EL CONFLICTO ENTRE LA PROPIEDAD INTELECTUAL Y EL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN LAS REDES *PEER TO PEER*

por Alfonso González Gozalo
Doctor en Derecho. Abogado

Resumen: La protección de la propiedad intelectual frente a las infracciones que tienen lugar a través de redes *peer to peer* de intercambio de archivos requiere el tratamiento de datos personales y datos de tráfico de los usuarios. Dicho tratamiento, en mayor o menor medida, es necesario no sólo para la identificación de los infractores a fin de poder ejercitar contra los mismos las acciones legales oportunas, sino también para recabar la colaboración de los prestadores de servicios de acceso con vistas a poner fin a las infracciones que cometen sus abonados. La propiedad intelectual y el derecho a la protección de datos entran así en un conflicto cuya solución ha de partir de una equilibrada ponderación de los diversos intereses implicados, como ha señalado el Tribunal de Justicia de las Comunidades Europeas en su sentencia de 29 de enero de 2008 (*asunto Promusicae*). El presente estudio analiza las claves de ese conflicto, tanto a nivel comunitario como a nivel español, para concluir que el derecho a la protección de datos no puede convertirse en una garantía de impunidad para los infractores de la propiedad intelectual a través de redes *peer to peer*.

Palabras Clave: confidencialidad de las comunicaciones, datos personales, datos de tráfico, derecho de información, intermediarios, Internet, *peer to peer*, prestadores de servicios, propiedad intelectual, protección de datos, tutela judicial

Sumario:

TITLE: THE CONFLICT BETWEEN COPYRIGHT AND THE DATA PROTECTION RIGHT IN PEER TO PEER FILE SHARING NETWORKS

ABSTRACT: Protection against copyright infringements that occur over peer to peer file sharing networks requires the processing of users' personal data and traffic data. That processing is necessary in order not only to identify copyright infringers so that they may be sued, but also to get service providers' assistance to prevent users from infringing copyright. Thus there is a conflict between copyright enforcement and protection of personal data, whose solution stems from an appropiate and equitable balance of the different interests at stake, just as the European Court of Justice held in its opinion dated January 29th 2008 (*Promusicae*). This article analyzes the keys of this conflict, both at European and at Spanish level, and concludes that the data protection right may not become a guarantee of impunity for copyright infringements taking place over peer to peer networks.

KEY WORDS: confidentiality of the communications, personal data, traffic data, right of information, intermediaries, Internet, *peer to peer*, service providers, intellectual property, copyright, data protection, copyright enforcement

I. INTRODUCCIÓN

Es de sobra conocida la enorme preocupación que el intercambio masivo de obras y prestaciones protegidas a través de redes *peer to peer* suscita entre los titulares de derechos de propiedad intelectual. Esta preocupación está más que justificada, si tenemos en cuenta no sólo que en determinados ámbitos (fonográfico y audiovisual, por ejemplo) se trata de la modalidad de piratería más extendida y con más repercusión económica para las industrias afectadas[1], sino también que, tanto por su aceptación social como por el propio funcionamiento de Internet, estas infracciones son las más difíciles de combatir en nuestro país.

El mayor obstáculo con el que se encuentran los titulares de derechos de propiedad intelectual a la hora de defenderse frente a las infracciones que se cometen a través de redes *peer to peer* es el anonimato en que se amparan los usuarios de Internet para llevar a cabo conductas ilícitas. Frente a la propiedad intelectual y el derecho fundamental a la tutela judicial efectiva, los usuarios (y los proveedores de acceso) esgrimen su derecho a la protección de datos, que en el ámbito de las redes digitales de comunicaciones parece haberse convertido, de facto, en un derecho absoluto.

---

[1] De acuerdo con un estudio realizado por el Centro de Investigación del Mercado del Entretenimiento y la Cultura (CIMEC) para la Sociedad General de Autores (SGAE), durante 2007 se descargaron ilegalmente 1.200 millones de canciones en España, frente a los 800 millones de descargas ilícitas en 2006 y 500 en 2005 (vid. www.sgae.es/recursos/boletines/marzo_2008/generalista/news3.htm). El ochenta por ciento de esas descargas tuvieron lugar a través de redes *peer to peer*. De conformidad con datos igualmente de la SGAE, el volumen de descargas ilícitas de películas cinematográficas ascendió en 2007 a 300 millones, según publicó el periódico *El País* el 23 de abril de 2008 (vid. http://www.elpais.com/articulo/cultura/SGAE/gana/2007/pese/pirateria/elpepicul/20080423elpepicul_6/Tes).

Hace casi tres años analicé por primera vez ese conflicto de derechos. Mantenía entonces, en un artículo publicado en esta misma Revista[2], que los proveedores de acceso estaban obligados a revelar la identidad de aquellos destinatarios de sus servicios que se valen de los mismos para infringir la propiedad intelectual ajena. Desde entonces se han incorporado al derecho español la Directiva 2004/48/CE, de 29 de abril, relativa al respeto de los derechos de propiedad intelectual (en adelante, DRD-PI) y la Directiva 2006/24/CE, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (en adelante, Directiva de Conservación de Datos). El Tribunal de Justicia de las Comunidades Europeas, por su parte, ha dictado (reunido en Gran Sala) una importantísima sentencia, la de 29 de enero de 2008 (*Promusicae*)[3], que, aunque menos determinante de lo que unos y otros hubieran querido desear, por su carácter salomónico, contiene algunos razonamientos muy reveladores para tratar de solucionar el problema que nos ocupa. Estos nuevos elementos de juicio me han llevado a replantearme mi opinión con respecto al conflicto entre la propiedad intelectual y el derecho a la protección de datos en el entorno digital. Y, tras un nuevo análisis jurídico de la situación, he llegado esencialmente a la misma conclusión que hace tres años: el derecho a la protección de datos no puede proporcionar un ámbito de impunidad a los usuarios de Internet.

En las próximas páginas se exponen las claves del conflicto entre la tutela judicial efectiva de la propiedad intelectual, por un lado, y el derecho a la protección de datos de los usuarios de Internet, por otro, tanto a nivel comunitario como a nivel nacional, para terminar analizando qué pueden hacer los titulares de derechos de propiedad intelectual en nuestro país para protegerlos frente a infracciones que tienen lugar a través de redes *peer to peer*.

II. LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL FRENTE A INFRACCIONES QUE SE PRODUCEN A TRAVÉS DE REDES *PEER TO PEER*

1. La infracción de la propiedad intelectual a través de redes *peer to peer*

Punto de partida de este trabajo es que el intercambio no autorizado de obras o prestaciones protegidas a través de redes *peer to peer* constituye una infracción de la propiedad intelectual.

Así, cuando un usuario de Internet se conecta a cualquiera de estas redes y coloca en una carpeta compartida del disco duro de su ordenador un archivo protegido por la propiedad intelectual, está llevando a cabo ilícitamente un acto de comunicación pública en su modalidad de puesta a disposición —art. 20.2.i)

[2] *Vid*. 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.*, núm. 20, mayo-agosto de 2005, pp. 77 y ss.

[3] Asunto C-275/06.

TRLPI—, en la medida en que cualquier otro usuario puede acceder a la obra o prestación en cuestión desde el lugar y en el momento que elija.

Asimismo, la reproducción de dicho archivo en la carpeta compartida del ordenador del usuario constituye un acto ilícito de reproducción, ya que no está amparado ni por la excepción de copia privada (pues el uso al que la copia está destinada no es privado, sino colectivo) ni por ningún otro límite a la propiedad intelectual[4].

2. El necesario tratamiento de datos de los usuarios para la protección de la propiedad intelectual en las redes *peer to peer*

Las redes *peer to peer*, tal y como están configuradas en la práctica, permiten su uso prácticamente (no absolutamente) anónimo por los usuarios[5]. En efecto, para conectarse a una red *peer to peer* no es necesario, como regla general, registrarse. Tampoco lo es indicar un nombre de usuario, un alias o un *nikname* (es opcional)[6]. Ello permite a los usuarios mantener oculta su identidad mientras intercambian archivos, y ampararse en ese anonimato para infringir derechos ajenos.

Para proteger la propiedad intelectual frente a las infracciones que tienen lugar a través de estas redes, los titulares de derechos necesariamente deben tratar datos personales (direcciones IP)[7] y datos de tráfico[8] de los usuarios. A fin

[4] En este sentido se ha pronunciado de forma prácticamente unánime nuestra doctrina. Vid., por ejemplo, Garrote Fernández-Díez, I., «Acciones civiles contra los prestadores de servicios de intermediación en relación la actividad de las plataformas p2p – Su regulación en la Ley 34/2002 y en la Ley de Propiedad Intelectual», *Pe. i.*, núm. 16, enero-abril 2004, pp. 55 y ss.; González de Alaiza Cardona, J. J., «La lucha de los titulares de derechos de autor contra las redes «peer to peer» (P2P)», *Pe. i.*, núm. 18, septiembre-diciembre de 2004, pp. 25 y ss; Sánchez Aristi, R., *El intercambio de obras protegidas a través de las plataformas peer to peer*, Ed. Instituto de Derecho de Autor, Madrid, 2007, pp. 163 y ss., y un largo etcétera.

[5] Desde el momento en que para conectarse a Internet hace falta una dirección IP, asignada por un proveedor de acceso, no es posible hablar de un absoluto anonimato en Internet, ya que, en última instancia, este prestador de servicios podría determinar quién es el titular de la cuenta de acceso a través de la cual se ha realizado una concreta conexión. Cierto es, sin embargo, que es posible que sea un usuario distinto del titular de la cuenta de acceso quien realice esa conexión en particular.

[6] En cualquier caso, sólo si los nombres de usuario o alias fueran únicos, de tal manera que dos usuarios no pudieran utilizar el mismo, tendrían virtualidad para identificarlos en alguna medida.

[7] Sobre el carácter de dato personal de las direcciones IP, me remito a lo que ya expuse en el artículo «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 111-112. A lo dicho entonces conviene añadir que el Dictamen 4/2007 del Grupo de Trabajo del Artículo 29 de la Unión Europea, sobre el concepto de datos personales, adoptado el 20 de junio de 2007, ha insistido en el carácter de dato personal de las direcciones IP en el ámbito que nos ocupa, señalando lo siguiente: «Especialmente en aquellos casos en los que el tratamiento de direcciones IP se lleva a cabo con objeto de identificar a los usuarios de un ordenador (por ejemplo, el realizado por los titulares de los derechos de autor para demandar a los usuarios por violación de los derechos de propiedad intelectual), el responsable del tratamiento prevé que «los medios que pueden ser razonablemente utilizados» para identificar a las personas pueden obtenerse, por ejemplo, a través de los tribunales competentes (de otro modo la recopilación de información no tiene ningún sentido), y por lo tanto la información debe considerarse como datos personales» (cfr. p. 18).

[8] Datos de tráfico, según el 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 elec-

de obtener pruebas de la infracción, los titulares se conectan, por sí o por un tercero contratado a tal efecto (de acuerdo con lo dispuesto en el art. 12 de la Ley Orgánica de Protección de Datos, en adelante LOPD), a la red *peer to peer* a través de la cual se está infringiendo su propiedad intelectual. Una vez conectados, detectan a los usuarios que intercambian de forma masiva sus obras o prestaciones protegidas. A continuación copian el listado de los archivos que se encuentran alojados en sus carpetas compartidas (y, por ende, puestos a disposición de los demás usuarios conectados) y comprueban, mediante descarga de una muestra, que tales archivos contienen efectivamente las obras o prestaciones protegidas en cuestión. Finalmente, si de las anteriores operaciones resulta aparente que se están infringiendo sus derechos de propiedad intelectual, registran la fecha y hora exacta en que se produjo la supuesta infracción, el nombre de usuario (si consta) del supuesto infractor[9] y su dirección IP, así como el listado de archivos compartidos.

