratamiento, incluso por medios automatizados, bien considerando que estamos en un supuesto previsto en el art. 6.2 *in fine* de la LOPD, bien por la vía del art. 6.1 LOPD entendiendo que existe una habilitación legal en los arts. 138.III, 139.1 h) y 141.6 de la LPI (respecto de la acción de cesación) y 140 LPI (respecto de la acción de indemnización).

---

[58] RJ 2010/6272.
[59] JUR 2007/276044.
[60] González Gozalo, A., «El conflicto entre la propiedad intelectual y el derecho a la protección de datos de carácter personal en las redes P2P», cit., p. 55.

2. *Posición propia: La dirección IP es un dato de tráfico, no un dato de carácter personal*

a) La dirección IP no es un dato de carácter personal según la LOPD española

Pese a que, como hemos visto, tanto a nivel nacional como a nivel comunitario se acepta generalmente la idea de que una dirección IP es un «dato de carácter personal» (o un dato de tráfico equiparable en su protección a un dato de carácter personal), a mi juicio dicha afirmación es muy discutible con el tenor del art. 3. a) de la LOPD en la mano, que define «dato personal» como *cualquier información concerniente a personas físicas, identificadas o identificables*. Dicha norma ha sido después aclarada por el art. 5.1 f) del Reglamento de desarrollo de la LOPD[61] que aclara que la definición de «datos de carácter personal» incluye «*cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*».

La cuestión clave consiste pues en determinar si la dirección IP hace a la persona física «identificable» por medios directos o indirectos. En ese sentido, señala el art. 5.1 o) del Reglamento respecto de lo que es una «persona identificable» que lo será «*toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas*».

Pues bien, a mí me parece claro que una dirección IP es únicamente un medio de identificar *una máquina* en Internet que no permite, ni siquiera de forma indirecta, identificar a una persona física. Ello viene provocado porque existe un grado de disociación muy importante entre los caracteres alfanuméricos que representan la IP y la identidad de una persona. Dicha disociación proviene de dos factores fundamentales.

El primero es de orden subjetivo, y surge porque únicamente los proveedores de acceso a Internet podrían, llegado el caso, determinar por medios razonables la identidad de la persona que contrató el servicio de conexión a Internet a la que se asignó una IP en un momento determinado, dado que son ellos los que las asignan. Para cualquier otra persona, física o jurídica, la averiguación de la identidad de una persona que se ha conectado a Internet a través de una dirección IP sencillamente no resulta posible por motivos técnicos.

En principio, esta limitación subjetiva no resulta relevante en la Directiva 95/46/CE, en la que un dato sigue siendo un «dato de carácter personal» cuando puede ser razonablemente utilizado para identificar a una persona no sólo por

[61] Aprobado por R.D. 1720/2007, de 21 de diciembre (BOE núm. 17, de 19 de enero de 2008).

el responsable del tratamiento, sino también por un tercero (en nuestro caso, un prestador de acceso).

El problema es que, en mi opinión, existe una segunda restricción técnica que provoca que ni siquiera los prestadores de acceso puedan, con un grado de certeza razonable, conocer la identidad de la persona que ha utilizado una dirección IP en un momento determinado sin realizar ulteriores actividades de investigación que pueden ser perfectamente calificables de desproporcionadas. Y ello porque la única información que proporciona una IP es que se ha utilizado una conexión a Internet un día y a una hora concreta. Pero nada garantiza que la persona que utilizó esa IP a ese día y a esa hora sea la misma que contrató el servicio. Así, por ejemplo, una cuenta de acceso a Internet puede ser utilizada fraudulentamente por un tercero y las propias direcciones IP pueden ser «suplantadas» utilizando direcciones IP proxy (método por el que se «hackea» el ordenador para ser utilizado por un tercero para intercambios ilícitos).

Esta desconexión se acentúa en el caso de las direcciones IP dinámicas, que sólo identifican a una máquina concreta mientras dura su conexión a Internet. Una vez que se interrumpe dicha conexión, la IP se asigna a otro ordenador. Y si el usuario vuelve a conectarse a la red, lo hará con una IP «nueva», que se la asigna para esta nueva sesión. Además, lo más habitual es que todos los ordenadores de una misma empresa o entidad «salgan» a Internet con la misma dirección IP, lo que implica que desde una única conexión estén intercambiando información cientos o incluso miles de usuarios de forma simultánea.

Esta doble disociación provoca a mi juicio que sea claramente incorrecto afirmar respecto del público en general que una dirección IP es un medio «razonable» para identificar al usuario en el sentido del art. 3. a) de la LOPD. Y respecto del caso concreto de los prestadores de acceso resulta muy discutible, pues requeriría por parte del prestador de una ulterior actividad investigadora que tiene que ser calificada de *desproporcionada* en los términos del art. 5.1 o) del Reglamento.

Esto no quiere por supuesto decir que sea totalmente imposible identificar a una persona a partir de una dirección IP, ni que no pueda exigírsele responsabilidad penal o civil por las conductas que llevó a cabo en la red mientras utilizaba una dirección IP determinada, bien de forma directa, bien mediante la utilización de presunciones razonables o ulteriores pesquisas (como se argumentará después en este trabajo).

Lo que se quiere decir es que la identificación del usuario por medios razonables a partir de una dirección IP es imposible respecto de cualquiera que no sea un prestador de acceso, y, para dichos prestadores, requiere en casi todas las ocasiones de una ulterior actividad de investigación que en mi opinión es desproporcionada, en el sentido del art. 5.1 o) del Reglamento de la LOPD.

Ello es así claramente en el caso antes señalado de intranets o redes internas de empresas o instituciones, en las que todos los ordenadores «salen» a Internet con la misma IP. Será necesaria una ulterior actividad investigadora para averiguar a qué ordenador concreto se asignó una IP en un momento determinado, dato que sólo conoce el administrador de la intranet. Y lo mismo ocurrirá en locales abiertos al público, como cibercafés.

Pero incluso en el caso más sencillo, el de una IP asignada a un único ordenador (por ejemplo, en un domicilio particular que sólo tiene una máquina conectada a la red), la identificación del usuario puede resultar problemática por el «hackeo» de la IP o la utilización del ordenador por varias personas. Dicha identificación podrá realizarse con ulteriores averiguaciones, o incluso deducirse de presunciones razonables (como que quien contrata el acceso a Internet es en principio quien utiliza el ordenador), pero, a mi juicio, tales pesquisas implican un grado de desconexión tal que hace imposible que consideremos que una dirección IP permite identificar a un usuario de forma razonable y sin investigaciones o plazos desproporcionados.

A este respecto, resulta a mi juicio interesante la postura de la Corte de Casación francesa, que mediante auto de la Sala de lo Penal de 13 de enero de 2009[62] resolvió el recurso planteado por la Sociedad de Autores, Compositores y Editores musicales en Francia (SACEM) contra un auto de la Corte de Apelación de Rennes de 22 de mayo de 2008 que había afirmado que la IP era un dato de carácter personal y que por tanto su utilización para preparar eventuales demandas contra usuarios de redes *peer-to-peer* debía ser considerada como «tratamiento» a efectos de los arts. 2 y 25 de la Ley de 6 de enero de 1978.

La conducta de SACEM había consistido en aportar documentación con «pantallazos» de aplicaciones P2P en la que aparecían una lista de direcciones IP, así como un CD-ROM en el que se almacenaban estas direcciones, conductas ambas que no son consideradas como «tratamiento» en sentido legal por el tribunal casacional francés. Por esto motivo, no se precisa para la recogida la autorización previa de la autoridad administrativa nacional en materia de protección de datos (en Francia, la CNIL).

Dicha postura ha sido mantenida consistentemente también por la Corte de Apelación de París, que mediante un auto de 1 de febrero de 2010 (también en el marco de un proceso penal de infracción de derechos de propiedad intelectual que acabó con la condena del usuario) añadió a la doctrina casacional de que la recogida de direcciones IP por parte de agentes de SACEM en el marco de procesos penales no es un «tratamiento» la afirmación directa de que la IP no es un «dato de carácter personal» según la legislación francesa.

---

[62] El auto está disponible en la dirección <http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-de-cassation-chambre-criminelle-13-janvier-2009-2837.html>.

Para ello recuerda el Tribunal parisino que una IP no permite identificar de forma directa al autor de un delito contra la propiedad intelectual por el sencillo motivo de que puede haber sido manipulada para enmascarar la IP realmente asignada por el prestador de acceso (técnica utilizada por algunas aplicaciones P2P y por muchos usuarios avezados en tecnologías de la información) o simplemente ser utilizado por personas que no han contratado la cuenta de acceso a Internet (como ocurre, por ejemplo, cuando se utiliza una web inalámbrica contratada por un tercero que la dejó por descuido sin contraseña).

De ahí concluye la Corte de Apelación de París que la dirección IP es simplemente un elemento más dentro de la investigación de la conducta delictiva, que, junto con otros, puede servir para determinar al verdadero autor de la infracción (de hecho, en el caso se demostró que quien había realizado los intercambios ilícitos mediante programas P2P no era la misma persona que había contratado el acceso a la Red[63]). Con este auto de 2010 se da continuidad a dos decisiones anteriores de esta misma Corte de Apelación de 27 de abril[64] y 15 de mayo de 2007[65] que habían abierto esta línea antes de la decisión del Tribunal de casación francés antes señalada[66].

Además de esta línea de resoluciones judiciales francesas, que a mi juicio resuelven correctamente el problema, en España debe citarse la conocida sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo) de 17 de septiembre de 2008[67], que resuelve el recurso impuesto contra la sanción de la AEPD a la empresa que gestiona los servicios de venta de tonos de telefonía móvil de *Tele 5*, que había mostrado algunos números de teléfono móvil en sobreimpresionados durante la emisión de determinados programas.

La Audiencia Nacional señala respecto del número de teléfono móvil y su inclusión dentro de la definición del art. 3 a) de la LOPD como «información concerniente a personas físicas identificadas o identificables» que aunque el

---

[63] Pese a estas decisiones judiciales, hay que recordar sin embargo que en Francia la entrada en vigor del sistema de desconexión tras tres avisos a los internautas, previsto por la Ley HADOPI 2, que tenía que entrar en vigor en enero de 2010 se ha visto sin embargo retrasada hasta que la autoridad administrativa francesa en materia de protección de datos, la CNIL, no emita su informe favorable a la recogida y «tratamiento» de direcciones IP que necesariamente tiene que hacer la HADOPI para identificar a los usuarios infractores a los que se quiere desconectar de Internet, como explica RYAN, J, en «Internet access controls: Three Strike's graduated response' initiatives», borrador de trabajo (draft) disponible en <http://cambridge.academia.edu/JohnnyRyan/Papers>.

[64] En este caso, un usuario había intercambiado 1875 ficheros musicales a través del programa Kazaa. La sentencia está disponible en <http://www.legalis.net/spip.php?page=jurisprudence-imprimer&id_article=1955>.

[65] En el caso un usuario había intercambiado un total de 3175 archivos en formato Mp3. La resolución está disponible en <http://www.legalis.net/jurisprudence-decision.php3?id_article=1954#>.

[66] A esto debe sumarse una decisión del Consejo de Estado de 23 de mayo de 2007, que anuló una decisión de la CNIL que prohibía a las entidades de gestión recopilar direcciones IP de usuarios para la preparación de ulteriores demandas contra ellos.