Esta primera actividad de detección de la infracción y recopilación de pruebas de la misma constituye un tratamiento de datos (personales y de tráfico) imprescindible para la tutela de la propiedad intelectual. Pero, por sí sola, esta labor resulta insuficiente para obtener la oportuna protección. Es necesario un segundo paso, el ejercicio de las acciones legales correspondientes, que, en abstracto, pueden ser penales o civiles. Sin entrar a valorar en este momento los problemas jurídicos que presentan una y otra vía, sí queremos dejar claro desde ahora que ambas requieren tratamientos adicionales de los datos de los infractores.

La vía penal, que se emprendería mediante la correspondiente denuncia, requiere la comunicación de los datos anteriormente reseñados a las autoridades competentes para el inicio de las diligencias previas de averiguación.

En cuanto a la vía civil, el titular de los derechos infringidos tiene dos alternativas. Puede demandar a los propios usuarios, ejercitando en su caso la acción de cesación y la de indemnización. Pero para ello es preciso, con carácter previo, averiguar su identidad, lo que no puede hacerse sin la colaboración del proveedor de acceso, quien, por otra parte, no es libre de comunicar el nombre y el domicilio (art. 11 LOPD). La averiguación de la identidad de los infractores, por tanto, sólo puede producirse mediante procedimientos de diligencias preliminares, a través de los cuales los titulares de derechos tratarían de obtener una orden judicial contra los prestadores de servicios que proveen acceso a Internet a los infractores, obligándoles a revelar la identidad de éstos.

---

trónicas, el servicio universal y la protección de los usuario, son cualesquiera datos tratados a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de su facturación. En el mismo sentido, vid. 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.

[9] La utilidad del nombre de usuario para identificar al infractor es mínima, como antes hemos indicado, salvo que se utilice como tal el nombre y los apellidos reales, que no es ni mucho menos lo normal. De hecho, si el nombre de usuario no sirve para identificar a la persona que está detrás del mismo, ni siquiera constituye un dato de carácter personal.

Ni que decir tiene que ello conlleva nuevos tratamientos de datos (comunicación a la autoridad judicial y al proveedor de acceso demandado de los datos recabados en la fase de detección de la infracción, tratamiento de esos datos por el operador para identificar al infractor si la solicitud de diligencias preliminares es estimada, comunicación de la identidad del infractor al titular de los derechos).

Si, por el contrario, el titular de los derechos se decantara por demandar a los proveedores de acceso, instándoles a suspender o terminar la conexión a Internet de sus abonados infractores —arts. 138.III, 139.1.h) y 141.6 TRLPI—, no sólo sería necesario tratar los datos de estos usuarios durante el procedimiento cautelar o principal correspondiente, sino también para dar cumplimiento a una eventual resolución condenatoria que obligara al proveedor de acceso a suspender el servicio prestado al infractor.

Así las cosas, es indudable que para la defensa de la propiedad intelectual frente a las infracciones que se producen a través de redes *peer to peer* es imprescindible el tratamiento de datos personales y de tráfico de los usuarios infractores. Ello supone un claro conflicto entre la propiedad intelectual y el derecho a la tutela judicial efectiva, por un lado, y el derecho a la protección de datos de los usuarios de Internet, por otro, para cuya resolución hemos de huir de opiniones extrajurídicas y convicciones apriorísticas, y centrarnos en el análisis riguroso de las disposiciones aplicables y las resoluciones judiciales que las interpretan, tanto a nivel comunitario como nacional.

III. LAS CLAVES DEL CONFLICTO A NIVEL COMUNITARIO

Son varias las normas comunitarias relevantes para la resolución del conflicto entre la tutela de la propiedad intelectual, por un lado, y la protección de datos (como manifestación del genérico derecho a la intimidad que la Carta de Derechos Humanos reconoce a los ciudadanos de la Unión Europea), por el otro. De dichas disposiciones no se desprende, en modo alguno, que el derecho a la protección de datos prevalezca sobre la propiedad intelectual.

En concreto, las normas comunitarias en las que los titulares de derechos de propiedad intelectual pueden fundar sus pretensiones son la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (en adelante, DCE); la Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información (DDASI); y, sobre todo, la Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril, relativa al respeto a los derechos de propiedad intelectual (DRDPI). También pueden invocar el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (Anexo 1C del

Acuerdo por el que se establece la Organización Mundial del Comercio y Acuerdos Anejos, entendimiento relativo a los compromisos en materia de servicios financieros y acuerdo sobre contratación pública, hechos en Marrakechel 15 de abril de 1994, en lo sucesivo Acuerdo ADPIC).

Por su parte, los prestadores de servicios de la sociedad de la información y los usuarios de Internet encuentran argumentos para su defensa en las Directivas que armonizan la protección de datos a nivel comunitario, en concreto la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva sobre Protección de Datos), la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la Privacidad y las Comunicaciones Electrónicas) y la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones por la que se modifica la Directiva 2002/58/CE (Directiva sobre Conservación de Datos).

Finalmente, ha de tenerse en cuenta lo dispuesto por la Carta de los Derechos Fundamentales de la Unión Europea.

Todas estas normas, excepción hecha de la Directiva sobre Conservación de Datos, han sido valoradas por el TJCE en su sentencia de 29 de enero de 2008, *Promusicae*, Asunto C-275/06, que resolvió una cuestión prejudicial planteada por el Juzgado de lo Mercantil núm. 5 de Madrid en el marco de un procedimiento de diligencias preliminares seguido por *Promusicae* (asociación para la defensa de los derechos de los productores fonográficos) contra *Telefónica*, en la que preguntaba si los ordenamientos nacionales pueden restringir al marco de una investigación criminal o para la salvaguardia de la seguridad pública y de la defensa nacional, con exclusión, por lo tanto, de los procesos civiles, el deber de retención y puesta a disposición de datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, que recae sobre los operadores de redes y servicios de comunicaciones electrónicas, proveedores de acceso a redes de telecomunicaciones y prestadores de servicios de alojamiento de datos

A continuación exponemos separadamente en qué medida inciden las normas comunitarias referidas en la resolución del conflicto que estamos analizando.

1. Las directivas comunitarias en materia de propiedad intelectual

Si bien no es una Directiva sobre propiedad intelectual, algunos preceptos de la **Directiva sobre Comercio Electrónico** pueden servir a los titulares de propiedad intelectual para defender la posibilidad de tratar datos personales y de

tráfico de los usuarios que infringen sus derechos a través de Internet. Es el caso del art. 15.2 DCE, del que se colige la facultad de los Estados miembros de establecer la obligación de los prestadores de servicios de la sociedad de la información, en el marco de procedimientos por infracción de derechos, de comunicar a las autoridades competentes, a solicitud de éstas, los datos que permitan identificar a los destinatarios de sus servicios con los que hayan celebrado contratos de almacenamiento. Aunque se trata de una norma dispositiva para los Estados miembros, y referida únicamente a los prestadores de servicios de alojamiento (no a los proveedores de acceso), tiene el interés de que legitima «a las autoridades competentes» para solicitar a los prestadores de servicios la comunicación de los datos de identificación de los usuarios que se valen de esos servicios para realizar actos ilícitos a través de Internet. No limita esta medida al ámbito penal, por lo tanto. Es más, la legitimación de los tribunales civiles vendría corroborada por el Considerando 25 DCE, de acuerdo con el cual «los tribunales nacionales, *incluidos los tribunales civiles*, que conocen de controversias de Derecho privado pueden adoptar medidas que establecen excepciones a la libertad de prestar servicios en el marco de la sociedad de la información de conformidad con las condiciones establecidas en la presente Directiva». Si los tribunales civiles que conocen de litigios sobre Derecho privado pueden limitar la libertad de prestar servicios de la sociedad de la información, imponiendo, por ejemplo, la suspensión de la prestación del servicio de acceso a Internet a un usuario determinado que vulnera derechos ajenos, ¿por qué no van a poder exigir igualmente la identificación de ese usuario infractor?

Resulta también relevante el art. 18.1 DCE, en cuanto que obliga a los Estados miembros (se trata, pues, de una norma imperativa) a prever recursos judiciales que permitan adoptar rápidamente medidas destinadas a poner término a cualquier presunta infracción. El tenor de este art. 18.1 DCE es muy amplio. Se refiere a cualquier medida judicial tendente a la cesación de la presunta infracción y a evitar la producción de nuevos daños para el perjudicado. Comprende, por tanto, no sólo medidas provisionales (cautelares) y definitivas de cesación, sino también cualesquiera otras sin las cuales esa cesación provisional o definitiva sería imposible. Y entre estas medidas se encuentran las que sean necesarias para identificar al infractor, como presupuesto para poder instar la cesación cautelar o definitiva de la conducta ilícita[10]. Además, dado que las medidas de cesación son de carácter civil, también han de serlo las medi-

[10] En consonancia con el art. 18.1, el Considerando 52 de la Directiva resalta la necesidad de garantizar a los perjudicados por las infracciones cometidas a través de Internet recursos judiciales eficaces para defender sus intereses. Dispone: «El ejercicio efectivo de las libertades del mercado interior *hace necesario que se garantice a las víctimas un acceso eficaz a los medios de resolución de litigios*. Los daños y perjuicios que se pueden producir en el marco de los servicios de la sociedad de la información se caracterizan por su rapidez y por su extensión geográfica. Debido a esta característica y a la necesidad de velar por que las autoridades nacionales eviten que se ponga en duda la confianza mutua que se deben conceder, *la presente Directiva requiere de los Estados miembros que establezcan las condiciones para que se puedan emprender los recursos judiciales pertinentes*. Los Estados miembros estudiarán la necesidad de ofrecer acceso a los procedimientos judiciales por los medios electrónicos adecuados».

das para la averiguación de la identidad del supuesto infractor. Por consiguiente, serán los tribunales civiles los competentes para adoptarlas.

Ahora bien, si los preceptos anteriores operan a favor de los titulares de derechos, no puede pasarse por alto que el art. 1.5.b) DCE establece que esta Directiva no se aplicará «a cuestiones relacionadas con servicios de la sociedad de la información incluidas en las Directivas 95/46/CE (Directiva sobre Protección de Datos) y 97/66/CE (predecesora de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas)». De donde cabría colegir que las disposiciones de la DCE no pueden funcionar como excepciones a los derechos que las Directivas en materia de protección de datos reconocen a los usuarios de Internet[11].

Otra Directiva que puede ser invocada por los titulares de derechos es la **Directiva relativa a los Derechos de Autor y los Derechos Afines en la Sociedad de la Información**. Según su art. 8 los Estados miembros deben garantizar a los titulares de derechos de propiedad intelectual los recursos y medidas judiciales necesarios para poder ejercitar las acciones pertinentes para poner fin, incluso cautelarmente, a cualquier infracción de sus derechos y obtener una indemnización por los daños y perjuicios derivados de esa infracción. En consonancia con este artículo, el Considerando 58 DDASI es claro cuando señala que los Estados miembros no sólo tienen que prever sanciones y vías de recurso efectivas contra las infracciones de derechos de propiedad intelectual, sino que también han de adoptar las medidas necesarias para garantizar que se apliquen tales sanciones y vías de recurso. Dado que, como hemos visto, el éxito de estas pretensiones requiere el tratamiento de datos de los presuntos infractores, parece que implícita en esta norma se encuentra una habilitación para tratar esos datos cuando existan indicios fundados de la infracción y el tratamiento resulte imprescindible para el ejercicio de las correspondientes acciones. Por otro lado, si tenemos en cuenta que tanto las pretensiones de cesación, definitiva o cautelar, como las pretensiones resarcitorias tienen carácter civil, y que estas últimas sólo pueden hacerse valer si se conoce la identidad de los supuestos infractores (pues de lo contrario no se les podría demandar), es posible deducir del art. 8 y del Considerando 58 DDASI que los Estados miembros están obligados a establecer medidas judiciales que permitan, en el marco de los procedimientos civiles por la infracción de derechos de propiedad intelectual, averiguar la identidad de los presuntos infractores, como presupuesto para ejercitar las acciones pertinentes para la cesación de la conducta ilícita y la indemnización de los daños y perjuicios.

Ahora bien, como ocurría con la DCE, no puede pasarse por alto que el art. 9 DDASI establece que esta Directiva «se entenderá sin perjuicio de las disposiciones relativas, en particular a (…) la protección de datos y el derecho a la intimidad». De donde cabría colegir, igualmente, que las disposiciones de la DDA-

[11] Este fue, de hecho, el argumento esgrimido por la Comisión en su escrito de alegaciones en el procedimiento prejudicial C-275/06 (*Promusicae*) seguido ante el TJCE.

SI no constituyen una excepción a los derechos que las Directivas sobre protección de Datos reconocen a los usuarios de Internet[12].

Pero sin duda, la Directiva que más favorable parece a los intereses de los titulares de propiedad intelectual es la **Directiva sobre Respeto de los Derechos de Propiedad Intelectual**, cuyo art. 8 les reconoce el llamado «derecho de información», que les faculta para solicitar a la autoridad judicial competente que requiera, entre otros, a quienes prestan a escala comercial servicios de los que un tercero se vale para vulnerar sus derechos (por ejemplo, un proveedor de acceso a Internet), para que faciliten los datos sobre el origen y las redes de distribución de las mercancías o servicios que infringen tales derechos, entre ellos la identidad del supuesto infractor.

Es indudable que cuando este artículo 8 DRDPI se refiere a las autoridades judiciales competentes está aludiendo a los tribunales civiles, y en ningún caso a los penales, tal y como se colige tanto del art. 16 como del Considerando 28 DRDPI, que califican las medidas, procedimientos y recursos establecidos por esta Directiva como de carácter civil o administrativo, y no penales. Por tanto, el derecho de información que se regula en el art. 8 DRDPI no consiste en el derecho a ser informado sobre el origen de la infracción en el marco de un procedimiento penal, sino a serlo en el ámbito de un procedimiento civil seguido por una infracción de derechos de propiedad intelectual. Lo que significa que, dado que la DRDPI es una Directiva que establece un mínimo de protección para los titulares de derechos de propiedad intelectual (art. 2.1 DRDPI), no se les puede privar de su facultad de solicitar a los tribunales civiles que ordenen a quienes prestan a escala comercial el servicio de acceso a Internet la comunicación de la identidad de quienes se valen de esos servicios para infringir su propiedad intelectual.

Ahora bien, la duda la suscita el art. 8.3.e) DRDPI, de acuerdo con el cual los apartados 1 y 2 de este artículo (que desarrollan el derecho de información) «se aplicarán sin perjuicio de otras disposiciones legales que rijan (…) el tratamiento de los datos personales». Una vez más, es posible interpretar este art. 8.3.e) en el sentido de que el derecho a la información está supeditado a lo que dispongan las Directivas en materia de protección de datos[13].

2. El acuerdo Adpic

El Acuerdo ADPIC, que fue ratificado por el Estado español el 30 de diciembre de 1994, es un convenio internacional que vincula a la Unión Europea desde su aprobación mediante Decisión de 94/800/CE del Consejo. En este sentido, el Tribunal de Justicia de las Comunidades Europeas ha resuelto que el Acuerdo ADPIC forma parte del Derecho comunitario, y que, por tanto, el pro-

[12] Como, de nuevo, alegó la Comisión en el marco de la cuestión prejudicial planteada ante el TJCE por el Juzgado de lo Mercantil núm. 5 de Madrid en el asunto *Promusicae*.

[13] Como, una vez más, alegó la Comisión en su escrito de alegaciones en el marco de la cuestión prejudicial del caso *Promusicae*.

pio Tribunal es competente para interpretarlo (vid. la sentencia de 16 de noviembre de 2004, *Anheuser-Busch* asunto C-245/02, apartados 41-43[14]).

El art. 41.1 obliga a los Estados miembros a establecer procedimientos de observancia de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acción infractora de los derechos de propiedad intelectual. El art. 42, por su parte, impone a los Estados miembros la obligación de poner al alcance de los titulares de derechos procedimientos civiles para lograr la observancia de los derechos de propiedad intelectual. De estos preceptos se desprende, pues, la obligación de los Estados miembros de prever las medidas que sean necesarias para que los titulares cuyos derechos de propiedad intelectual sean infringidos puedan iniciar el correspondiente proceso civil con vistas a poner fin a la infracción y obtener una indemnización por los daños y perjuicios sufridos. Entre esas medidas se encontrará la identificación de los supuestos infractores, si es presupuesto necesario para poder ejercitar la acción civil de defensa de derechos de propiedad intelectual.

En contra de la anterior afirmación puede oponerse que el art. 47 alude expresamente al derecho de información, si bien no lo configura como un derecho de reconocimiento obligatorio por los Estados miembros, sino facultativo. De acuerdo con este artículo, los Estados miembros «podrán disponer que, salvo que resulte desproporcionado con la gravedad de la infracción, las autoridades judiciales puedan ordenar al infractor que informe al titular del derecho sobre la identidad de los terceros que hayan participado en la producción y distribución de los bienes o servicios infractores, y sobre sus circuitos de distribución». El principio de especialidad podría conducir a entender que si este deber de información es de incorporación facultativa, los arts. 41 y 42 no pueden ser interpretados en el sentido de que obligan a establecer medidas dirigidas a identificar al infractor. Sin embargo, si bien nos fijamos, el art. 47 parte de la base de que ya hay un infractor identificado, que es el obligado a informar sobre la identidad de otras personas que hayan participado en la infracción y sobre los circuitos de distribución. Si ningún infractor está identificado, no estaríamos en el ámbito del art. 47, sino en el de los arts. 41 y 42, siempre que las medidas de identificación puedan tener éxito y sean imprescindibles para poder ejercitar las correspondientes acciones de cesación e indemnización.

---

[14] Señala el TJCE en esta sentencia: «41. De su jurisprudencia resulta que el Tribunal de Justicia es competente para interpretar una disposición del Acuerdo ADPIC con el fin de responder a las necesidades de las autoridades judiciales de los Estados miembros cuando éstas tengan que aplicar sus normas nacionales para ordenar medidas con objeto de proteger los derechos que se derivan de una normativa comunitaria comprendida en el ámbito de aplicación del citado Acuerdo (véase, en este sentido, la sentencia Dior y otros, antes citada, apartados 35 y 40 y jurisprudencia citada).

«42. En efecto, dado que la Comunidad es parte del Acuerdo ADPIC, está obligada a interpretar su normativa en materia de marcas, en la medida de lo posible, a la luz del texto y de la finalidad de dicho Acuerdo (véase, por lo que se refiere a una situación regulada a la vez por una disposición del Acuerdo ADPIC y por otra de la Directiva 89/104, la sentencia de 24 de junio de 2004, Heidelberger Bauchemie, C49/02, Rec. p. II0000, apartado 20).

«43. Por tanto, el Tribunal de Justicia es competente para interpretar el artículo 16, apartado 1, del Acuerdo ADPIC, disposición que constituye el objeto de las cuestiones prejudiciales segunda y tercera».

3. Las directivas comunitarias en materia de protección de datos

Hasta ahora hemos visto que para garantizar la correcta protección de la propiedad intelectual en Internet es preciso tratar los datos de los usuarios infractores, y que de las Directivas 2000/31/CE, 2001/29/CE y 2004/48/CE, así como del Acuerdo ADPIC, se desprende la obligación de los Estados miembros de adoptar todas las medidas necesarias para asegurar que los titulares de derechos de propiedad intelectual pueden ejercitar las acciones judiciales oportunas para obtener la cesación, cautelar y definitiva, de las infracciones de sus derechos como la correspondiente indemnización de daños y perjuicios. En la medida en que el ejercicio de tales acciones judiciales requiere el tratamiento de los datos de los infractores, podría colegirse que las citadas disposiciones habilitan a los titulares de derechos y a los prestadores de servicios para realizar dicho tratamiento aun sin el consentimiento de los usuarios.

Debemos analizar ahora si las Directivas comunitarias en materia de protección de datos se oponen a dicho tratamiento de los datos de los usuarios infractores. En caso de que pudiera ser así, el siguiente paso sería estudiar la relación existente entre unas y otras Directivas, a fin de determinar si alguna debe prevalecer sobre las demás.

Antes de adentrarnos en el examen de las Directivas sobre protección de datos, conviene hacer una apreciación común a todas ellas. La armonización llevada a cabo por el Derecho comunitario en relación con el derecho a la protección de datos no es mínima, sino completa, tal y como ha declarado el TJCE en su sentencia de 6 de noviembre de 2003, *Lindqvist* (asunto C-101/01, apartados 95 y 96), en relación con la Directiva 95/46/CE[15]. Esto quiere decir que, dentro del ámbito de aplicación de estas Directivas, no pueden los Estados miembros establecer una protección más rigurosa de los datos[16].

Entrando ya en el examen individual de las Directivas en materia de protección de datos, debe comenzarse por la **Directiva 95/46/CE sobre Protección de Datos Personales**. Esta Directiva resulta aplicable al conflicto que nos ocupa, en tanto en cuanto las direcciones IP constituyen datos personales y, a través de ellas, los titulares de derechos de propiedad intelectual quieren averi-

[15] Señala, en su parágrafo 96: «Por tanto, la armonización de dichas legislaciones nacionales no se limita a una armonización mínima, sino que constituye, en principio, una *armonización completa*. Desde este punto de vista, la Directiva 95/46 trata de asegurar la libre circulación de datos personales, garantizando al mismo tiempo un alto nivel de protección de los derechos e intereses de las personas titulares de dichos datos».

[16] Así lo ha señalado el TJCE en la referida sentencia de 6 de noviembre de 2003, *Lindqvist* (asunto C-101/01, apartado 99): «A la luz de estas consideraciones, procede responder a la séptima cuestión que las medidas adoptadas por los Estados miembros para garantizar la protección de los datos personales deben atenerse tanto a las disposiciones de la Directiva 95/46/CE como a su objetivo, que consiste en mantener el equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad. En cambio, nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a la Directiva 95/46 a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de derecho comunitario se oponga a ello».

guar el nombre y el domicilio de los infractores, con vistas a ejercitar contra ellos las acciones legales pertinentes. O, como mínimo, quieren valerse de esas direcciones para ejercitar contra los proveedores de acceso acciones dirigidas a obtener la suspensión cautelar o definitiva de los servicios que prestan a los infractores.