[67] JUR 2008/307282.

número de teléfono considerado de forma aislada puede ser considerado como un dato de carácter personal en nuestra Ley «*el citado número de teléfono ayuno de otras circunstancias que identifiquen o pudiesen permitir identificar al titular del mismo impide que pueda encajarse en la definición legal de dato de carácter personal*».

La idea es por tanto que, para el público en general, un número de teléfono móvil, desconectado de otros elementos, no permite identificar a su titular. Y si esto es así respecto de un número de teléfono, mucho más lo debe ser respecto de una dirección IP, en la que la conexión con el usuario es mucho más remota que la que existe en el caso de un aparato como el teléfono móvil.

En resumen, es razonable concluir (y así se hace en el presente trabajo), que una dirección IP no es un dato de carácter personal en el sentido del art. 3 a) de la LOPD porque, por sí mismo, no es suficiente para identificar por medios razonables a una persona física, ni siquiera en el caso del sujeto mejor ubicado para ello, el prestador de acceso.

De ahí se deprende la consecuencia lógica de que la actividad de recogida de direcciones IP que necesariamente hay que realizar para demandar a los usuarios de redes P2P y su ulterior «tratamiento» queda exenta de la normativa europea y nacional sobre protección de datos personales, que no resulta aplicable al caso.

b) El régimen jurídico de la dirección IP como «dato de tráfico»

Esta postura que entiende que una dirección IP no entra dentro de la categoría de «dato de carácter personal» del art. 3 a) de la LOPD no significa naturalmente conceder patente de corso para que se pueda recopilar o almacenar de forma indiscriminada las direcciones IP de los usuarios en Internet sin su consentimiento por parte de terceros.

Por el contrario, es evidente que nuestra legislación debe impedir que las direcciones IP sean utilizadas por terceros, pero para ello no es necesario afirmar sin más que la IP es un «dato de carácter personal», sino ser rigurosos en su consideración de «dato de tráfico» tal y como ha sido establecido por la LCDCE, dato de tráfico que no puede ser cedido a terceros ni usado por los prestadores de servicios de la sociedad de la información más que en los casos y para los fines que las leyes prevean.

En ese sentido, creo que es indudable que la postura del Grupo de Trabajo del art. 29 y de la AEPD que entiende que hay que elevar las direcciones IP a la categoría de «dato de carácter personal» está pensada fundamentalmente para garantizar que los prestadores de acceso no cedieran sus datos de conexión a

terceros y para evitar que los titulares de páginas web «recolecten» las IP de los usuarios que las visitan sin su consentimiento para crear perfiles comerciales. Pero este objetivo, que a principios de este siglo se lograba fundamentalmente gracias a las normas sobre protección de datos personales, puede lograrse perfectamente hoy en día manteniendo a la dirección IP como un mero «dato de tráfico» de acuerdo con la legislación europea y la Ley de 2007, sin que exista necesidad alguna de elevar la dirección IP a la categoría de «dato de carácter personal».

De hecho, lo más correcto a mi juicio es afirmar que la IP, en cuanto que dato de tráfico, tiene que recibir la protección del derecho a la intimidad, pero en un escalón inferior en cuanto a la intensidad de la protección del derecho respecto de los datos de carácter personal. Esta ubicación en la periferia del derecho a la intimidad permite, aplicando el principio de proporcionalidad, que se conjugue la regla general de protección de los datos de tráfico con la posibilidad de recopilar direcciones IP cuando existe un interés legítimo relevante que lo justifique en un caso concreto.

En mi opinión, cuando dichos datos de tráfico (en este caso las direcciones IP) están disponibles en fuentes accesibles al público (como es una red P2P) la recogida y «tratamiento» debería poder llevarse a cabo incluso sin una autorización judicial previa cuando se trata de un interés legítimo contemplado en la Ley. Y ello porque, como señalan las sentencias francesas e irlandesas antes citadas, se puede pensar que el usuario de una red P2P ha consentido tácitamente que su dirección IP esté a disposición de los demás usuarios de la red cuando las utiliza.

También puede argumentarse con naturalidad que el art. 140 LPI contiene una autorización legal implícita para la recogida y tratamiento de determinados datos de tráfico y, en especial, para las direcciones IP, para lo que habrá que hacer una interpretación correcta de la LCDCE, como luego señalaré.

Sin embargo, no puede ignorarse la postura de la Sala de lo Penal de nuestro Tribunal Supremo, que aunque ha afirmado explícitamente que los datos de tráfico no tienen exactamente la misma protección que los datos personales, también ha aceptado la tesis de que la protección de la intimidad de los usuarios de los arts. 18.1 y 18.4 CE requiere de la intervención judicial para pedir a los prestadores de acceso la cesión de diferentes datos de tráfico mencionados en el art. 3 de la Ley 25/2007, entre los que se encuentra la dirección IP.

En efecto, en algunas sentencias de la Sala Segunda del Tribunal Supremo se había considerado conforme con los arts. 18.1 y 18.4 de la CE la recogida por parte de la Policía judicial de direcciones IP utilizadas por los usuarios en redes P2P en casos de difusión de pornografía infantil. Dicha línea jurisprudencial

arranca con la sentencia de 9 de mayo de 2008[68], que fue seguida después por otras de 28 de mayo de 2008[69] y 12 de noviembre de 2008[70].

Posteriormente, sin embargo, se produjo un acuerdo del Pleno no jurisdiccional de la Sala de lo Penal de 23 de febrero de 2010 que determinó que es necesaria la autorización judicial para que los prestadores de acceso cedan los datos de tráfico del art. 3 de la LOPD, por lo que el Ministerio Fiscal debe pedir dicha autorización para obtener de los operadores los datos durante el curso de sus investigaciones.

De este modo, aunque incluso con posterioridad a dicho acuerdo la propia Sala Segunda ha venido admitiendo la recopilación de direcciones IP por parte del Ministerio Fiscal o de la policía sin autorización judicial si los hechos acontecieron antes de la reunión plenaria (Vid. en este sentido las SSTS de 10 de marzo de 2010[71], 14 de julio de 2010[72] y 7 de octubre de 2010[73]), se ha aclarado expresamente en la STS de 10 de marzo de 2010 que cuando los hechos presuntamente delictivos se hayan producido después de la entrada en vigor de la Ley 25/2007 debe requerirse autorización judicial para recopilar direcciones IP.

Este acuerdo de la Sala Segunda en mi opinión es claramente desacertado. Así, no parece lógico que la LOPD permita recoger y tratar datos personales en determinados supuestos sin autorización judicial (art. 6) y, sin embargo, sea necesaria la autorización judicial en el caso de las direcciones IP, que son datos de tráfico que tienen que tener un grado de protección inferior. Con todo, parece que la posición de la Sala Segunda en esta cuestión va a ser decisiva en la práctica si no media una ulterior actividad del legislador, por lo que, de *lege data*, creo que resulta necesario recabar una autorización judicial previa para recopilar y «tratar» direcciones IP (u otros datos de tráfico) en los casos en los que se estén preparando demandas civiles por violación de derechos de propiedad intelectual, autorización que, de acuerdo con la interpretación más correcta de la Ley de Conservación de Datos que se realiza en el apartado si-

---

[68] RJ 2008/4648. En el caso, el Grupo de Delitos Telemáticos de la Policía Judicial de la Guardia Civil había recopilado, sin autorización judicial, una serie de direcciones IP que habían sido utilizadas para ofrecer en redes P2P archivos que contenían pornografía infantil. Al ser cuestionado el TS sobre la legalidad de tal recopilación, el Alto Tribunal dice literalmente que «*No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma*. *La huella de* entrada [continúa el Alto Tribunal] (...) *queda registrada siempre, y eso el usuario lo sabe*». Es más continúa el Tribunal Supremo añadiendo que «*(....) quien utiliza un programa P2P, en nuestro caso Emule, asume que muchos de los datos se convierten en públicos para los usuarios de Internet, circunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía, datos públicos de internet, no se hallaban protegidos por el art. 18.1 ni por el 18.3 CE*».

[69] RJ 2008/3241.

[70] RJ 2009/167.

[71] RJ 2010/2425.

[72] RJ 2010/3506.

[73] RJ 2010/7684.

guiente de este trabajo (al que ahora me remito) puede lograrse a través de la diligencia preliminar prevista en el art. 256 1.7º de la LEC.

Dicha diligencia preliminar podrá usarse por tanto no sólo para solicitar que se revele la identidad de los usuarios, sino también para autorizar la recogida y tratamiento por parte de particulares de direcciones IP en la preparación de procesos civiles si se respetan determinadas condiciones que luego se explicarán (básicamente, que se aplique rigurosamente el principio de proporcionalidad, que haya *prima facie* un acto de infracción de derechos y que no exista otro medio menos lesivo para el derecho a la intimidad de obtener información suficiente sobre la conducta presuntamente infractora).

V. LA REVELACIÓN DE LA IDENTIDAD DEL USUARIO EN PROCESOS CIVILES

Una vez que los derechohabientes han recopilado y organizado una lista de direcciones IP (actividad para la que según la Sala 2ª del TS se necesita autorización judicial previa), es evidente que para descubrir el nombre y dirección postal de la persona que hay detrás de cada una de estas direcciones IP se deben solicitar estos datos a los prestadores de acceso[74], que son los únicos que conocen a qué cuenta de acceso a la Red corresponden las direcciones IP «infractoras».

Sin embargo, dichos prestadores se han negado sistemáticamente a suministrar dicha información a los derechohabientes por temor a estar realizando una cesión no autorizada de datos de tráfico o una cesión de datos de carácter personal. Tampoco quieren, seguramente, ser los primeros en desvelar la identidad de sus usuarios a los derechohabientes, lo que probablemente provocaría una migración de internautas hacia otros prestadores menos dispuestos a colaborar con los titulares de derechos de propiedad intelectual.

A este respecto, es evidente que los prestadores de acceso no tienen la obligación de suministrar el nombre y dirección de sus clientes directamente a los titulares de derechos cuando son requeridos por vía extrajudicial. Además de no haber norma alguna en la LCDCE o en la LSSI que les obligue a ello, el nombre y dirección de los usuarios son sin duda «datos de carácter personal», por lo que el art. 11.1 LOPD prohíbe expresamente su cesión fuera de los casos particulares del art. 11.2 (casos particulares que no resultan de aplicación en un supuesto como el que nos planteamos[75]).

---

[74] Cada dirección IP es asignada por un prestador de acceso, de manera que habrá que agrupar las peticiones en función de los distintos prestadores que aparezcan vinculados a las listas de direcciones IP obtenidas por los derechohabientes.

[75] González Gozalo, A., «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», p. 119.

Será necesaria en todo caso la autorización del juez, autorización que en el campo penal se acepta generalmente incluso por los propios prestadores de acceso que corresponde al juez instructor de la causa (SSTS —Sala Segunda— de 9 de mayo de 2008[76], 28 de mayo de 2008[77] y la de 12 de noviembre de 2008[78]).

Sin embargo, se discute abiertamente en nuestro Derecho si también el juez civil puede ordenar al prestador de acceso que comunique a los derechohabientes el nombre y apellidos del titular del contrato de acceso a Internet al que se le asignó una IP que ha sido utilizada para intercambiar archivos protegidos por la Propiedad Intelectual.

Respecto de esta cuestión, a mi juicio la interpretación correcta del art. 256.1.7º LEC y de la Ley de Conservación de Datos es que los Juzgados de lo Mercantil sí tienen esta potestad, puesto que nuestro Ordenamiento jurídico en ningún caso establece una prevalencia absoluta del derecho a la protección de datos de carácter personal frente al derecho de propiedad intelectual de los derechohabientes.

No es ésta sin embargo la interpretación dominante en España[79], en donde la LCDCE estableció la obligación de revelar ciertos datos de tráfico protegidos (entre los que se encuentra el nombre del usuario) únicamente para el caso de la comisión de delitos graves.

Y esta regla ha sido interpretada «a contrario», de manera que tanto la Agencia Española de Protección de Datos como nuestros jueces y Tribunales han mantenido de forma consistente que este deber de cesión de datos no existe cuando se está en el marco de un pleito civil (por ejemplo, en el marco de una acción indemnizatoria contra un usuario de una red P2P).

Esta situación resulta además conforme con el Derecho comunitario para el Tribunal de Justicia, que en su sentencia sobre en el *Asunto Promusicae*[80] declaró que la legislación de la UE no obliga a los Estados miembros a establecer en su legislación nacional este deber de cesión de los datos de los usuarios infractores de propiedad intelectual en el marco de procedimientos civiles.

---

[76] RJ 2008/4648.
[77] RJ 2008/3241.
[78] RJ 2009/167.
[79] Vid. por ejemplo Durán Rivacoba, R.,/García Llerena, V., «Protección de datos personales y del derecho a la intimidad vs. protección de la propiedad privada de carácter intelectual: consecuencias del caso PROMUSICAE», en *Los derechos de propiedad intelectual en la obra audiovisual*, (O'Callaghan, X., Coordinador), Dykinson, Madrid, 2011, p. 228.
[80] Sentencia del TJ de 29 de enero de 2008, asunto C275/06. La sentencia trae causa de una cuestión prejudicial planteada por el Juzgado de lo Mercantil núm. 5 de Madrid durante un procedimiento de diligencias preliminares (anterior a la entrada en vigor del art. 256.1 7º LEC) iniciado por la asociación representativa de los productores discográficos contra un prestador de acceso (*Telefónica*) para que desvelara los datos de ciertos usuarios que habían utilizado el programa *KaZaA* para el intercambio ilícito de fonogramas.

Sin embargo, en este trabajo se defiende que hay elementos suficientes en nuestro Ordenamiento Jurídico para entender con la normativa vigente en la mano que los prestadores de acceso están obligados a revelar el nombre y dirección postal de los usuarios de sus servicios a un juez civil cuando éste se lo requiere en el marco de unas diligencias preliminares de las previstas en el art. 257.1 7º LEC.

No es obstáculo para ello a mi juicio la regulación de la Ley de Conservación de Datos, siempre que se interprete correctamente desde el punto del Derecho comunitario y de la propia Constitución española. En este sentido, la reciente reforma del art. 8 de la LSSI por la Disposición Adicional 43 de la Ley de Economía Sostenible es un paso modesto, aunque adecuado, en la dirección correcta, como se tratará de explicar a continuación.

1. El origen del problema: el art. 12 de la LSSI

El problema en torno a esta cuestión arranca cuando el ahora derogado art. 12.3 de la LSSI únicamente mencionaba de forma expresa la obligación de que los prestadores de acceso cedieran los datos de tráfico de los usuarios a las autoridades competentes «*en el marco de una investigación criminal o para la salvaguarda de la seguridad pública y la defensa nacional*». El deber de colaboración e información del prestador de acceso se predicaba por tanto literalmente sólo en el marco de un proceso penal o por motivos de seguridad pública y defensa nacional (por ejemplo, dentro de las funciones de los Cuerpos y Fuerzas de Seguridad del Estado o del CNI).

Sin embargo, ya entonces era posible interpretar la LSSI en el sentido de que también debían incluirse dentro de este deber de colaboración con las autoridades los ilícitos civiles (como las violaciones de derechos de propiedad intelectual), pues de otro modo se estaría dando carta blanca a numerosas actividades ilícitas sin que hubiera una vía legalmente habilitada para identificar a los infractores[81]. Así lo exigía el art. 24 CE, que proscribe la existencia de un espacio de inmunidad para quienes violen derechos de terceros[82].

Además de esta ausencia de mención expresa de los ilícitos civiles en su art. 12.3, el problema desde el punto de vista procesal estribaba en que la LSSI no contenía ningún procedimiento específico para que los titulares acudieran al juez civil para que requiriera al prestador de acceso los nombres y direcciones

[81] Vid. más ampliamente Garrote Fernández-Díez, I., «Acciones civiles contra los prestadores de servicios de intermediación en relación con la actividad de las plataformas P2P», *pe. i. (Revista de Propiedad Intelectual),* núm. 16, pp. 55-104.

[82] En ese sentido, González de Alaiza, J.J., «La lucha de los titulares contra las redes «peer-to-peer»», cit., p. 64, señalando que nada impide que el Juez solicite los datos para otros fines dignos de protección.

de quienes usaban redes *peer-to-peer* para intercambiar obras y prestaciones protegidas por la propiedad intelectual. El hecho de que la lista de diligencias preliminares del art. 256 LEC fuera *numerus clausus* obstaculizaba además sus pretensiones.

2. La diligencia preliminar del art. 256.1.7º de la LEC

1. *La interpretación de la mención a la escala comercial de la infracción*

Cuatro años después de la aprobación de la LSSI, la Ley 19/2006 introdujo en nuestra legislación el art. 256.1.7º de la LEC, estableciendo una nueva diligencia preliminar específica para las violaciones de derechos exclusivos de propiedad industrial e intelectual cuya *ratio* es obtener información sobre el origen de la infracción, y, en especial, cuál es la identidad del infractor o infractores.

Esta norma parece en principio un camino sencillo para que los derechohabientes soliciten a los Jueces de lo Mercantil que ordenen a los prestadores de acceso la revelación de la identidad de los usuarios que utilizan sus servicios para cometer violaciones de derechos de propiedad industrial e intelectual.

El problema estriba en que este art. 256.1.7º LEC exige que la infracción sea «cometida mediante actos desarrollados a escala comercial[83]», lo que ha provocado que en la práctica las Audiencias Provinciales denieguen las peticiones de diligencias preliminares amparadas en esta norma para solicitar la identificación de usuarios de redes P2P que han infringido derechos de propiedad intelectual.

La primera de dichas denegaciones se contiene en el auto 199/2009, de la AP de Barcelona (Sección 15ª), de 10 de diciembre de 2009, que confirma una decisión del Juzgado Mercantil número 4 de Barcelona de 20 de abril de 2009 que no concedió dicha petición de datos[84]. La doctrina sentada en dicho auto fue confirmada después por otro de esta misma Sección 15ª de la AP de Barcelona de 15 de diciembre de 2009[85].

---

[83] A estos efectos señala en el art. 256.1.8º LEC que «se entiende por actos desarrollados a escala comercial aquellos que son realizados para obtener beneficios económicos o comerciales directos o indirectos».

[84] El supuesto se refería al intercambio de películas en redes P2P, en donde una productora alemana (*Hustler GmbH*) solicita a dos prestadores de acceso (*Telefónica* y *ONO*) que identifiquen a los usuarios de una lista de direcciones IP concretas.

[85] JUR 2010/117178. Señala en este auto la AP de Barcelona que «*De este modo, se aprecia que en nuestro derecho no existe ningún deber legal de colaboración impuesto a las entidades suministradoras de acceso a Internet para suministrar la información interesada por la actora, para justificar una reclamación civil. Y la ausencia de este deber no contraría la normativa comunitaria, que restringe dicho deber de colaboración únicamente en relación con la persecución de delitos, sin perjuicio de la valoración que el legislador nacional pudiera realizar a la hora de introducir este deber de colaboración para proteger los derechos de propiedad intelectual en caso de infracciones civiles, a la vista de los*

La Sección 15ª de la AP de Barcelona hace así una lectura literal de la norma que exige que *el propio infractor* lleve a cabo actos de violación de derechos exclusivos a escala comercial. De hecho, el convencimiento de la Audiencia es tal que en ambos casos acepta que el Juzgado de lo Mercantil deniegue la concesión de la diligencia preliminar de oficio, sin que fuera necesaria la oposición de los prestadores de acceso.

Sin embargo, esta lectura de la LEC no parece que sea conforme con el art. 8.1 c) de la Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual (en adelante, Directiva Antipiratería), que es la norma que se implementa en el Derecho español mediante este art. 256.1.7º LEC.

En dicho art. 8.1 c) se ordena a los Estados miembros que garanticen 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, que las autoridades judiciales competentes puedan ordenar que se le faciliten datos sobre el origen y las redes de distribución de las mercancías o servicios que infringen un derecho de propiedad intelectual a «*cualquier persona que haya sido hallada prestando a escala comercial servicios utilizados en las actividades infractoras*».

Durante el trámite legislativo de la norma se planteó la cuestión de si la misma podía ser utilizada para detener los actos de piratería cometidos en redes P2P. Y este debate claramente tuvo reflejo en el último inciso del Considerado 14 de la Directiva, que define los actos a escala comercial como los «*los realizados para obtener beneficios económicos o comerciales directos o indirectos; esto excluye normalmente los actos realizados por los consumidores finales de buena fe*».

Es claro por tanto que la intención de la Directiva es limitar el alcance del derecho de información respecto de los usuarios finales (que la Directiva llama «consumidores finales»), pero también es claro que la norma señala que eso ocurre sólo *normalmente* (no en todos los casos) y para consumidores finales de *buena fe* (y es muy dudoso que los usuarios de redes P2P sean en todo caso consumidores de buena fe). El hecho de que el infractor de la propiedad intelectual o industrial sea un consumidor final (por ejemplo, una persona física usuaria de Internet) nos indicará *en la mayoría* de los casos una ausencia de carácter comercial en la conducta. Pero no en todos ellos.

Así, es perfectamente posible que una conducta llevada a cabo por un usuario de una red P2P pueda tener «escala comercial» si es llevada a cabo por un

---

derechos afectados. Pero esta ponderación no le corresponde hacerla al juzgador, sino al legislador, quien si lo estima oportuno impondrá expresamente este deber de colaboración y con ello habrá pie para acordar las diligencias preliminares.»

usuario de mala fe que busca obtener un lucro con ello. Así, pensemos por ejemplo en los usuarios «profesionales», que ofrecen archivos a otros con la finalidad de captar su atención respecto de un determinado sitio web (por ejemplo, añadiendo en el nombre del archivo la dirección de la página). Estos usuarios tienen claramente ánimo de lucro indirecto y son de mala fe. Su conducta suele implicar además la puesta a disposición de un número enorme de archivos (frecuentemente, miles), por lo que difícilmente podrá argumentarse que no estamos ante una conducta llevada a cabo «a escala comercial». Así ha sido declarado además en algunas sentencias de Tribunales de Apelación alemanes[86] respecto de la regulación del parágrafo 101 de la *UrhG*, que contiene una obligación de revelar la identidad del usuario infractor de propiedad intelectual cuando la infracción se comete a escala comercial.