De acuerdo con el art. 2.b) de esta Directiva, tanto la obtención por los titulares de derechos de las direcciones IP de los usuarios que intercambian obras o prestaciones protegidas a través de redes *peer to peer* (conectándose con ellos a través de la propia red) como su utilización por los proveedores de acceso para cumplir una orden judicial de suspensión del servicio proporcionado a su abonado infractor o de revelación de su identidad y la posterior comunicación del nombre y el domicilio del usuario a la autoridad judicial constituyen un tratamiento de datos personales a los efectos de la Directiva. Ese tratamiento está legitimado si cuenta con el consentimiento del usuario afectado, según dispone el art. 7.a) de esta Directiva. Pero, aun sin ese consentimiento (falta de consentimiento que será el supuesto normal), dicho tratamiento es lícito, conforme al art. 7.f), 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», siempre que no prevalezca el derecho a la protección de datos personales.

El citado art. 7.f) de la Directiva sobre Protección de Datos Personales pone sobre la mesa que en ocasiones el tratamiento no consentido de estos datos puede estar justificado por un interés legítimo preponderante del responsable del tratamiento o del tercero al que se le comunican los datos. En esa medida, obliga a realizar una ponderación de los derechos e intereses en conflicto. Lo que no nos dice ese artículo es quién ha de efectuar esa ponderación, ni cómo ha de hacerse, ni qué criterios deben utilizarse. Esa indeterminación no impide que sea un tribunal civil el que compare los intereses afectados y concluya, en su caso, que, a la vista de las circunstancias concurrentes, el derecho de protección de datos personales debe ceder ante un interés legítimo preferente de un tercero[17].

De forma similar, el art. 13.1.g) de la Directiva sobre Protección de Datos Personales faculta a los Estados miembros para limitar este derecho cuando sea necesario para salvaguardar la protección del interesado «o de los derechos y libertades de otra persona».

---

[17] En la misma línea, el art. 8.2.c) de la Directiva 95/46/CE, referido al tratamiento de categorías especiales de datos personales, que requieren una mayor protección, establece como excepción a la prohibición de tratar datos especialmente protegidos (art. 8.1) que el tratamiento «sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial». Los datos personales implicados en nuestro caso (direcciones IP, nombre y domicilio) no pertenecen a esa categoría de datos especiales a los que se aplica el art. 8. Pero este precepto tiene el interés de establecer como excepción al consentimiento para el tratamiento de los datos personales más necesitados de protección que éste sea preciso para la defensa de un derecho en un procedimiento judicial. Y tal excepción, además, no está limitada ni en atención al tipo de derecho de que se trate ni al procedimiento judicial en cuestión, por lo que bien podría ser un procedimiento civil. Si esto es así para los datos personales más sensibles, con más razón debe serlo para los demás datos.

En definitiva, de esta Directiva se desprende la posibilidad, o incluso la necesidad, de restringir el derecho de protección de datos personales cuando choque con los derechos de terceros, como son, en nuestro caso, los derechos de propiedad intelectual y el derecho a la tutela judicial efectiva. Por consiguiente, no exonera a los Estados miembros de la obligación, establecida por las Directivas 2000/31/CE, 2001/29/CE y 2004/48/CE, de establecer todas las medidas necesarias para asegurar la tutela de la propiedad intelectual en Internet, incluido el derecho de información previsto en el art. 8 DRDPI. Ahora bien, si en el caso concreto la protección de la propiedad intelectual requiere el tratamiento de datos personales de los supuestos infractores, deberán ponderarse los distintos intereses en conflicto, a la vista de las circunstancias concurrentes, para determinar si ese tratamiento es legítimo.

También resulta aplicable a nuestro caso la **Directiva 2002/58/CE sobre la Privacidad en las Comunicaciones Electrónicas**[18]. Esta Directiva no desplaza las disposiciones de la Directiva sobre Protección de Datos Personales que acabamos de estudiar, sino que las «especifica y completa» (cfr. art. 1.2)[19].

La relevancia de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas se basa en que para que los prestadores de servicios puedan cumplir órdenes judiciales en relación con infracciones cometidas a través de Internet, ya sean de revelación del nombre y el domicilio de quienes infringen derechos de propiedad intelectual a través de redes *peer to peer* o de suspensión del servicio que les prestan a éstos, es imprescindible tratar algunos datos de tráfico relativos a su conexión a Internet. En efecto, presupuesto para el cumplimiento de esas órdenes es determinar la identidad del presunto infractor. A tal fin son precisos el día y la hora en que se produjo la conexión mediante la cual se cometió la infracción, así como la dirección IP asignada por el proveedor de acceso para realizar esa conexión, que constituyen datos de tráfico, según el art. 2.b) de la Directiva 2002/58/CE[20]. Tratándose de datos de tráfico, es preciso determinar si su obtención por los titulares de derechos y su posterior tratamiento por los proveedores de acceso podría vulnerar los arts. 5 y 6 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas.

---

[18] Que derogó la Directiva 97/66/CE, de 15 de diciembre, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

[19] Lo corrobora el Considerando 10 de esta Directiva, que señala: «En el sector de las comunicaciones electrónicas es de aplicación la Directiva 95/46/CE, en particular para todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales que no están cubiertas de forma específica por las disposiciones de la presente Directiva, incluidas las obligaciones del responsable del tratamiento de los datos y los derechos de las personas. La Directiva 95/46/CE se aplica a los servicios de comunicaciones electrónicas que no sean de carácter público».

[20] De acuerdo con este artículo, cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma es un dato de tráfico. El Considerando 15 precisa que «los datos de tráfico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión».

El art. 5 garantiza la confidencialidad de las comunicaciones y de los datos de tráfico asociados a ellas, prohibiendo la escucha, la grabación, el almacenamiento o cualquier otro tipo de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios interesados, sin el consentimiento de éstos. Este precepto no impide la recopilación por parte de los titulares de derechos de los datos de tráfico relativos a las infracciones cometidas a través de redes *peer to peer* por dos razones. En primer lugar, porque se trata de una norma que rige las comunicaciones privadas (sólo las comunicaciones privadas son confidenciales), no los actos de comunicación pública, que son los que realizan los usuarios que ponen a disposición del público obras o prestaciones protegidas a través de redes *peer to peer*. En efecto, la fecha y hora de la conexión, así como la dirección IP asignada a estos usuarios, son datos de tráfico accesibles para todo aquel que se conecte a la misma red *peer to peer* mediante la cual se comunica el usuario infractor. En segundo lugar, aun cuando pudiera estimarse que el acto de comunicación[21] no es público, sino privado, ya que el intercambio de información no se produce mientras no se establece una conexión punto a punto entre el ordenador de quien pone a disposición un archivo y quien se lo descarga, no puede pasarse por alto que el art. 5. de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas garantiza la confidencialidad de las comunicaciones en relación con terceros, pero no, lógicamente, con respecto a los propios participantes en el acto de comunicación. Quiere esto decir que cualquiera de los intervinientes en una comunicación puede grabarla, de igual manera que puede registrar los datos de tráfico correspondientes, sin atentar contra la confidencialidad de la comunicación. Y eso es precisamente lo que hacen los titulares de derechos: se conectan a una red *peer to peer*, inician un acto de comunicación con un usuario infractor y registran los datos relacionados con ese acto de comunicación en el que han participado.

En cuanto al uso de los datos de tráfico por los prestadores de servicios, no es el art. 5 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas el que lo regula, sino su art. 6. Por tanto, es éste el que determina si puede instarse a uno de estos prestadores de servicios a tratar esos datos con vistas a identificar al infractor o suspender el servicio que le viene prestando.

Según se desprende del art. 6.1, los proveedores de acceso a Internet deben eliminar o hacer anónimos los datos de tráfico cuando ya no sean necesarios a efectos de la transmisión de una comunicación. Esta regla, que tiene excepciones establecidas en el propio artículo 6, ha sido superada para los datos que nos interesan por la Directiva sobre Conservación de Datos, que obliga a los proveedores de acceso a retenerlos un mínimo de seis meses y un máximo de dos años (arts. 3 y 6 de la Directiva sobre Conservación de Datos).

[21] No me refiero al acto de comunicación pública (puesta a disposición) de la obra o prestación protegida, con relevancia desde el punto de vista de la propiedad intelectual, sino a la conexión entre el ordenador que contiene el archivo en su carpeta compartida y el ordenador del usuario que pretende descargárselo.

Los datos así conservados sólo pueden ser tratados por los proveedores de acceso a efectos de facturación y pago de las interconexiones (art. 6.2 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas), así como para la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios con valor añadido, siempre que medie el consentimiento del usuario (art. 6.3). Esos datos podrán ser igualmente tratados por los proveedores de acceso a fin de colaborar con las autoridades competentes en la detección, investigación y enjuiciamiento de delitos graves, conforme a la Directiva sobre Conservación de Datos, como luego veremos. Finalmente, pueden ser comunicados a los organismos competentes con vistas a la resolución de litigios, en particular los relativos a la interconexión o la facturación (art. 6.6 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas)[22].

Dados los términos taxativos del art. 6, bien podría interpretarse en el sentido de que prohíbe a los proveedores de acceso todo tratamiento de datos para cuya realización no estuviera habilitado por esta u otra Directiva. Esta interpretación, que a mí me parece adecuada, conduce a plantearnos si las Directivas sobre propiedad intelectual (incluyendo entre éstas, por razones de afinidad, la Directiva sobre Comercio Electrónico) pueden contener semejante habilitación. Cuestión ésta sumamente complicada, pues, como hemos visto, tanto la DCE como la DDASI y la DRDPI se aplican sin perjuicio de las normas sobre protección de datos. La respuesta a este interrogante dependerá, entonces, de la relación que exista entre las Directivas sobre protección de datos y las Directivas sobre propiedad intelectual, que se analizará en el próximo epígrafe.

La última apreciación que ha de hacerse sobre la Directiva sobre la Privacidad y las Comunicaciones Electrónicas es que su artículo 15.1 legitima a los Estados miembros para limitar el alcance de los derechos y obligaciones establecidos por los arts. 5 y 6 «cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas[23] a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE».

---

[22] Este art. 6.6 ha sido interpretado por el TJCE en el sentido de que los proveedores de acceso pueden comunicar datos de tráfico a los organismos competentes (normalmente tribunales civiles) para resolver litigios entre proveedores y usuarios sobre interconexión o facturación, pero no a entidades de gestión o asociaciones de defensa profesional o empresarial que pretenden entablar un litigio sobre propiedad intelectual (cfr. Sentencia de 29 de enero de 2008, *Promusicae*, asunto C-275/06, parágrafo 48).

[23] El TJCE declaró en la sentencia del asunto *Promusicae* que esta excepción parece referirse a las utilizaciones que ponen en peligro la integridad o la seguridad del sistema, como ocurre en los casos de intervención o vigilancia de las comunicaciones sin el consentimiento de los usuarios interesados, y no, como alegaron a lo largo del procedimiento *Promusicae* y el Reino Unido, al uso del sistema para cometer ilícitos civiles, por mucho que en el contrato de prestación del servicio de acceso se haya previsto como causa de resolución del mismo la comisión de ilícitos civiles valiéndose del servicio prestado (cfr. parágrafo 53).