Además el art. 8.1 c) de la Directiva Antipiratería habilita expresamente a los jueces civiles (art. 16 en relación con el Considerando 28) para pedir la información a cualquier persona que preste a escala comercial servicios utilizados en las actividades infractoras. Y los prestadores de acceso a Internet son sin duda *personas que prestan a escala comercial servicios utilizados en las actividades infractoras*.

El hecho de que no sean los prestadores de acceso los que realicen la actividad infractora por sí mismos no resulta relevante según el tenor literal de la norma. En efecto, como ha señalado en nuestra doctrina González Gozalo[87], es *el servicio a través del cual se comete la infracción* (servicio de acceso a Internet) lo que tiene que llevarse a cabo a escala comercial *y no la propia infracción*. Y por eso mismo el legitimado pasivo en la diligencia preliminar es el intermediario que ayuda al infractor, no el propio infractor (usuario de la red P2P).

Así, pensemos por ejemplo que se contrata un servicio de transporte por carretera para distribuir mercancías pirateadas, ignorando el transportista prestador del servicio el carácter ilícito de la mercancía. En este caso, es claro que podría requerirse a dicho transportista para que revele quién contrató el transporte, cuál era el destino de la mercancía, la cantidad transportada, etc., puesto que está prestando con finalidad comercial un servicio que ha sido usado por un tercero para infringir derechos de propiedad intelectual. Pues bien, de igual

---

[86] Vid. por ejemplo la sentencia del *OLG Karlsruhe* de 1 de septiembre de 2009, aunque hay otros tribunales que en supuestos de intercambios en redes P2P han interpretado que la infracción no se ha cometido a escala comercial (vid., por ejemplo, al sentencia del *OLG de Oldenburg* de 1 de diciembre de 2008). Puede encontrarse un resumen de estos casos en el Informe de Comisión de septiembre 2009 titulado «Study on Online Copyright Enforcement and Data Protection in Selected Member States», disponible en Internet en <http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf>.

[87] González Gozalo, A., «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», cit., p. 132.

modo puede requerirse a quien presta un servicio de acceso a Internet con carácter comercial que desvele la identidad de quienes utilizan ese servicio fraudulentamente para intercambiar archivos en redes P2P.

Y si ésta es la lectura correcta de la Directiva Antipiratería, la interpretación literal del art. 256.1.7º LEC que han hecho los autos de la Sección 15ª de la AP Barcelona antes comentados implicaría que el legislador español ha incumplido dicha Directiva, que es una norma de mínimos que los Estados miembros deben implementar sin incluir restricciones adicionales (art. 2 de la Directiva).

Sólo una interpretación del art. 256.1.7º LEC conforme con la Directiva que entendiera que si el servicio de conexión a Internet se presta a escala comercial es indiferente que la conducta del usuario (es decir, la infracción) se haga a escala comercial, podría evitar este incumplimiento[88]. Y con esta interpretación se podría solicitar ante el Juez de lo Mercantil que se desvele el nombre y dirección de los usuarios de redes P2P si se cumplen el resto de requisitos que deben tener las diligencias preliminares (en especial, la proporcionalidad[89]).

2. *El respeto de la regulación comunitaria de la protección de datos en las comunicaciones electrónicas*

La interpretación de la diligencia preliminar del art. 256.1.7º que acabamos de señalar es además perfectamente compatible con la normativa comunitaria en materia de protección de datos en las comunicaciones electrónicas.

En efecto, en la sentencia del Tribunal de Justicia sobre el *Asunto Promusicae* se afirma expresamente que de la lectura conjunta de los arts. 8.1 y 8.3 a) de la Directiva Antipiratería[90] se desprende que no existe una obligación para los Estados miembros de establecer en su legislación nacional un deber de comunicar datos personales en el marco de un procedimiento civil con el objeto de garantizar una protección efectiva de los derechos de autor[91]. Pero el propio Tribunal de Justicia también afirma en su sentencia que el Derecho comunitario no impide que los Estados miembros decidan imponer dicho deber en la legislación nacional.

---

[88] Hay que señalar que no estamos ante una interpretación extensiva de la norma, sino acorde con su tenor literal a la luz del Derecho comunitario aplicable.

[89] Lo señala así González Gozalo, A., «La propiedad intelectual y la protección de datos de carácter personal en las redes P2P», cit., p. 48.

[90] Dicha norma señala que la regulación de la Directiva se aplica «*sin perjuicio de otras disposiciones legales que rijan* (...) *el tratamiento de los datos personales*».

[91] Así lo señala también, Kuner, C., «Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of Justice», *E.I.P.R.,* 2008, num. 5, p. 200.

Por tanto, es obvio que si dicho deber *ya existe* según el Derecho nacional en un Estado miembro concreto (aunque sea de forma implícita[92], como ocurre en España a través de la interpretación del art. 256.1.7º de la LEC que hemos visto) la existencia de dicho deber es perfectamente compatible con las reglas de protección de datos en las comunicaciones electrónicas[93].

Lo dicho se confirma si tenemos en cuenta que el análisis que hizo el Tribunal de Justicia en el asunto *Promusicae* no tuvo cuenta la nueva regulación de la Directiva de Conservación de Datos, que no era aplicable al caso por haberse publicado en 2006, después de acontecidos los hechos que dieron lugar a la cuestión prejudicial[94]. Dicha Directiva ha regulado específicamente la cuestión de la protección de los datos de tráfico, desplazando en éste ámbito a la Directiva de Intimidad en las Comunicaciones Electrónicas[95].

Este hecho ha provocado que el mismo magistrado que fue ponente de la sentencia de *Promusicae* manifestara cuando pudo tener en cuenta la regulación de la Directiva de Conservación (en el *Asunto Tele 2*, auto de 19 de febrero de 2009[96]), que el art. 15.1 de la Directiva sobre la Intimidad en las Comunicaciones Electrónicas no impide que los Estados miembros establezcan en su legislación interna esta obligación de cesión de datos para permitir ejercer acciones civiles contra las infracciones al Derecho de propiedad intelectual.

Respalda esta interpretación el hecho de que el propio Tribunal de Justicia haya señalado expresamente que «*corresponde a las autoridades a los órganos*

---

[92] No obstante, habrá que esperar a la decisión que tome el propio Tribunal de Justicia en el caso de *Scarlet Extended Sa vs. Societé Belge des auteurs, compositeurs ed editeurs* (Caso C-70/10), en donde en las conclusiones del Abogado General Cruz Villalón a una cuestión prejudicial presentada ante el Tribunal se señala que cualquier medida que afecte a la protección de los datos personales debe estar prevista en la legislación nacional de forma expresa, previa, clara y precisa (lo que inclina a Cruz Villalón a sostener que un Tribunal de un estado miembro no puede imponer una obligación de filtrado de contenidos en la Red, por faltar el requisito de la previsibilidad). La Opinión está disponible en la dirección <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-70/10>.

[93] Así lo han entendido además en países como Holanda, en donde se considera conforme con la doctrina del asunto *Promusicae* la resolución de su Tribunal Supremo que permite a los titulares solicitar al juez civil que ordene al prestador de acceso que se revele el nombre y dirección del operador de un sitio web que colabora en la infracción de derechos de propiedad intelectual.

[94] Dicha Directiva añadió un nuevo apartado 1 bis al art. 15.1 de la DPDCE para aclarar que lo dispuesto en el art. 15.1 (que es lo que examinó el Tribunal de Justicia en el *Asunto Promusicae*) no será de aplicación a los datos que deban conservarse de acuerdo con la Directiva de Conservación de Datos en relación con los fines del art. 1.1 (la investigación de delitos graves).

[95] En todo caso, el art. 6 de la Directiva de Intimidad, a menudo citado por los prestadores de acceso para negarse a revelar la identidad de los usuarios de sus servicios, se aplica únicamente a los datos de tráfico, como su rúbrica y su propio tenor literal señalan, no a los datos personales, como señala González Gozalo, A., «La propiedad intelectual y la protección de datos de carácter personal en las redes P2P», cit., p. 36.

[96] El caso es *LSG-Gesellschaft zur Wharnehmung von Leistungsschuztrechten GmbH* contra *Tele 2 Telecommunication GmbH* (2009TJCE/103).

jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con dichas Directivas [se refiere a la Directiva Antipiratería, a la Directiva sobre Comercio Electrónico, y a la DDASI], *sino también no basarse en una interpretación de las mismas que entre en conflicto con los derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad*».

Y resulta obvio, que, como el propio Tribunal señala (parágrafo 62 de la sentencia *Promusicae*), los derechos de propiedad intelectual forman parte del derecho fundamental a la propiedad, y que tanto éste derecho de propiedad como el derecho a una tutela judicial efectiva constituyen principios esenciales del Ordenamiento jurídico comunitario[97].

La intención del Tribunal, aunque sea entre líneas, parece evidente[98]: es el intérprete del Derecho comunitario (que de forma primaria es el juez nacional) el que debe equilibrar la protección de derechos fundamentales a la luz del principio de proporcionalidad incluso cuando exista un Estado miembro concreto que no haya previsto esta cuestión *expresamente* en su legislación civil (como ocurre en España).

De ahí que en mi opinión, la sentencia del *Asunto Promusicae* exija que los jueces y tribunales españoles interpreten la regla del art. 256.1.7º LEC de forma que no se elimine en la práctica los derechos fundamentales a la tutela judicial efectiva y a la propiedad privada de carácter intelectual. Y la única manera de evitar dicha eliminación es entender que existe un deber de revelar la identidad de los usuarios en redes P2P al juez civil en un proceso de diligencias preliminares si el juez, en el uso de su discrecionalidad, decide en el caso concreto que la petición de los derechohabientes es pertinente y está suficientemente justificada.

En resumen, creo que la interpretación más correcta del art. 257.1.7º LEC a la luz de la Directiva Antipiratería debe ser que, puesto que el servicio de acceso a Internet se presta por las empresas de acceso a la red de forma comercial, es posible instar mediante una diligencia preliminar que el juez de lo Mercantil ordene a las empresas que prestan servicios de acceso a Internet que revelen el nombre y dirección de las personas que han utilizado su conexión a la Red para intercambiar obras y prestaciones protegidas en redes *peer-to-peer*. Y no obstaculiza dicha conclusión ni la normativa europea en materia de protección

---

[97] Lo que sorprende de la sentencia del *Asunto Promusicae* es que el máximo garante del Derecho comunitario encomiende la labor de vigilancia y cumplimiento de dos derechos fundamentales en el ordenamiento comunitario (que son, además, principios básicos de dicho ordenamiento) a los órganos administrativos y judiciales nacionales, en lugar de garantizar él mismo el respeto de los mismos.

[98] Así lo apunta también Almagro Nosete, J., «Aspectos procesales del intercambio de ficheros en redes P2P», en *Los derechos de propiedad intelectual en la obra audiovisual*, cit., p. 295.

de datos personales en las comunicaciones electrónicas ni la interpretación que ha hecho el Tribunal de Justicia de la Directiva Antipiratería a la luz de dicha normativa.

3. *La aplicación del art. 256.1.7º LEC para identificar al usuario que utilizó una determinada dirección IP para el intercambio ilícito de archivos*

Naturalmente, afirmar que una de las diligencias preliminares previstas en la LEC puede ser utilizada como canal válido para obligar a los prestadores de acceso a proporcionar información sobre los usuarios de sus servicios que intercambian archivos en redes P2P no significa que se puedan articular peticiones de información indiscriminadas por esta vía.

Bien al contrario, estamos ante una situación en la que hay que ponderar distintos derechos implicados, y, como en toda diligencia preliminar, deberán verificarse que se cumplen los requisitos generales de los arts. 256.2 y 258.1 LEC (interés legítimo, justa causa, proporcionalidad o adecuación entre la medida y la finalidad perseguida). Será el juez civil por tanto el que tenga que hacer una ponderación caso a caso, valorando en especial si es imprescindible desvelar dicha identidad para la protección del interés legítimo perseguido (la tutela de la propiedad intelectual)[99].

Para valorar la existencia de indicios suficientes que justifiquen la pertinencia de la diligencia preliminar el Juez de lo Mercantil seguramente podrá tener en cuenta el número de archivos que han sido intercambiados y la correlación entre dichos archivos y las obras o prestaciones protegidas respecto de los cuales se reclama la protección. A mayor número de archivos intercambiados y mayor número de archivos que aparentemente contienen obras y prestaciones protegidas, mayor posibilidad de que se estime pertinente la práctica de la diligencia preliminar.

También deberá tener en cuenta que la revelación de los datos personales es una medida idónea de cara a la tutela judicial efectiva de la propiedad intelectual y además resulta necesaria para ella (sin dicha revelación, dicha tutela judicial efectiva resulta imposible[100], porque no hay ningún medio alternativo para descubrir la identidad del usuario infractor).

---

[99] Así lo sugiere González Gozalo, A., «La propiedad intelectual y la protección de datos de carácter personal en las redes P2P», cit., p. 34.

[100] No están de acuerdo sin embargo Durán Rivacoba, R.,/García Llerena, V., «Protección de datos personales y del derecho a la intimidad vs. protección de la propiedad privada de carácter intelectual: consecuencias del caso PROMUSICAE», en *Los derechos de propiedad intelectual en la obra audiovisual*, cit., pp. 229 y ss. Para estos autores, la revelación de la identidad de los usuarios no resulta una medida necesaria porque los derechohabientes tienen otros mecanismos para compensar las pérdidas que sufren en las redes P2P, como la utilización de medidas tecnológicas de protec-

Una vez que el juez ha valorado positivamente la pertinencia de la diligencia preliminar analizando las circunstancias del caso, parece posible que se utilice la vía prevista en el art. 261.1.6º LEC, ordenando ante la negativa del prestador de acceso requerido que se acuerden las medidas de intervención necesarias, incluida la de entrada o registro en sus sedes para encontrar los documentos o datos precisos.

Naturalmente, la información obtenida mediante esta diligencia preliminar sólo podrá ser utilizada para las finalidades mencionadas en el art. 259.4 LEC (también modificado por la Ley 19/2006), de modo que se utilice «exclusivamente para la tutela jurisdiccional de los derechos de propiedad industrial o intelectual del solicitante de las medidas, con prohibición de divulgarla o comunicarla a terceros».

Además, a instancia de cualquier interesado, el Juez podrá atribuir carácter reservado a las actuaciones, «*para garantizar la protección de los datos* [en nuestro caso, el nombre y dirección de los usuarios de las redes P2P] *e información que tuvieran carácter confidencial*».

Una vez que se ha suministrado a los derechohabientes el nombre y dirección postal de los usuarios asociados a una determinada lista de direcciones IP «infractoras», los titulares de derechos deben resolver aún el problema de que, como hemos afirmado ya, una dirección IP sólo identifica a quien contrató una cuenta de acceso a Internet, no a la persona concreta que llevó a cabo la actividad ilícita (en nuestro caso, la violación de los derechos de propiedad intelectual)[101].

En especial, podrán plantearse dudas sobre la identidad concreta del infractor en dos supuestos distintos. El primero se presenta cuando hay distintos terminales (ordenadores) en una red de área local (LAN) o intranet. En este caso, el camino de salida a Internet es único (hay un único *router*), por lo que todos los ordenadores utilizan la misma IP para conectarse a Internet (que es llamada por ello IP pública). Sólo el administrador de la red de área local conoce a qué terminal concreto se le ha asignado la IP en un momento dado (IP privada)[102].

El segundo supuesto problemático a efectos de la identificación del infractor surge cuando varias personas tienen acceso al mismo terminal (los distintos miembros de una familia, los distintos usuarios de un ordenador ubicado en un cibercafé). Ello plantea la duda de cuál de dichas personas fue la que uti-

---

ción, la suspensión del servicio por los intermediarios, el deber de información de las empresas prestadoras de servicios de Internet y el canon digital.

[101] Así lo señala también González Gozalo, A., «La propiedad intelectual y la protección de datos de carácter personal en las redes P2P», cit., p. 17, nota 5.

[102] Así lo señala González Gozalo, A., «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», cit., p. 82.

lizó el equipo el día y la hora concreta en la que intercambiaron los archivos protegidos por la propiedad intelectual.

Con todo, creo que las dudas que puede plantear la aplicación de las diligencias preliminares del art. 256.1.7.º LEC en estos supuestos también pueden resolverse con nuestra legislación civil en la mano.

En concreto, respecto de las redes de área local, porque igual que es posible dirigir las diligencias preliminares de este art. 256.1.7º LEC contra un prestador de acceso, también es posible solicitarlas contra el administrador de una red de área local (empresa, administración, Universidad), una vez que el prestador de acceso nos ha facilitado la identidad del administrador de dicha LAN[103]. Será este administrador de área local el que deba comunicar al Juez civil quién es la persona titular del terminal a la que se asignó una IP privada en un momento dado.

A partir de ahí, parece que podremos utilizar una presunción razonable de que la persona que usa habitualmente el terminal es la misma que se ha conectado a Internet para llevar a cabo los actos de infracción de derechos de propiedad intelectual. Naturalmente, estamos ante una presunción *iuris tantum* que el utilizador habitual del terminal podrá vencer, identificando en su caso a otras personas que tienen acceso al ordenador o al infractor concreto, si es que lo conoce. Ello podrá desembocar en, su caso, en la aplicación de las reglas de la solidaridad impropia a este supuesto. Habrá que tener en cuenta además la regla del art. 1903.4º CC respecto de la responsabilidad del empresario por los actos realizados por sus dependientes.

Algo similar debe ocurrir en el supuesto de que haya una pluralidad de personas que utiliza un mismo ordenador, en el que parece que debe existir la presunción *iuris tantum* de que el titular de la cuenta de acceso a Internet es quien lo ha utilizado para conectarse a la Red.

De este modo, si dicho titular alega que no ha sido él el que ha cometido la infracción, para poder eximirse totalmente de responsabilidad deberá realizar una identificación concreta de quién es la persona responsable. Si no puede o no quiere realizar dicha identificación, el abonado que contrató la cuenta de acceso a Internet debe ser considerado al menos como responsable solidario de la infracción, sin perjuicio de que pueda repetir luego lo pagado del verdadero infractor[104]. Así ocurrirá, por ejemplo, en el caso de un cibercafé o cuando un ordenador es utilizado por los distintos miembros de una familia.

---

[103] González Gozalo, A., «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», cit., p. 133.
[104] En Alemania se ha llegado a afirmar esta responsabilidad solidaria respecto de hijos mayores de edad que convivían en el hogar, como ocurre con la sentencia del *Landgerich* de Düsseldorf de

Habrá que tener en cuenta además en su caso las reglas generales de responsabilidad de los padres respecto de sus hijos menores (1903.II CC), como ha ocurrido por ejemplo en Alemania, en donde la sentencia del *Landgericht* de Colonia de 1 de diciembre de 2010[105] ha afirmado que los padres son los responsables del uso de Internet por parte de su hijo adolescente cuando lo utiliza para intercambiar archivos en redes *peer-to-peer*.

3. El régimen de la Ley 25/2007, de Conservación de datos en las Comunicaciones Electrónicas

Hemos afirmado que la diligencia preliminar del art. 256.1.7º LEC puede utilizarse para obligar a los prestadores de acceso a desvelar el nombre y dirección de los usuarios de sus servicios cuando los utilizan para intercambiar archivos en redes P2P, sin que sea un obstáculo para dicha interpretación la mención a la «escala comercial» de la infracción ni la regulación comunitaria en materia de protección de datos personales en las comunicaciones electrónicas.

Sin embargo, debemos analizar si dicha interpretación es también compatible con la consideración del nombre del usuario y de su dirección IP como «datos de tráfico» y con la regulación que hace de esta materia la Ley de Conservación de Datos en las Comunicaciones Electrónicas, norma posterior a la introducción en la LEC de la diligencia preliminar que hemos estudiado.

1. *La regulación de la LCDCE*

El régimen originariamente previsto en el art. 12 de la LSSI por la Ley 34/2002 debía modificarse por la ulterior publicación de la Directiva sobre Conservación de Datos en las Comunicaciones Electrónicas, lo que se hizo mediante la LCDCE, cuyo art. 1 establece que los prestadores de acceso tienen el deber de ceder un lista de datos de tráfico especialmente protegidos a los agentes facultados «siempre que le sean *requeridos a través de la correspondiente autorización judicial* con fines de detección, investigación y enjuiciamiento *de delitos graves* contemplados en el Código penal o en las Leyes penales especiales».

Los «datos de tráfico» que han de conservarse (y eventualmente, cederse con autorización judicial) están definidos en el art. 3 de la Ley, que incluye respecto del servicio de acceso a Internet «*el nombre y dirección del abonado o del usuario* registrado al que se le ha asignado en el momento de la comunicación

---

25 de mayo de 2009, disponible en <http://www.lawfirm.biz/nc/decisions-file-sharing/27-05-2009-lg-duesseldorf-12-o-134-09.html>.

[105] La sentencia está disponible en <http://www.lawfirm.biz/nc/decisions-file-sharing/01-12-2010-lg-koeln-28-o-594-10.html>.

una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono» (vid la letra a), número 2º, apartado ii) del art. 3.1 LCDCE), y también las propias *direcciones IP y la fecha y hora de la conexión y desconexión del usuario* (letra c), número 2º, apartado i) de este art. 3 LCDCE)[106].

A la vista de dicha regulación resulta evidente que este art. 1 de LCDCE es susceptible de ser interpretado de manera que cuando el ilícito es meramente civil, o es un delito no catalogado como grave, *no existiría obligación* por parte de los prestadores de acceso de ceder los datos protegidos por el art. 3 a las autoridades nacionales (en este caso, a juez civil). Con ello, no sólo se habrían reiterado los efectos negativos del ahora derogado art. 12 LSSI en cuanto a la impunidad de las conductas civiles, sino que incluso se habría endurecido dicho régimen, al considerarse ahora posible la cesión de los datos de tráfico a las autoridades nacionales únicamente para el caso de delitos *graves*.

A estos efectos, serían delitos graves según el art. 13.1 del Código Penal (CP) aquellos para los que propio Código prevé una pena calificada como grave, lo que, según el art. 33.2 CP incluye, entre otras, la pena de prisión *superior* a cinco años[107]. A ello hay que añadir que el TC ha considerado en sus SSTC 299/2000, de 11 de diciembre y 82/2002, de 22 de abril que, además de la cuantía de la pena, un delito puede ser calificado como grave también por la importancia del bien jurídico protegido o a la relevancia social de los hechos.