La mención del art. 13.1 de la Directiva sobre Protección de Datos Personales ha servido al TJCE para entender que los Estados miembros pueden limitar el alcance de los arts. 5 y 6 cuando sea necesario para la protección de los derechos y libertades de otra persona, conforme dispone el art. 13.1.g)[24].

La tercera Directiva sobre protección de datos relevante es la **Directiva 2006/24/CE de Conservación de Datos**. Esta Directiva establece la obligación de los proveedores de servicios de comunicaciones electrónicas de acceso público de conservar los datos de tráfico generados en el marco de una comunicación electrónica, para su eventual uso en la investigación, detección y enjuiciamiento de delitos graves (art. 1.1).

A raíz de la aprobación de esta Directiva, podría entenderse que en la actualidad sólo es posible retener los datos de tráfico con vistas a su utilización en el ámbito de un procedimiento penal seguido por la comisión de delitos graves. Si así fuera, los tribunales civiles no estarían legitimados para requerir la comunicación de dichos datos para su uso en un procedimiento de carácter civil. Tampoco las autoridades competentes para la investigación, detección y enjuiciamiento de delitos si éstos no fueran graves. Ello implicaría, de facto, crear un ámbito de impunidad en relación con aquellos actos ilícitos realizados a través de Internet que no estuvieran tipificados como delitos graves.

Una lectura atenta de la Directiva, sin embargo, demuestra que no pretende crear ningún ámbito de impunidad, como no podía ser de otra manera. De entrada, tal y como se desprende del art. 3.1, esta Directiva se configura como una excepción a los arts. 5, 6 y 9 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, pero no a los arts. 18 DCE, 8 DDASI ni 8 DRDPI. Por consiguiente, la Directiva sobre Conservación de Datos no constituye un límite ni al derecho de información de los titulares de derechos de propiedad intelectual ni al derecho a la tutela judicial efectiva, que encuentran su plasmación, en cuanto a las infracciones de propiedad intelectual cometidas a través de Internet, en estos artículos.

Por otra parte, es claro que el art. 3.1 obliga a los prestadores de servicios de comunicaciones electrónicas a conservar los datos de tráfico y localización, así como otros datos relacionados necesarios para identificar al destinatario del servicio, para garantizar su disponibilidad con vistas a la detección, investigación y enjuiciamiento de delitos graves. Pero de ahí no se desprende que dichos datos sólo puedan ser utilizados en ese ámbito. Esos datos, como hemos visto anteriormente, pueden ser usados sin el consentimiento de sus titulares a efectos de la facturación de los abonados y los pagos de las interconexiones (art. 6.2 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas). Pueden ser comunicados a los organismos competentes (incluidos los tribunales civiles) con vistas a la resolución de litigios (art. 6.6 de la Directiva

[24] Vid. Sentencia de 29 de enero de 2008, *Promusicae*, asunto C-275/06.

2002/58/CE)[25]. Y pueden también ser utilizados a otros efectos legalmente establecidos, tal y como parece deducirse del Considerando 25 de la Directiva sobre Conservación de Datos, que faculta a los Estados miembros «para adoptar medidas legislativas relativas al derecho de acceso y de utilización de los datos por parte de las autoridades nacionales tal como determinen los mismos».

De este Considerando 25 se colige, en efecto, que el objeto de la Directiva es única y exclusivamente establecer la obligación de retención de datos de tráfico, de modo que se garantice su disponibilidad para la investigación, detección y enjuiciamiento de delitos graves. Pero no constituye el objeto de la Directiva regular el acceso de las autoridades nacionales a los datos conservados ni el uso que puedan hacer de ellos[26]. En este sentido, y siempre que se respete el contenido esencial del derecho a la intimidad, tal y como deriva del art. 8 de la Convención Europea de Derechos Humanos y de la interpretación que del mismo ha hecho el Tribunal Europeo de Derechos Humanos, los Estados miembros pueden facultar a las autoridades competentes (incluidos los tribunales civiles) para que ordenen la entrega de esos datos con vistas a la detección, investigación o enjuiciamiento de delitos que no sean graves, e incluso para la averiguación de la identidad de quien supuestamente ha realizado un ilícito civil a través de Internet[27].

Ello explica que ningún artículo de la Directiva sobre Conservación de Datos limite la utilización de los datos retenidos al ámbito de un procedimiento pe-

---

[25] Es evidente, por la propia naturaleza de la Directiva sobre Conservación de Datos, que supone una excepción a la obligación de eliminar o hacer anónimos los datos de tráfico cuando no sean ya necesarios para la transmisión de la comunicación, la facturación del abonado o el pago de las interconexiones, pero no a la posibilidad de tratar los datos con esos fines, o de comunicar esos datos a la autoridad competente para la resolución de litigios.

[26] De hecho, al tratamiento de los datos conservados le es aplicable lo dispuesto por la Directiva sobre Protección de Datos Personales y la Directiva sobre la Privacidad y las Comunicaciones Electrónicas. Así se desprende del Considerando 15 de la Directiva sobre Conservación de Datos, de acuerdo con el cual «la Directiva 95/46/CE y la Directiva 2002/58/CE son plenamente aplicables a los datos conservados de conformidad con la presente Directiva».

[27] La historia legislativa de la Directiva sobre Conservación de Datos avala esta interpretación. La Propuesta de Directiva de la Comisión de 21 de septiembre de 2005 —Documento COM(2005) 438 final— era muy clara a la hora de restringir a los procedimientos penales por delitos graves el uso de los datos que obligaba a conservar. Su art. 3.2 establecía: «Los Estados miembros adoptarán medidas para garantizar que los datos conservados de conformidad con esta Directiva solamente se proporcionen a las autoridades nacionales competentes y, en casos específicos, de conformidad con la legislación nacional, con fines de prevención, investigación, detección y enjuiciamiento de delitos graves, como el terrorismo y la delincuencia organizada». En consonancia con ello, en la Propuesta de Directiva no existía ni el actual Considerando 25 ni el actual artículo 4. Pues bien, el texto definitivo de la Directiva procede de la negociación entre el Parlamento y el Consejo, que dio como resultado la introducción de cambios muy importantes en la Propuesta de la Comisión. Entre esos cambios se encontraba el añadido del Considerando 25 y la sustitución del art. 3.2 por un nuevo art. 4. Esos cambios, como hemos visto, iban dirigidos a dar libertad a los Estados miembros en cuanto a la regulación de la puesta a disposición de las autoridades nacionales competentes de los datos retenidos. En concreto, los datos ya no se proporcionarán a las autoridades nacionales competentes con fines de prevención, investigación, detección y enjuiciamiento de delitos graves, como el terrorismo y la delincuencia organizada, sino que simplemente se proporcionarán a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional.

nal por delitos graves. Si nos fijamos bien en el artículo 1.1, el único que podría parecer que restringe el uso de los datos, podemos apreciar que simplemente establece que el objeto de la Directiva es la obligación de retener datos relativos a las comunicaciones electrónicas «*para garantizar* que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves». Por tanto, si se asegura que esos datos están disponibles a tales efectos, se está cumpliendo el objeto de la Directiva, sin perjuicio de que esos datos puedan destinarse también a otros fines legalmente permitidos. Sólo una interpretación *a contrario*, siempre endeble[28] y lesiva del derecho a la tutela judicial efectiva[29], permitiría entender que la Directiva sobre Conservación de Datos restringe el uso de los datos de tráfico al ámbito penal y únicamente en relación con delitos graves[30].

4. La relación entre las Directivas sobre comercio electrónico y propiedad intelectual y las Directivas sobre protección de datos

De la lectura de las Directivas sobre comercio electrónico y propiedad intelectual, por un lado, y las Directivas sobre protección de datos, por otro, no se desprende la prevalencia de ninguna de ellas, sino la necesidad de integrar las disposiciones de unas y otras. Y ello de tal modo que se garantice un adecuado equilibrio entre la necesaria tutela de los derechos de propiedad intelectual y la igualmente deseable salvaguardia de los datos personales de los usuarios de Internet, tal y como exige el TJCE en su sentencia de 29 de enero de 2008, *Promusicae*, asunto C-275/06.

Es cierto que, como hemos visto con anterioridad, la DCE no se aplicará a cuestiones relacionadas con servicios de la sociedad de la información incluidas en la Directiva sobre Protección de Datos y la Directiva sobre la Privacidad y las Comunicaciones Electrónicas —art. 1.5.b) DCE—, y que tanto el art. 8 DDASI como el art. 8 DRDPI se aplicarán sin perjuicio de las disposiciones relativas a la protección de datos —arts. 9 DDASI y 8.3.e) DRDPI—. Sin embargo, ello no implica ninguna prioridad a favor de las normas sobre protección de datos.

---

[28] Que se indique que la finalidad de la Directiva es garantizar que los datos de tráfico estén disponibles para la investigación, detección y enjuiciamiento de delitos graves no significa, sin más, que los datos retenidos no puedan destinarse a otros usos legalmente previstos.

[29] De acuerdo con el Considerando 22, la Directiva sobre Conservación de Datos respeta los derechos fundamentales y observa los principios reconocidos por la Carta de Derechos Fundamentales. Por tanto, no puede interpretarse de forma tal que conlleve la ineficacia de los derechos de propiedad intelectual y tutela judicial efectiva de terceros.

[30] En línea con lo anterior, el art. 4 de la Directiva sobre Conservación de Datos establece que los datos conservados sólo podrán comunicarse a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional. Obsérvese que no dice que esas autoridades competentes tengan que estar dedicadas a la investigación, detección o enjuiciamiento de delitos graves. Tampoco dice que los casos específicos en los que podrá comunicarse esos datos a la autoridad competente sólo sean los que tienen relevancia penal. Por consiguiente, nada impide que entre esas autoridades nacionales competentes se incluyan los tribunales civiles, ni que entre los casos específicos en que pueden proporcionárseles esos datos se incluyan los procedimientos civiles por infracción de derechos de propiedad intelectual.

Comenzando por la DCE, y aunque el tenor literal del art. 1.5.b) parece claro y tajante en el sentido de que esta Directiva no afecta en nada a lo dispuesto por las Directivas sobre protección de datos, mencionando expresamente a la antecesora de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, no puede pasarse por alto la imposibilidad de interpretar aquel precepto de modo tal que conduzca a la total ineficacia de alguna disposición imperativa de la propia DCE. Semejante interpretación iría en contra de la doctrina del TJCE según la cual se ha de garantizar la plena efectividad de todas las disposiciones comunitarias (vid. Sentencia de 13 de septiembre de 2005, *Comisión v. Consejo*, asunto C-176/03). Pues bien, el artículo 18.1 DCE obliga a los Estados Miembros a garantizar que se puedan adoptar rápidamente medidas de cesación ante presuntas infracciones cometidas a través de Internet (en el mismo sentido, vid. Considerandos 52 y 54 DCE). Sólo pueden adoptarse estas medidas si se conoce, al menos por el prestador de servicios, la identidad del infractor, lo que obliga a establecer medios para averiguar esa identidad. Teniendo en cuenta que cualquier medio de averiguación de la identidad del infractor conlleva un tratamiento de sus datos personales, la interpretación literal de ese art. 1.5.b) dejaría vacío de contenido el art. 18.1[31].

Por su parte, la DDASI y la DRDPI no son tan taxativas como la DCE excluyendo su aplicación a cuestiones relacionadas con la protección de datos. Se limitan a establecer que se aplicarán «sin perjuicio» de las disposiciones sobre protección de datos.