Resulta claro por tanto que, salvo que consideremos como «grave» el delito contra la propiedad intelectual por los etéreos criterios del bien jurídico protegido o la relevancia social de los hechos (como ha hecho por cierto el propio TC en algún caso relacionado con la propiedad intelectual, en las SSTC 167/2002, de 18 de septiembre y 104/2006, de 3 de abril), en principio quedan al margen de esta interpretación de la Ley de Conservación de Datos los delitos tipificados en los arts. 270 y ss del CP. También otros delitos no considerados como graves, y todas las faltas reguladas en el Código Penal (incluyendo las faltas contra la propiedad intelectual del art. 623.5 CP). Y también, naturalmente, todos los

---

[106] El plazo de conservación de los datos de tráfico es con carácter general de 12 meses (art. 5.1 LCDCE), aunque determinados datos pueden ver ampliado hasta dos años su plazo de conservación máximo, mientras que en otros el plazo mínimo se puede reducir a sólo seis meses, tomando en cuenta para esta ampliación o reducción del plazo el coste de almacenamiento y conservación de los datos frente a su interés de cara la investigación, detección y enjuiciamiento de un delito grave.

[107] Otras penas graves citadas por el art. 33.1 del Código Penal son la inhabilitación absoluta, las inhabilitaciones especiales por tiempo superior a cinco años, la suspensión de empleo o cargo público por tiempo superior a cinco años, la privación del derecho a conducir vehículos a motor y ciclomotores por tiempo superior a ocho años, la privación del derecho a la tenencia y porte de armas por tiempo superior a ocho años, la privación del derecho a residir en determinados lugares o acudir a ellos, por tiempo superior a cinco años, la prohibición de aproximarse a la víctima o a aquellos de sus familiares u otras personas que determine el juez o tribunal, por tiempo superior a cinco años, la prohibición de comunicarse con la víctima o con aquellos de sus familiares u otras personas que determine el juez o tribunal, por tiempo superior a cinco años y la privación de la patria potestad.

ilícitos civiles, como son las violaciones de derechos de propiedad intelectual que tienen lugar a través de redes *peer-to-peer*.

Esta interpretación literal del art. 1 de la LCDCE parece confirmarse porque el art. 6 establece que la cesión de los datos protegidos por el art. 3 sólo puede hacerse conforme a lo previsto en la propia LCDCE, para los fines que en ella se determinan y contando con una autorización judicial previa. Ello parece excluir la posibilidad de que los datos de tráfico puedan ser cedidos utilizando habilitaciones legales previstas por otras leyes.

Además, sólo pueden cederse los datos de tráfico protegidos por la Ley a una lista cerrada de «agentes facultados», nominados expresamente en el art. 6.2 de la LCDCE. Y entre estos agentes facultados (básicamente los encargados en nuestro sistema de la detección y prevención de delitos, como los Cuerpos y Fuerzas de seguridad del Estado, el personal del CNI o los funcionarios de Vigilancia Aduanera) no se encuentran los jueces civiles.

También confirmaría esta interpretación literal de la LCDCE el hecho de que su art. 7, al regular el procedimiento de cesión de datos, señale que la resolución judicial en la que se ordena la cesión debe determinar los datos que han de ser cedidos a los agentes facultados «*conforme a los previsto en la Ley de Enjuiciamiento Criminal* y de acuerdo con los principios de necesidad y proporcionalidad». Parece por tanto que sólo el Juez penal, en el marco de la investigación de un delito, puede autorizar la cesión de los datos de tráfico mencionados en el art. 3 de la Ley.

A partir de esta regulación, la Sección 28ª de la Audiencia Provincial de Madrid ha denegado hasta en tres ocasiones la petición de que los prestadores de acceso a Internet faciliten la identidad de los usuarios de redes P2P para promover un ulterior juicio en sede civil contra ellos (autos de 19 de febrero de 2010[108], 12 de abril de 2010[109] y 12 de noviembre de 2010[110]).

En el primero de estos autos (que los otros reproducen casi íntegramente, por estar ante supuestos de hecho idénticos), la AP de Madrid afirma respecto de los arts. 1 y 6 de la LCDCE que «*La claridad de precepto no puede ofrecer el menor atisbo de duda sobre la imposibilidad de requerir a las entidades prestadoras del servicio a Internet para que cedan sus datos para finalidades distintas de las previstas en la Ley, en este caso para promover un litigio civil sobre infracciones de propiedad intelectual*».

Añade la AP de Madrid que mediante la regulación de la LCDCE el legislador ha calibrado los distintos intereses en juego, haciendo que prevalezca el de-

[108] JUR 2010/133094.
[109] AC 2010/1001.
[110] AC 2010/2305.

recho a la intimidad personal y de la confidencialidad de los datos de tráfico en las comunicaciones electrónicas sobre los derechos exclusivos de propiedad intelectual, sin que esto resulte contrario al derecho a la tutela judicial efectiva del art. 24 CE.

Es evidente por tanto que en nuestros Tribunales (al menos en la AP de Madrid) ha prevalecido una interpretación literal de la Ley, que, sin embargo, no es desde mi punto de vista la más acertada a la luz de otras normas de nuestro Ordenamiento jurídico (en especial, de la Constitución) y del Derecho comunitario, como se explica a continuación.

2. *La LCDCE a la luz del Derecho constitucional*

La interpretación de la LCDCE que afirma que Juez de lo Mercantil no puede requerir a un prestador de acceso a Internet para que desvele el nombre y dirección de un usuario que ha infringido derechos de propiedad intelectual en una red P2P implica en la práctica una negación absoluta de la posibilidad de tutelar dichos derechos a través de la acción prevista en el art. 140 LPI.

Esto genera en los titulares de derechos de propiedad intelectual una evidente indefensión y crea un ámbito de impunidad que de ninguna manera puede admitirse sin violentar el contenido esencial de los derechos previstos en los arts. 32.1 CE (derecho de propiedad, que incluye la propiedad intelectual) y 24 CE (tutela judicial efectiva), derecho éste último que incluye tanto la protección del derecho al acceso a los tribunales para plantear cuantas peticiones sean procedentes para la defensa de los intereses legítimos (art. 24.1 CE) como la posibilidad de utilizar todos los medios probatorios que se estimen pertinentes (art. 24.2 CE)[111].

Dichas normas de rango constitucional garantizan que los titulares de cualquier derecho subjetivo (incluyendo los derechos de propiedad intelectual) puedan, con la ayuda del juez civil, y si éste lo considera pertinente, identificar al posible infractor de sus derechos a los efectos de plantear una demanda indemnizatoria.

Lo que decimos se comprende más fácilmente si pensamos en otros supuestos no relacionados con la propiedad intelectual que no serían calificables como delito grave a efectos de la LCDCE, pero que tienen evidentes implicaciones constitucionales. Así, pensemos por ejemplo en un usuario de redes P2P concreto que sólo tiene en su carpeta compartida fotografías de una persona desnuda, lo que obviamente supone una violación del derecho a la intimidad personal de la persona fotografiada de acuerdo con el art. 18.1 CE.

---

[111] Así lo señala también González Gozalo, A., «La propiedad intelectual y la protección de datos de carácter personal en las redes P2P», cit., p. 61.

En este supuesto, el art. 18.4 CE, base constitucional de la protección de datos de carácter personal, expresamente prevé que la Ley «*limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos, y el pleno ejercicio de sus Derechos*». Y es evidente que la Ley no sólo debe limitar la informática para proteger la intimidad de las personas frente al mal uso de los datos de carácter personal. También debe limitar la informática (en este caso, el intercambio en redes informáticas) cuando otras facetas del derecho a la intimidad garantizado por el art. 18.1 CE están comprometidas. El hecho de que la intromisión ilegítima se haya cometido a través de una red *peer-to-peer* en nada debe obstaculizar la tutela judicial efectiva del derecho.

No puede ser por tanto más evidente que estamos ante derechos constitucionales que están en pie de igualdad, sin que uno pueda prevalecer de forma absoluta sobre el otro. Así lo exige además el propio art. 9.2 de la Ley 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen, que expresamente prevé que «la tutela judicial comprenderá *todas las medidas necesarias* para poner fin a la intromisión ilegítima de que se trate, y restablecer al perjudicado en el pleno disfrute de sus derechos, *así como para prevenir o impedir intromisiones ulteriores*. Y no parece que la LCDCE haya supuesto una derogación de dicho precepto.

De ahí se desprende a mi juicio que si «la Ley» no garantiza derechos fundamentales en un caso concreto (como ocurriría con una interpretación literal de la LCDCE que entendiera que no se puede desvelar en la identidad del usuario de la red P2P en supuestos como el del intercambio de fotografías que vulneran el derecho a la intimidad por no estar ante un delito grave), dicha Ley es derechamente inconstitucional[112].

De hecho, esta interpretación de la LCDCE privaría a cualquier afectado por un ilícito civil cometido a través de redes P2P de su derecho a ser indemnizado por los daños sufridos, lo que no sólo resulta contrario a nuestra Carta Magna, sino también a uno de los principios esenciales de nuestro Derecho civil, el principio de *neminem laedere* y la consiguiente obligación de reparar el daño causado del art. 1902 del CC.

Fortalece esta afirmación el hecho de que la Sala Primera del Tribunal Supremo haya afirmado (como no podía ser menos) que la protección civil de los derechos

---

[112] Algo similar a lo que hemos señalado respecto de la Constitución española ocurre en la Carta de los Derechos Fundamentales de la Unión Europea, que reconoce no sólo el Derecho a la protección de datos de carácter personal (art. 8) sino también el Derecho de propiedad (art. 17.1), incluyendo el Derecho de propiedad intelectual (art. 17.2) y el Derecho a la tutela judicial efectiva (art. 47). Es claro por tanto estos tres derechos se limitan y condicionan recíprocamente, como expresamente señala el art. 52.1 *in fine* de la propia Carta. Vid. en ese sentido, González Gozalo, A., «El conflicto entre la propiedad intelectual y el derecho a la protección de datos de carácter personal en las redes P2P», cit., pp. 37-39.

fundamentales también debe tener lugar respecto de los servicios de la sociedad de la información. Así se dice por ejemplo claramente en la STS (Sala de lo Civil) de 10 de febrero de 2011[113], en un supuesto en el que el demandado era un prestador de alojamiento de la página web «alasbarricadas.org» que había consentido la aparición en los foros de su página de comentarios y fotografías claramente vejatorios[114] para el derecho al honor del actor, el artista *Ramoncín*.

Y si ello ocurre respecto del prestador de alojamiento de una página web, no parece haber motivo alguno que nos incline a pensar que la solución debe ser distinta en el hipotético caso de que dichos comentarios y fotografías vejatorias para el derecho al honor se distribuyeran en redes P2P (por ejemplo, a través de archivos PDF).

Y ello porque, en definitiva, el medio tecnológico utilizado para la intromisión en un derecho fundamental (radio, televisión, prensa, redes sociales, páginas web, redes P2P...) no debería ser relevante respecto de la obtención de una tutela judicial efectiva de dicho derecho fundamental en nuestro sistema constitucional.

De hecho, es impensable a mi juicio que nos atuviéramos a la literalidad de la Ley y consideráramos que no se puede solicitar que se desvele la identidad de usuarios de redes P2P implicados en determinadas modalidades del delito de difusión de imágenes pornográficas de menores o incapaces, conducta que tiene una consideración penal en principio de «delito no grave» en los arts. 189.1 CP (pena de prisión de uno a cinco años para la elaboración y difusión de este material pornográfico) y 189.2 CP (pena de tres meses a un año o multa de seis meses a dos años para la posesión para uso propio de dicho material) si no concurren los agravantes previstos en el apartado 3 de este mismo artículo.

Tan impensable, que ya hemos visto que la jurisprudencia de la Sala Segunda del Tribunal Supremo antes citada ha ampliado el concepto de «delito grave» de la LCDCE a este supuesto, considerando conforme a nuestra legislación que el juez instructor obligara a los prestadores de acceso a desvelar la identidad de los usuarios de redes P2P en estos casos[115].

---

[113] RJ 2011/313.

[114] Además de una fotografía manipulada en la que el artista aparecía con la cabeza cortada, los comentarios calificaban a *Ramoncín*, entre otras cosas, de «gilipollas, pedante, creído, tocapelotas/ovarios, farandulero, feo pasado por los quirófanos...».

[115] Con todo, hay que señalar cómo lamentablemente la literalidad de la LCDCE no sólo está sirviendo para que las AP denieguen la petición de identificación de usuarios de Internet en casos de violaciones de derechos de propiedad intelectual, sino también incluso en el ámbito de delitos no graves. Así, ocurre por ejemplo una decisión del Juzgado de Instrucción número 5 de Córdoba que deniega la solicitud de la policía de revelar la identidad que se ocultaba detrás de una serie de direcciones IP utilizadas para colgar comentarios a las noticas aparecidas en la página web del *Diario de Córdoba* que podían implicar un delito de calumnias. El Juez rechaza mediante auto de 15 de noviembre de 2010 (ARP 2011/270) la petición de identificación de los usuarios por no estar

Además de estas consideraciones de orden constitucional, desde el punto de vista estrictamente legal parece claro que la LCDCE debe ser compatible con el resto de normas de rango legal, lo que incluye los arts. 256.1.7º LEC y el art. 140 LPI, que no han sido derogados por esta Ley. Y ello hace posible interpretar que la cesión del nombre y de la dirección postal del usuario en casos de violación de derechos de propiedad intelectual es una cuestión resuelta por las normas civiles antes citadas, que serían a estos efectos ley especial sobre la LCDCE[116].

Respalda esta argumentación el hecho de que la LCDCE es posterior a la Ley 19/2006, en la que se incluyó la nueva diligencia del art. 256.1.7º LEC en materia de propiedad intelectual, norma que no fue derogada ni expresa ni tácitamente por la propia LCDCE[117], a pesar de que obviamente el legislador de 2007 la conocía, al haberse aprobado apenas un año antes.

Resulta por tanto a mi juicio posible que el juez realice una interpretación de la LCDCE que, yendo más allá de su literalidad, integre los distintos derechos fundamentales en juicio haciendo en un análisis basado en el principio de proporcionalidad que concluya que deben desvelarse los datos de los usuarios cuando ello resulta necesario para la adecuada protección de la propiedad intelectual en redes P2P[118]

3. *La LCDCE desde el punto de vista del Derecho comunitario*

Además de los argumentos que provienen del Derecho español, encontramos también argumentos en el Derecho comunitario para defender que la interpretación correcta de la LCDCE debe ser que los jueces del orden jurisdiccional civil están facultados para solicitar al prestador de acceso la revelación de los nombres y direcciones postales de los usuarios que contrataron servicios de acceso a Internet desde los que se han producido intercambios en redes P2P.

---

dichos delitos entre los calificados como «graves» por la LCDCE ni por la entidad de la pena (dos años, lejos del mínimo requerido de cinco), ni por la relevancia social de los hechos, ni por la afectación al bien jurídico concreto, el honor de las personas. Lo sorprendente de este auto es que el propio juez reconoce que de esta manera se está creando un espacio de impunidad en la Red, de manera que los querellantes (unos Profesores de Medicina a los que se les acusaba de haber favorecido a sus hijas durante los estudios universitarios, dándoles preguntas de los exámenes y presionando a otros profesores para que les dieran las mejores calificaciones posibles) deben soportar tales afirmaciones sin tener ningún medio judicial para su defensa por el mero de hecho de verterse los comentarios calumniosos en la página web de un diario digital, en lugar, de por ejemplo, en la versión escrita del diario.

[116] Así lo señala también González Gozalo, A., «El conflicto entre la propiedad intelectual y el derecho a la protección de datos de carácter personal en las redes P2P», cit., p. 62.

[117] González Gozalo, A., «El conflicto entre la propiedad intelectual y el derecho a la protección de datos de carácter personal en las redes P2P», cit., p. 62.

[118] Así lo señala también Almagro Nosete, J., «Aspectos procesales del intercambio de ficheros en redes P2P», en *Los derechos de propiedad intelectual en la obra audiovisual*, cit., p. 298.

a) La LCDCE como implementación de la Directiva de Conservación de Datos

Así, tenemos en primer lugar la propia Directiva de Conservación de Datos, que es la norma implementada en el Derecho español por esta Ley 25/2007. Dicha Directiva establecía en su art.1 que su regulación tenía como objetivo armonizar las obligaciones de los proveedores de servicios de comunicaciones electrónicas (entre los que se encuentran los prestadores de acceso a Internet) en relación con la conservación de datos para garantizar que dichos datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal y como éstos se definan en la legislación de cada Estado miembro.

Es claro por tanto que la Directiva no tenía como objeto regular *todos los supuestos* en los cuales las autoridades nacionales (en especial, los jueces civiles), podían tener acceso a dichos datos (como se desprende del Considerando 25 de la norma), sino únicamente garantizar un mínimo en toda la UE en el supuesto de delitos graves[119].

Resulta por tanto legítimo interpretar la norma en el sentido de que sólo existe la *obligación comunitaria* de garantizar la cesión de los datos en estos supuestos (recuérdese que la norma se adopta poco después de los atentados terroristas de Londres, en un ambiente de preocupación porque Internet se convirtiera en un «canal seguro» para las actividades criminales).

Pero de ello no se desprende en absoluto que los Estados miembros no puedan en su legislación nacional prever otros supuestos distintos de cesión de datos de tráfico si se respetan el resto de normas comunitarias (en especial, las normas sobre protección de datos). Sólo así puede explicarse que, como hemos visto ya, en algunos Estados miembros (Reino Unido, Irlanda, Holanda, Suecia y Polonia), se considere perfectamente admisible y conforme con el Derecho comunitario establecer esta posibilidad en el ámbito de los litigios civiles para la defensa de derechos de propiedad intelectual.

b) La LCDCE a la luz de la Directiva 2001/29/CE, de Derechos de Autor en la Sociedad de la Información

Existe un segundo argumento proveniente del Derecho comunitario que impide interpretar la LCDCE como una barrera que imposibilita que los jueces civiles ordenen a los prestadores de acceso que les revelen el nombre y la dirección postal de los usuarios de sus servicios mediante unas diligencias preliminares en el marco de procesos de violación de derechos de propiedad intelectual.

---

[119] González Gozalo, A., «El conflicto entre la propiedad intelectual y el derecho a la protección de datos de carácter personal en las redes P2P», cit. pp. 30-31.

Se trata del art. 8.2 de la Directiva 2001/29/CE, de Derechos de Autor en la Sociedad de la Información (DDASI), norma que obliga a los Estados miembros a adoptar «*medidas necesarias para garantizar que los titulares de derechos cuyos intereses se vean perjudicados por un actividad ilícita llevada a cabo en su territorio puedan interponer una acción de resarcimiento por daños y/o solicitar medidas cautelares (…)*».

Parece claro que precisamente una de esas «medidas necesarias» para garantizar que los derechohabientes puedan interponer una acción indemnizatoria es lograr identificar la identidad de la persona que contrató una cuenta de acceso a Internet a la que se le asignó una dirección IP que fue utilizada para intercambiar archivos en redes P2P.

Sin esta identificación, y al contrario de lo que ocurre con la acción de cesación (en la que puede instarse la suspensión del servicio de acceso a la red al abonado sin necesidad de conocer su identidad) no es posible para los derechohabientes entablar una demanda con pretensiones indemnizatorias, lo que convertiría a la interpretación literal de la LCDCE que ha hecho la Audiencia Provincial de Madrid en no conforme con esta Directiva.

Con todo, y como ocurrió también con el caso de la Directiva Antipiratería, hay que tener en cuenta que el art. 9 de la propia DDASI expresamente señala que lo dispuesto en ella se aplica «sin perjuicio» de las disposiciones relativas a otras materias en las que incide el Derecho comunitario, entre las que se encuentran «la protección de datos y el derecho a la intimidad».

Dicha referencia en el art. 9 *in fine* de la DDASI fue interpretada por la sentencia del Tribunal de Justicia en el asunto *Promusicae* como una prueba de que la Directiva no crea la obligación para los Estados miembros de establecer un deber de comunicar los datos personales de los usuarios en el marco de un proceso civil para garantizar una protección efectiva a los derechos de autor. Se hace así un análisis de la norma literal, no finalista: como el deber de desvelar los datos de los usuarios en un proceso civil no se impone expresamente en la DDASI, dicho deber es inexistente a nivel comunitario.

Sin embargo, a mí me parece claro que con dicha interpretación se está desactivando lo previsto en este art. 8.2 DDASI, pues el resultado práctico de ver las cosas de este modo es que existe al menos un Estado miembro (España), en donde los titulares de derechos de propiedad intelectual perjudicados por una actividad ilícita no tienen garantizado que puedan interponer una acción de resarcimiento por daños en el caso concreto de las infracciones que cometen los usuarios a través de redes de pares.

Por este motivo creo que el «sin perjuicio» del art. 9 de la DDASI lo que significa es que hay que hacer compatibles por vía interpretativa las reglas sobre

protección de datos personales y el derecho a la intimidad con las reglas previstas en la DDASI, sin que unas prevalezcan sobre las otras. De otro modo, se estaría privando de eficacia a una disposición comunitaria imperativa (el art. 8.2 DDASI) en contra de las más elementales reglas de interpretación de las normas jurídicas.

No hay por tanto relación de jerarquía normativa a nivel comunitario que permita entender que la normativa sobre protección de datos personales es preferente respecto de la normativa sobre protección de los derechos de propiedad intelectual[120]. Como no la hay tampoco entre otras normas comunitarias que el propio art. 9 DDASI cita, entre las que se encuentran algunas tan variopintas como el derecho de contratos, la protección del patrimonio nacional, la legislación sobre prácticas restrictivas y competencia desleal, etc.

4. La situación tras la aprobación de la Disposición Adicional cuadragésimo tercera de la Ley de Economía Sostenible («Ley Sinde»)

Ya hemos señalado cómo a mi juicio la interpretación del art. 256.1.7º de la LEC a la luz de la Directiva Antipiratería permite a los jueces de lo Mercantil ordenar a los prestadores de acceso a Internet que les revelen el nombre y dirección de los usuarios de redes P2P que violan derechos de propiedad intelectual, sin que la regulación de la LCDCE haya derogado o modificado dicha interpretación.