La expresión «sin perjuicio de» no establece necesariamente una relación jerárquica entre la DDASI o el derecho de información de la DRDPI y las Directivas sobre protección de datos. De hecho, el significado de esa expresión dista de ser claro. Así lo han reconocido las instituciones comunitarias en la Guía Práctica Común del Parlamento Europeo, del Consejo y de la Comisión, dirigida a las personas que contribuyen a la redacción de los textos legislativos en las instituciones comunitarias, hecha en 2003[32]. En la Regla 16.9 de dicha Guía se alerta a los redactores de textos legislativos de la poca claridad de la expresión «sin perjuicio de», porque pueden existir contradicciones entre el acto al que se hace referencia y el acto al que se remite[33].

---

[31] Otro ejemplo de que no cabe dicha interpretación lo encontramos en el art. 15.2 DCE. Este artículo, como hemos visto, permite a los Estados miembros establecer la obligación de los prestadores de servicios de la sociedad de la información de comunicar a las autoridades competentes, a solicitud de éstas, información que les permita identificar a los destinatarios de su servicio. Esta norma requiere en todo caso un tratamiento de datos personales distinto de los previstos en las Directivas sobre Protección de Datos. Por tanto, si interpretamos literalmente el art. 1.5.b), si entendemos que la Directiva sobre Comercio Electrónico no puede abordar cuestiones relativas a la protección de datos, ese segundo inciso del artículo 15.2 no se aplicaría nunca, resultando absolutamente inútil. El hecho de que se trate de una norma facultativa no cambia las cosas. Aunque no sea de incorporación obligatoria, debe al menos poderse incorporar. Si no, no tendría ningún valor.

[32] Disponible en http://eur-lex.europa.eu/es/techleg/pdf/es.pdf.

[33] Señala esta Regla: «Las consecuencias de las referencias introducidas por la fórmula «sin perjuicio» con frecuencia distan mucho de ser claras. En particular, pueden existir contradicciones entre el acto en el que se hace la referencia y el acto al que se remite. En general, se podrá prescindir de tales referencias delimitando mejor el ámbito de aplicación. Además, es superfluo remitir mediante esta fórmula a disposiciones de rango superior que son de aplicación».

En este contexto, no parece razonable hacer una interpretación radical de esta expresión, que conduzca a imposibilitar el ejercicio de acciones para la protección de la propiedad intelectual en Internet en contra de lo dispuesto por el art. 8 DDASI, o a dejar sin efecto el derecho de información de los titulares de derechos frente a quienes prestan a escala comercial los servicios de los que se vale el infractor para cometer la infracción —art. 8.1.c) DRDPI—. No se olvide, en este sentido, que, como hemos señalado con anterioridad, es un principio interpretativo básico que las normas jurídicas, y por tanto también las disposiciones comunitarias, deben ser interpretadas de forma tal que se garantice su eficacia.

Así las cosas, la fórmula «sin perjuicio de las disposiciones que rijan el tratamiento de los datos personales» debe ser interpretada en el sentido de que ni las disposiciones de la DDASI ni el derecho de información reconocido por el art. 8 DRDPI tienen carácter absoluto[34]. Significa que debe buscarse un punto de equilibrio entre la tutela judicial de la propiedad intelectual y el derecho a la protección de datos personales, tal y como sugiere la Sentencia del TJCE de 29 de enero de 2008, *Promusicae*, asunto C-275/06, a la que posteriormente me referiré. Así se desprende de los arts. 7.f) y 13.1.g) de la Directiva sobre Protección de Datos Personales. Ese punto de equilibrio se alcanza limitando el tratamiento de datos no consentido a aquellos casos en los que sea imprescindible para la defensa de la propiedad intelectual; restringiendo el deber de los prestadores de servicios de revelar la identidad de los usuarios a aquellos supuestos en los que se presenten indicios suficientes de que se ha producido una infracción y se justifique que no existe otra forma de averiguar la identidad del infractor; exigiendo que sea un tribunal, que perfectamente puede ser civil, el que decida, a la vista del caso concreto, si los datos personales de los supuestos infractores deben ser revelados al titular de los derechos infringidos; imponiendo que los datos que en su caso se pongan a disposición del tribunal sean utilizados únicamente para la defensa de los derechos infringidos…

Centrándonos ya en el derecho a la información del art. 8 DRDPI, y su relación con las Directivas sobre protección de datos, hemos de tener en cuenta, de entrada, que, como hemos visto con anterioridad, la Directiva sobre Protección de Datos Personales asume que este derecho ha de ceder ante intereses legítimos preponderantes —arts. 7 f) y 13.1—. También que la Directiva de Conservación de Datos se limita a garantizar que los datos relativos a una comunicación electrónica estén disponibles para su utilización con fines de detección, investigación y enjuiciamiento de delitos graves, pero no impide que los datos así retenidos se utilicen para otros fines legítimos. Por tanto, es la Directiva sobre la Privacidad y las Comunicaciones Electrónicas la que puede dificultar el tratamiento de datos por los prestadores de servicios con vistas a identificar a los destinatarios de sus servicios que se valen de ellos para in-

[34] En este sentido se manifestó el Reino Unido en su escrito de alegaciones en la cuestión prejudicial seguida ante el TJCE en el asunto *Promusicae*, parágrafos 41 y 42.

fringir la propiedad intelectual. Pues bien, en mi opinión esta Directiva no prevalece sobre la DRDPI[35].

La falta de prioridad de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas sobre el derecho de información de la DRDPI me parece manifiesta[36], aun cuando el TJCE no lo ha visto así en la sentencia del caso *Promusicae*. La DRDPI, al regular el derecho de información de los titulares de derechos de propiedad intelectual, establece que los apartados 1 y 2 de su art. 8 «se aplicarán sin perjuicio de otras disposiciones legales que rijan la protección de la confidencialidad de las fuentes de información o el tratamiento de datos personales». Así lo establece el art. 8.3.e) DRDPI. Para determinar a qué disposiciones legales relativas al tratamiento de datos personales se refiere, debemos acudir a su artículo 2.3. Éste establece que la DRDPI «no afectará a las disposiciones comunitarias que regulan el Derecho sustantivo de propiedad intelectual, la Directiva 95/46/CE, la Directiva 1999/93/CE y la Directiva 2000/31/CE, en general, y los arts. 12 a 15 de esta última en particular», como ya se anticipaba en su Considerando 15. Obsérvese que tanto en el art. 2.3 como en el Considerando 15 se menciona expresamente la Directiva 95/46/CE, sobre Protección de Datos Personales, pero no la Directiva sobre la Privacidad y las Comunicaciones Electrónicas. Esta omisión, como veremos a continuación, es deliberada. Ello significa que los apartados 1 y 2 del art. 8 DRDPI se aplicarán sin perjuicio de las disposiciones de la Directiva 95/46/CE, sobre Protección de Datos Personales, pero no de las disposiciones de la Directiva 2002/58/CE, sobre la Privacidad y las Comunicaciones Electrónicas.

Se ha intentado salvar este escollo afirmando que la Directiva sobre la Privacidad y las Comunicaciones Electrónicas en realidad simplemente viene a traducir en normas concretas para el sector de las telecomunicaciones los principios establecidos por la Directiva sobre Protección de Datos Personales, razón por la cual la mención de ésta en el Considerando 15 y en el art. 2.3 DRDPI incluiría tácitamente aquélla[37]. Este argumento, sin embargo, se compadece mal con la his-

---

[35] De hecho, tal y como establece su Considerando 2, la Directiva sobre la Privacidad y las Comunicaciones Electrónicas pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados en la Carta de los Derechos Fundamentales. La propiedad intelectual y la tutela judicial efectiva son derechos fundamentales en el ámbito del Derecho comunitario, como la intimidad y la protección de datos personales. Es un principio de la Carta de Derechos Fundamentales que la protección de un derecho fundamental termina donde empieza la de otro derecho distinto. Por tanto, la Directiva sobre la Privacidad y las Comunicaciones Electrónicas no pretende situar el derecho de protección de datos por encima de los derechos de propiedad intelectual y tutela judicial efectiva, sino que trata de alcanzar un punto de equilibrio entre aquel derecho y éstos.

[36] Es más, la expresión «sin perjuicio de las disposiciones que rijan el tratamiento de datos personales» que utiliza el art. 8.3.e) DRDPI produce una paradoja, y es que el art. 7.c) permite el tratamiento no consentido de datos personales para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento. Pues bien, el art. 8.1.c) DRDPI obliga a los proveedores de acceso a escala comercial a revelar en procedimientos civiles o administrativos la identidad de quienes se valen de sus servicios para infringir derechos de propiedad intelectual. Ello nos conduce a un círculo vicioso, donde la DRDPI establece una obligación jurídica sin perjuicio de las normas sobre protección de datos personales, y la Directiva sobre la Protección de los Datos Personales permite un tratamiento cuando es imprescindible para cumplir una obligación jurídica.

[37] Vid. alegaciones de la Comisión en la cuestión prejudicial del asunto *Promusicae*, parágrafo 40.

toria legislativa del art. 8 DRDPI. La tramitación de la DRDPI demuestra que el legislador comunitario quiso que el derecho de información no tuviera más límites relacionados con la protección de datos que los derivados de la Directiva sobre de Protección de Datos Personales. Así, durante los trabajos preparatorios llevados a cabo en el Consejo, Alemania y Austria propusieron que se incluyera en el art. 2.3 DRDPI la legislación comunitaria más reciente en materia de protección de datos, en clara referencia a la Directiva sobre la Privacidad y las Comunicaciones Electrónicas aprobada el año anterior[38]. Esta propuesta, sin embargo, fue rechazada por el Consejo, lo que demuestra la voluntad del legislador de no supeditar el derecho de información establecido por el art. 8 DRDPI a la Directiva sobre la Privacidad y las Comunicaciones Electrónicas.

Pero no sólo eso. Si comparamos la DRDPI con la DCE, podemos comprobar que si el legislador comunitario hubiera querido dejar a salvo la Directiva sobre la Privacidad y las Comunicaciones Electrónicas al regular el derecho de información del art. 8 DRDPI, la habría mencionado expresamente. Así lo hace el art. 1.5.b) DCE, igual que su Considerando 14, al establecer que dicha Directiva «no se aplicará (…) a cuestiones relacionadas con servicios de la sociedad de la información incluidas en las Directivas 95/46/CE y 97/66/CE»[39].

Además, es innegable que la DRDPI pretendía, entre otras cosas, ayudar a reducir la piratería en Internet, tal y como se desprende de su Considerando 10. Pues bien, difícilmente podría alcanzarse esa meta si la Directiva sobre la Privacidad y las Comunicaciones Electrónicas limitara el derecho de información hasta el punto de hacerlo inexistente en la red.

Finalmente, incluso si se considerara que la referencia que se hace a la Directiva sobre Protección de Datos Personales en el art. 2.3 DRDPI comprende también la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, y que ésta prima sobre aquélla, ello no querría decir que el derecho de información esté limitado por los arts. 5 y 6 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas. El art. 8.3.e) DRDPI establece que los apartados 1 y 2 del art. 8 se aplicarán sin perjuicio de las disposiciones legales que rijan «el tratamiento de datos *personales*». Los arts. 5 y 6 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, que son los que les sirven a los prestadores de servicios para justificar su negativa a revelar la identidad de los usuarios infractores, se refieren a datos de tráfico, y no a datos personales. Por lo tanto, esos dos artículos no limitan, conforme al art. 8.3.e) DRDPI, el derecho de información de los titulares de derechos de propiedad intelectual. Fortalece esta interpretación el hecho de que, a diferencia de lo concreto que es el art. 8.3.e) DRDPI, que alude específicamente al «tratamiento de datos personales», el art. 9 DDASI es mucho más amplio, ya que deja a sal-

[38] Vid. Documento del Consejo núm. 11107/03, de 3 de julio.