Pues bien, parece que el último desarrollo legislativo en la materia, el de la D.A. 43 de la Ley de Economía sostenible, va en la línea señalada en este trabajo. En efecto, una de las novedades principales de esta «Ley Sinde» ha consistido en dar una nueva redacción al apartado segundo del art. 8 de la LSSI para hacer posible que los «órganos competentes para su protección» (la Comisión de Propiedad Intelectual) pueda requerir los datos identificativos de los responsables de infracciones de propiedad intelectual a los prestadores de servicios de la sociedad de la información a fin de que quien está realizando la conducta infractora pueda comparecer en el procedimiento que, conforme a este art. 8, puede acabar en la suspensión del servicio.

Dicha petición debe contar con el aval de una autorización previa del juez, que se debe obtener de acuerdo con el también novedoso art. 122 bis de la Ley reguladora de la jurisdicción contencioso-administrativa. En la solicitud dirigida al juez deben exponerse los motivos que justifican la petición y la documentación que la apoya, lo que obviamente deberá ser valorado por el juez de lo contencioso-administrativo para determinar si, a la luz del principio de proporcionalidad, hay indicios de infracción suficientes como para autorizar

[120] En el mismo sentido, González Gozalo, A., «La propiedad intelectual y la protección de datos de carácter personal en las redes P2P», cit., p. 33.

la cesión de los datos personales. Obtenida dicha autorización judicial, señala el art. 8.2 *in fine* de la LSSI que «los prestadores estarán obligados a facilitar los datos para llevar a cabo la identificación».

La nueva regulación plantea numerosas cuestiones, como, por ejemplo, quiénes son los «prestadores de servicios de la sociedad de la información» a los que se les puede requerir la cesión de los datos. Parece que lo más lógico será entender que la LSSI se quiere referir en realidad a quienes poseen esos datos, que son los «prestadores de servicios de intermediación» (lo que incluye en principio tanto a los prestadores de acceso como a los prestadores de alojamiento).

También resulta dudoso cómo va a poder cumplirse el plazo de 24 horas desde la petición hasta la resolución, especialmente si, como es el caso, tiene también que oírse al Ministerio Fiscal (apartado primero del art. 122 bis de la Ley reguladora de la jurisdicción contencioso-administrativa). Y desde luego no resulta fácil adivinar por qué en la Ley rituaria de lo contencioso-administrativo se hace una mención expresa al respeto de los arts. 18.1 y 18.3 de la Constitución, puesto que el secreto de las comunicaciones del art. 18.3 no se ve afectado en ningún caso por la revelación de los datos del operador de la página web en la que se están produciendo las conductas infractoras. Y el art. 18.1, respecto del derecho a la intimidad, debe ser respetado en todo caso, no sólo en este procedimiento.

Con todo, una cuestión sí parece clara: la nueva redacción del art. 8.2 de la LSSI no es directamente aplicable a los casos de infracción de Derechos de propiedad intelectual en redes *peer-to-peer*[121], pues el cauce del art. 122 bis de la Ley reguladora de la jurisdicción contencioso-administrativa sólo puede utilizarse para «identificar al *responsable de un servicio de la sociedad de la información* que está realizando la conducta presuntamente vulneradora». Y los usuarios que intercambian archivos en redes P2P no encajan en dicho concepto según la definición de la letra a) del Anexo de la LSSI, por no estar realizando una «actividad económica para el prestador de servicios».

Sin embargo, la reforma legal deja claro que el derecho de protección de datos personales no puede esgrimirse como argumento absoluto frente a la tutela judicial efectiva de los derechos de propiedad intelectual en la Red, que ahora están citados expresamente en la letra e) del art. 8.1 de la LSSI como uno de los bienes jurídicos especialmente protegidos a la hora de solicitar la suspensión de los servicios de la sociedad de la información[122].

---

[121] La propia Exposición de Motivos del Proyecto de Ley señalaba que el objetivo de la misma era que hacer frente a «las vulneraciones de la misma [la propiedad intelectual] realizadas mediante la puesta a disposición de contenidos en la web».

[122] Le parece insólita dicha adición a Durán Rivacoba, R., «La protección de la propiedad intelectual en el ámbito de la sociedad de la información y de comercio electrónico», *Aranzadi Civil-Mercantil*, núm. 2/2011, p. 4 de la versión en línea (BIB/2011/467).

Ello viene a corroborar la idea, antes expresada, de que la LCDCE pretende obligar a los prestadores de acceso a ceder los datos de tráfico para *garantizar* la persecución de determinados crímenes especialmente graves, pero que existen otras Leyes en nuestro Ordenamiento (como este nuevo art. 8.2 LSSI) que pueden autorizar la cesión de los datos de tráfico que permitan identificar a los responsables de distintos ilícitos civiles y penales a los efectos que las propias leyes señalen (en este caso, a los efectos de suspender un servicio de alojamiento de páginas web).

De hecho, sería absurdo a mi juicio pensar que el juez de lo contencioso-administrativo pudiera autorizar que se identifique a un usuario persona física que ofrece en una página web o en un blog personal una serie de enlaces a contenidos protegidos por la propiedad intelectual de acuerdo con el nuevo art. 8.2 de la LSSI para que se puedan retirar dichos contenidos de la red o bloquear el acceso a los mismos, y, sin embargo, el Juez de lo Mercantil no pudiera identificar *a este mismo usuario*[123] cuando intercambia directamente los contenidos en una red P2P a los efectos de entablar la correspondiente acción indemnizatoria de acuerdo con el art. 140 LPI[124]. Ello equivaldría a afirmar que los derechos de propiedad intelectual (contemplados en el art. 33 CE) tienen un valor diferente según sea la vía procesal elegida para su tutela, lo que no resulta admisible en nuestro sistema constitucional.

VI. CONCLUSIÓN

Hemos tratado en el presente trabajo de las complicadas relaciones entre el Derecho de protección de datos personales y el derecho a la tutela judicial efectiva de la propiedad intelectual, constatando lo excepcional de la situación española respecto de los países de nuestro entorno.

Así, mientras que en los Estados Unidos y en buena parte de los países importantes de la UE se parte de la base de que el intercambio ilícito de ficheros es suficiente para justificar la recogida y tratamiento de las direcciones IP y que se desvele el nombre los usuarios que se ocultan tras dichas direcciones IP en aras del interés legítimo a la tutela judicial efectiva, en nuestro país la situación es muy distinta.

En efecto, en España es también indiscutible que el intercambio de archivos en redes P2P es, cuanto menos, un ilícito civil de acuerdo con nuestra Ley de

---

[123] De hecho, si el operador del sitio web es una persona física en ambos casos los datos que se estarían solicitando al prestador de acceso son exactamente los mismos (el nombre y dirección del responsable de la infracción de un derecho de propiedad intelectual).

[124] De hecho, en una red P2P la afectación al derecho de propiedad intelectual es mayor, puesto que se pone la obra o prestación protegida directamente a disposición del público (no de forma indirecta, mediante un enlace).

Propiedad Intelectual, lo que genera una obligación de reparar el daño causado con dicho intercambio.

Sin embargo, la interpretación que se han hecho por parte de nuestras autoridades administrativas y judiciales del art. 256.1 7º LEC y de la regulación de la Ley 25/2007 impide *de facto* a los derechohabientes no sólo solicitar que se desvele la identidad de que quienes realizan este tipo de intercambios, sino incluso recoger y «tratar» direcciones IP utilizadas en el proceso de infracción sin la pertinente autorización judicial.

Se ha entendido por tanto entre nosotros que el derecho de protección de los datos personales y de los datos de tráfico debe prevalecer de forma absoluta sobre el derecho a la tutela judicial efectiva de la propiedad intelectual en el entorno de Internet.

Ello no sólo es incorrecto desde el punto de vista del Derecho comunitario y español (especialmente desde el punto de vista constitucional), sino que además convierte a España en refugio de aquellos usuarios que quieren llevar a cabo este tipo de conductas. Se ha creado así un auténtico paraíso para la piratería doméstica en Internet que resulta incompatible con las más elementales exigencias de un estado de Derecho, en donde el imperio de la Ley y la tutela judicial efectiva de los derechos han de ser la regla, no la excepción.

BIBLIOGRAFÍA

Almagro Nosete, J., «Aspectos procesales del intercambio de ficheros en redes P2P», en *Los derechos de propiedad intelectual en la obra audiovisual*, (O'Callaghan, X., Coordinador), Dykinson, Madrid, 2011.

Aparicio Vaquero, J.P., «El intercambio de archivos en redes de pares a la luz del derecho vigente», *Revista de Derecho y Nuevas Tecnologías, núm. 8,* 2005.

Bercovitz Rodríguez-Cano, R., y Marín López, J.J., «El límite de copia privada y las redes de intercambio peer to peer», *Cuadernos de Derecho Judicial,* 2007-3.

Bouza, M.A., y Castro Marques, M., «El caso Napster», en *Actas de Derecho Industrial y Derecho de Autor*, Tomo XXI-2000, Santiago de Compostela, 2001.

Durán Rivacoba, R., «La protección de la propiedad intelectual en el ámbito de la sociedad de la información y de comercio electrónico», *Aranzadi Civil-Mercantil*, núm. 2/2011.

Durán Rivacoba, R.,/García Llerena, V., «Protección de datos personales y del derecho a la intimidad vs. protección de la propiedad privada de carácter intelectual: consecuencias del caso PROMUSICAE», en *Los derechos de propiedad intelectual en la obra audiovisual*, (O'Callaghan, X., Coordinador), Dykinson, Madrid, 2011.

Garrote Fernández-Diez, I., «La suspensión cautelar o cesación definitiva de los servicios a los usuarios infractores de derechos de propiedad intelectual», *pe.i (Revista de Propiedad Intelectual),* núm. 27, 2007.

Ginsburg, J.,/Gaubiac, Y., «Contrefaçon, fourniture de moyens et faute: perspectives dans les systèmes de *Common Law* et civilistes à la suite des arrêts *Grokster* et *Kazaa*», *RIDA,* núm. 207, enero 2006.

González de Alaiza, J.J., «La lucha de los titulares contra las redes «peer-to-peer»», *Pe.i, Revista de Propiedad Intelectual,* núm. 18, 2004.

— «La sentencia de la Corte Suprema estadounidense en el caso Grokster: La matizada condena a los operadores P2P», *Pe.i (Revista de Propiedad Intelectual),* núm. 20, 2005.

— «Napster «Copias robadas», responsabilidad de los intermediarios y otros interrogantes para el derecho de autor en Internet», *Pe.i. (Revista de Propiedad Intelectual),* núm. 6, 2000.

González Gozalo, A., «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», *Pe.i, Revista de Propiedad Intelectual,* núm. 20, 2005.

— «La propiedad intelectual y la protección de datos de carácter personal en las redes P2P», *Pe.i, Revista de Propiedad Intelectual,* núm. 28, 2008.

Kuner, C., «Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of Justice», *E.I.P.R.,* 2008, num. 5.

Lucas-Schloetter, A., «La Loi Française relative au droit d'auteur dans la société de l'information», *Pe.i (revista de propiedad intelectual),* num. 25, 2007.

Plaza Penadés, J., *Propiedad Intelectual y Sociedad de la Información*, Aranzadi, 2001.