[39] La Directiva 97/66/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, es la predecesora de la Directiva del año 2002 sobre Privacidad y Comunicaciones Electrónicas, como es sabido.

vo las disposiciones relativas a (literalmente) «la protección de datos». Mientras que el primero se refiere únicamente a los datos personales, el segundo atañe a todos los datos que el ordenamiento comunitario proteja, lo que incluye también los datos de tráfico y de localización.

Si cabe defender, conforme a lo que acabamos de exponer, que el derecho de información del art. 8 DRDPI no está limitado por la Directiva sobre la Privacidad y las Comunicaciones Electrónicas o, al menos, que no lo está por las disposiciones de ésta que rigen los datos de tráfico, no se puede negar que sí lo está por la Directiva sobre Protección de Datos Personales de 1995. Esta Directiva se aplica incluso por lo que se refiere al ejercicio del derecho de información en relación con infracciones cometidas a través de Internet. Así es como debe interpretarse no sólo el art. 8.3.e) DRDPI, sino también su Considerando 2, de acuerdo con el cual la DRDPI «no debe ser un obstáculo (...) para la protección de los datos personales, inclusive en Internet»[40], en relación con el Considerando 10 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, que comienza «en el sector de las comunicaciones electrónicas es de aplicación la Directiva 95/46/CE...»[41].

Pues bien, ningún precepto de la Directiva sobre Protección de Datos Personales impide que los datos personales de un infractor puedan ser revelados sin su consentimiento en el marco de un procedimiento civil. Es más, del art. 7.f) se desprende que los datos pueden ser tratados (también cedidos, por lo tanto) sin consentimiento de su titular cuando lo exija la satisfacción de un interés legítimo prevalente, como es el derecho a la tutela judicial de la propiedad intelectual, y del art. 13.1.g), que los Estados miembros tienen la facultad de restringir el derecho de protección de datos personales cuando ello sea necesario para la tutela de los derechos y libertades de otra persona.

5. La Carta de los Derechos Fundamentales de la Unión Europea

La Carta de los Derechos Fundamentales de la Unión Europea reconoce en su art. 8 el derecho a la protección de datos de carácter personal. De acuerdo con este artículo «toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para

[40] Obsérvese que vuelve a referirse a la protección de datos personales, no de otros datos, como los datos de tráfico.

[41] No se olvide, por otro lado, que la Directiva sobre Protección de Datos Personales no es una Directiva de mínimos, sino que establece un nivel de protección uniforme, dentro del cual deja un muy escaso margen de maniobra a los Estados miembros (vid. art. 5 en relación con los Considerandos 8 y 9). Ese nivel de protección es el mismo con independencia de las técnicas de tratamiento utilizadas, como se desprende del principio de neutralidad tecnológica consagrado en el Considerando 27 de esta Directiva. Por tanto, el nivel de protección de los datos personales en Internet debe ser el mismo que en otros ámbitos, lo que permite la aplicación de los principios generales de legitimación para el tratamiento del art. 7 de la Directiva sobre Protección de Datos Personales.

fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley».

Pero el derecho a la protección de datos personales no es un derecho absoluto[42]. Ningún derecho fundamental lo es. Así se desprende del art. 52.1 de la propia Carta de los Derechos Fundamentales de la Unión Europea, que establece: «Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión *o a la necesidad de protección de los derechos y libertades de los demás*». También del art. 54, según el cual ninguna de las disposiciones de la Carta podrá interpretarse en un sentido que implique un derecho cualquiera a dedicarse a una actividad o a realizar un acto tendente a la destrucción de los derechos o libertades reconocidos en la Carta o a limitaciones más amplias de estos derechos y libertades que las establecidas en la misma[43].

El art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea, en relación con el art. 52.1 de la misma, permite, por tanto, el tratamiento no consentido de datos personales siempre que exista un fundamento legítimo previsto por la Ley. Ese fundamento legítimo puede ser la protección de los derechos de terceros. Y en nuestro caso, son dos derechos fundamentales distintos los que se ven afectados. En primer lugar, el derecho de propiedad. El art. 17 de la Carta reconoce entre los derechos fundamentales de toda persona, en efecto, el derecho a la propiedad. A continuación, en su apartado 2, establece que «se protegerá la propiedad intelectual». Luego la propiedad intelectual es un derecho fundamental según la Carta de Derechos Fundamentales de la Unión Europea. En segundo lugar, el derecho a la tutela judicial efectiva, reconocido por el art. 47 de la Carta, de conformidad con el cual «toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela efectiva respetando las condiciones establecidas en el presente artículo». El derecho a la tutela judicial efectiva asiste a los ciudadanos de la Unión Europea en todos los órdenes jurisdiccionales, incluido el civil[44]. Por consiguiente, los ciudadanos de la Unión Europea deben estar en condiciones de acudir a los tribunales para defender sus legítimos intereses, y deben tener derecho a que estos tribunales adopten todas las medidas necesarias para satisfacer sus legítimas pretensiones.

---

[42] Vid. la sentencia del TJCE de 6 de noviembre de 2003, *Lindqvist*, asunto C-101/01.

[43] En este sentido, vid. sentencias del TJCE de 6 de marzo de 2001, *Conolly v. Comisión,* asunto C-274/99; de 12 de junio de 2003, *Schmidberger v. Austria,* asunto C-112/00; de 25 de marzo de 2004, *Karner*, asunto C-71/02.

[44] En efecto, tal y como ha señalado el Tribunal Europeo de los Derechos Humanos, el derecho a la tutela judicial efectiva comprende el derecho a acceder a un tribunal para que resuelva sobre cuestiones de índole civil (vid., por todas, la sentencia de 12 de julio de 2005 [final 30 de noviembre de 2005], *Moldavan v. Rumanía* [41138/98 y 64320/01, apartado 118]).

Ante la colisión del derecho de protección de datos personales con la propiedad intelectual y la tutela judicial efectiva, incumbe a los tribunales, a la vista de las circunstancias del caso, garantizar un justo equilibrio entre los derechos en conflicto. En este sentido se ha pronunciado el Tribunal de Justicia de las Comunidades Europeas en su sentencia de 6 de noviembre de 2003, *Lindqvist*, asunto, C-101/01, apartado 90[45]. Tal y como expuso el TJCE en la sentencia de 14 de septiembre de 2000, *Fisher*, asunto C-369/98, es necesario realizar una adecuada ponderación de los intereses en conflicto para alcanzar una solución proporcionada, equilibrada, que asegure la mayor protección posible de todos los derechos involucrados.

Negar a una persona la posibilidad de demandar a quien ha infringido sus derechos, por no permitirle solicitar a la autoridad judicial competente la adopción de medidas encaminadas a averiguar la identidad del infractor, o la posibilidad de obtener una medida de cesación, por no autorizar al proveedor de acceso a tratar los datos del infractor con vistas a suspender, de conformidad con lo dispuesto por una resolución judicial, el servicio prestado al infractor, es privar a esa persona de su derecho a la tutela judicial efectiva y generarle indefensión. Esa solución del conflicto conlleva un evidente desequilibrio a favor de la protección de los datos personales del infractor a costa de la propiedad intelectual y la tutela judicial efectiva de la víctima. Implica generar un ámbito de impunidad en Internet carente de toda justificación.

En mi opinión, el adecuado equilibrio entre los derechos en conflicto se garantiza con una previsión legal en el sentido de que no hará falta el consentimiento del afectado para el tratamiento de sus datos personales cuando prime el interés legítimo de un tercero, como hace el art. 7.f) de la Directiva sobre Protección de Datos Personales, y dejando a los tribunales, sean del orden jurisdiccional que sean, la ponderación de los derechos en cuestión para determinar, a la vista de las circunstancias concurrentes, cuál ha de primar. Ello es conforme con el art. 8.2 del Convenio Europeo para la Protección de los Derechos Humanos, según es interpretado por el Tribunal de Estrasburgo, de acuerdo con el cual no podrá haber injerencia de la autoridad pública en el derecho a la vida privada (donde se entiende subsumido el derecho a la protección de datos personales) «sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

---

[45] Señala el TJCE: «Las disposiciones de la Directiva 95/46/CE no entrañan, por sí mismas, una restricción contraria al principio general de la libertad de expresión o a otros derechos y libertades vigentes en la Unión Europea y que tienen su equivalente, entre otros, en el artículo 10 CEDH. Incumbe a las autoridades y a los órganos jurisdiccionales nacionales encargados de aplicar la normativa nacional que adapta el Derecho interno a la Directiva 95/46 garantizar el justo equilibrio entre los derechos e intereses en juego, incluidos los derechos fundamentales tutelados por el ordenamiento jurídico comunitario».

Como hemos venido diciendo, los arts. 18.1 DCE, 8 DDASI y 8 DRDPI permiten a los tribunales civiles realizar la injerencia en la esfera privada de una persona que ha infringido derechos de terceros a través de Internet, consistente en tratar sus datos con vistas a identificarlo o, cuando menos, a suspender el servicio del que se vale para cometer la infracción. Dicha injerencia es necesaria para asegurar la protección de los derechos vulnerados y para garantizar al perjudicado una tutela judicial efectiva. Se trata de una medida proporcionada y pertinente, pues sólo se admitirá cuando existan indicios suficientes de ilicitud en la conducta de aquel cuyos datos han de tratarse, y adoptándose las cautelas necesarias para que esos datos se utilicen únicamente para la protección de la propiedad intelectual de terceros[46].

6. La sentencia del Tribunal de Justicia de las Comunidades Europeas de 29 de enero de 2008

El TJCE ha tenido ocasión de pronunciarse sobre el conflicto entre el derecho a la protección de datos y el derecho a la propiedad intelectual que aquí nos planteamos, en la resolución de una cuestión prejudicial planteada por el Juzgado de lo Mercantil núm. 5 de Madrid en el marco de un procedimiento de diligencias preliminares seguido por *Promusicae* contra *Telefónica* para la averiguación de la identidad de usuarios de Internet que infringían derechos de propiedad intelectual de los productores fonográficos a través de una red *peer to peer*[47].

La solicitud de diligencias preliminares se planteó antes de la incorporación al Derecho español del derecho de información del art. 8 DRDPI. La ausencia entonces de un supuesto específico de diligencias preliminares en materia de propiedad intelectual motivó que la solicitud se fundara en el art. 24 de la Ley de Competencia Desleal (sobre la base de que la conducta de los usuarios infractores podía constituir un acto de competencia desleal) y en el art. 12 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), hoy derogado, en relación con las Directivas comunitarias en materia de propiedad intelectual[48].

---

[46] Por otra parte, la circunstancia de que la propiedad intelectual, como toda propiedad, deba cumplir una función social no es un obstáculo para la solución del conflicto de derechos que entiendo mejor. La función social de la propiedad no implica que necesariamente deba ceder siempre ante el derecho a la protección de datos personales de los posibles infractores. La jurisprudencia del TJCE está plagada de ejemplos en los que se reconoce que la propiedad puede primar sobre otros derechos fundamentales, pese a su función social. De hecho, tal y como se resalta en la sentencia de 12 de mayo de 2005, *ERSA v. Ministerio de la Política Agrícola y Forestal,* asunto C-347/03, las limitaciones del derecho de propiedad basadas en su función social no pueden suponer una injerencia tan desproporcionada e intolerable que prive a la propiedad de su propia sustancia. La aplicación de esta doctrina a la propiedad intelectual ha llevado al TJCE a declarar, por ejemplo, que la propiedad intelectual puede constituir un límite a un derecho fundamental tan importante en un estado democrático como es la libertad de expresión (sentencia de 12 de septiembre de 2006, *Laserdisken*, asunto C-479/04).

[47] Para un comentario de la sentencia, *vid.* Kuner, C., «Data Protection and Rights Protection on the Internet: The Promusicae Judgement of the European Court of Justice», en *European Intellectual Property Review*, 2008, 30(5), pp. 199 y ss.

[48] *Promusicae* alegaba, en síntesis, que aunque el art. 12 LSSI no establecía un supuesto específico de diligencias preliminares, sí contemplaba un deber de colaboración o información de los pres-

El Juzgado de lo Mercantil acogió inicialmente la pretensión de *Promusicae*, por respeto al derecho fundamental de esta asociación a la tutela judicial efectiva, y ordenó a *Telefónica* la puesta a disposición del tribunal de los datos de identificación de los presuntos infractores. *Telefónica* formuló la correspondiente oposición, que se fundaba, entre otras razones, en que, según establecía el entonces vigente art. 12 LSSI, los datos reclamados por *Promusicae* sólo podían comunicarse a las autoridades competentes en el ámbito de una investigación criminal o para la defensa nacional o la salvaguardia de la seguridad pública, pero no para la preparación de un proceso civil.

Así las cosas, el Juzgado, con la conformidad de las partes, decidió plantear una cuestión prejudicial ante el TJCE para determinar si el art. 12 LSSI era compatible con el derecho comunitario. La pregunta, en concreto, era si los arts. 15.2 y 18 DCE, los arts. 8.1) y 2) DDASI, el art. 8 DRDPI y los art. 17.2 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea permiten a los Estados miembros restringir al marco de una investigación criminal o para la salvaguardia de la seguridad pública y de la defensa nacional, con exclusión, por lo tanto, de los procesos civiles, el deber de retención y puesta a disposición de datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, que recae sobre los operadores de redes y servicios de comunicaciones electrónicas, proveedores de acceso a redes de telecomunicaciones y prestadores de servicios de alojamiento de datos.

Presentaron alegaciones ante el TJCE, además de las partes en el procedimiento nacional, la Comisión, el Reino Unido, Italia, Finlandia y Eslovenia. La Comisión hizo una defensa a ultranza de la primacía del derecho a la protección de datos, secundada por Italia. El Reino Unido, Finlandia y Eslovenia, por su parte, defendieron la necesidad de que los tribunales civiles estuvieran legitimados para ordenar a los proveedores de acceso la revelación de la identidad de sus abonados que utilizaran la conexión a Internet para infringir derechos de propiedad intelectual. El 17 de julio de 2007 la Abogada General, Juliane Kokott, presentó sus conclusiones, en las que se decantó por la prevalencia de las Directivas sobre protección de datos y propuso al Tribunal que respondiera a la petición de decisión prejudicial en el sentido de que es compatible con el Derecho comunitario que los Estados miembros excluyan la comunicación de datos de tráfico personales para la persecución por vía civil de las infracciones de los derechos de propiedad intelectual.

El TJCE, reunido en Gran Sala, resolvió la cuestión de forma salomónica, en el sentido de que los arts. 15.2 y 18 DCE, 8 DDASI y 8 DRDPI, en relación con la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, no obligan

---

tadores de servicios respecto de los datos de conexión y tráfico de sus abonados. Ese deber de información, puesto en relación con los arts. 15 y 18 DCE, con el art. 8 DDASI y, sobre todo, con el art. 8 DRDPI, de los que cabría colegir la obligación de los proveedores de acceso de comunicar a los titulares de derechos de propiedad intelectual infringidos, en el marco de un procedimiento civil, la identidad de los usuarios infractores, habilitaba de forma implícita a *Promusicae* para solicitar en nombre de sus asociados estas diligencias preliminares.

a los Estados miembros a imponer, en una situación como la que nos ocupa, el deber de comunicar datos personales con objeto de garantizar la protección efectiva de los derechos de autor en el marco de un procedimiento civil. «Sin embargo —continúa—, el Derecho comunitario exige que dichos Estados miembros, a la hora de adaptar su ordenamiento jurídico interno a estas Directivas, procuren basarse en una interpretación de éstas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario. A continuación, en el momento de aplicar las medidas de adaptación del ordenamiento jurídico interno a dichas Directivas, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su derecho nacional de conformidad con estas mismas Directivas, sino también no basarse en una interpretación de éstas que entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad».

Antes de adentrarme en el comentario de la respuesta dada por el TJCE a la cuestión planteada, me parece importante resaltar que se resuelve sin tener en cuenta la Directiva sobre Conservación de Datos, pues no era temporalmente aplicable a los hechos que dieron lugar al procedimiento principal seguido ante el Juzgado de lo Mercantil núm. 5[49]. Aunque a primera vista ello podría restar importancia a esta sentencia[50], lo cierto es que la doctrina que sienta es intemporal, en la medida en que insiste en la necesidad de interpretar el Derecho comunitario y las normas nacionales que lo incorporan de forma tal que garantice un adecuado equilibrio entre el derecho a la protección de datos personales y los demás derechos fundamentales.

Entrando ya en el examen, siquiera sucinto, de la sentencia, tres son las conclusiones esenciales que se extraen de su lectura.

---

[49] La Directiva sobre Conservación de Datos entró en vigor en mayo de 2006, mientras que las diligencias preliminares que dieron lugar a la cuestión prejudicial se solicitaron en noviembre de 2005, en relación con unos datos de tráfico generados en mayo de 2005. De acuerdo con la jurisprudencia del TJCE, los actos comunitarios, como regla general, no producen efectos retroactivos. Por tanto, para que la Directiva sobre Conservación de Datos afectara a situaciones anteriores a la fecha de su publicación debería haberlo previsto expresamente. Así se desprende de la sentencia del TJCE de 25 de enero de 1979, *Racke*, asunto 98/78, Rec. 69, que califica como excepcional que un acto comunitario tenga efectos retroactivos. En la misma línea, en la sentencia de 1 de abril de 1993, *Diversinte, S.A.*, asunto C-260/91 y C-261/91, apartados 9 y 10, el TJCE declara que «si bien, por regla general, el principio de seguridad de las situaciones jurídicas se opone a que el punto de partida del ámbito de aplicación temporal de un acto comunitario se fije en una fecha anterior a su publicación, puede ocurrir de otro modo, con carácter excepcional, siempre que lo exija el fin perseguido y se respete debidamente la confianza legítima de los interesados (véase recientemente la sentencia de 11 de julio de 2001, Crispoltoni, C-368/89, Rec. P. I-3695, apartado 17). No obstante, procede recordar que, según esta jurisprudencia, aunque los efectos retroactivos de los actos comunitarios no han de excluirse necesariamente, es preciso que los actos que tengan tales efectos contengan en su exposición de motivos las indicaciones que justifiquen los efectos retroactivos que se pretenden (véase el auto de 1 de febrero de 1984, Ilford/Comisión, 1/84 R, Rec. P. 423, apartado 19)». De acuerdo con esta jurisprudencia, una Directiva sólo producirá efectos retroactivos si así lo indica expresamente y lo justifica en su exposición de motivos, lo que no ocurre en el caso de la Directiva sobre Conservación de Datos.

[50] Parecería que esta doctrina jurisprudencial ha nacido desfasada.

La primera es que, para el TJCE, los Estados miembros pueden limitar el alcance de los derechos reconocidos en los arts. 5 y 6 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas (referidos a la confidencialidad de las comunicaciones y protección de los datos de tráfico) cuando sea necesario para la protección de los derechos y libertades de otras personas, tal y como establece el art. 13.1.g) de la Directiva sobre Protección de Datos Personales, aplicable por la remisión contenida en el art. 15.1 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas[51]. Señala asimismo que este art. 15.1 expresa «la voluntad del legislador comunitario de no excluir de su ámbito de aplicación la protección del derecho de propiedad ni la de las situaciones en que los autores pretenden obtener estar protección en el marco de un procedimiento civil» (parágrafo 53). Esto viene a significar que los artículos 5 y 6 de la Directiva no excluyen, sin más, cualquier tratamiento de datos relacionados con la identificación de usuarios de servicios de comunicaciones electrónicas que no sea realizado por la autoridad competente en el marco de la detección, investigación o enjuiciamiento de un delito. O, lo que es lo mismo, significa que los ordenamientos nacionales pueden permitir tratamientos vedados por estos arts. 5 y 6 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas cuando sea necesario para proteger derechos de terceros, incluida la propiedad intelectual. Esta doctrina permite a Estados miembros como el Reino Unido[52],

---

[51] Señala al respecto el TJCE: «49. En lo que atañe, por otra parte, al artículo 15, apartado 1, de la Directiva 2002/58, es necesario recordar que, a tenor de esta disposición, los Estados miembros pueden adoptar medidas legales para limitar el alcance, en particular, de la obligación de garantizar la confidencialidad de los datos de tráfico cuando tal limitación constituya una medida necesaria, proporcionada y apropiada, en una sociedad democrática, para proteger la seguridad nacional —es decir, la seguridad del Estado—, la defensa y la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el artículo 13, apartado 1, de la Directiva 95/46. 50. El artículo 15, apartado 1, de la Directiva 2002/58 ofrece así a los Estados miembros la posibilidad de establecer excepciones a la obligación de principio de garantizar la confidencialidad de los datos personales que les incumbe en virtud del artículo 5 de la misma Directiva. (…) 53. Sin embargo, es preciso constatar que el artículo 15, apartado 1, de la Directiva 2002/58 termina la enumeración de las excepciones mencionadas haciendo una referencia expresa al artículo 13, apartado 1, de la Directiva 95/46. Pues bien, éste autoriza también a los Estados miembros a adoptar medidas que limiten la obligación de confidencialidad de los datos personales, cuando tal limitación constituya una medida necesaria para la salvaguardia de la protección de los derechos y libertades de otras personas. Puesto que no precisan los derechos y libertades de que se trata, debe interpretarse que dichas disposiciones del artículo 15, apartado 1, de la Directiva 2002/58 expresan la voluntad del legislador comunitario de no excluir de su ámbito de aplicación la protección del derecho de propiedad ni la de las situaciones en que los autores pretenden obtener esta protección en el marco de un procedimiento civil».

[52] En el Reino Unido nunca se ha planteado problema en cuanto a la recopilación por los titulares de derechos de propiedad intelectual de las direcciones IP de quienes infringen sus derechos a través de redes *peer to peer*. De hecho, son numerosas las órdenes judiciales (denominadas *Norwich-Pharmacal Orders*) dictadas por los tribunales civiles, a instancia de productores fonográficos, para que los prestadores de servicios de la sociedad de la información revelen la identidad de los usuarios de redes *peer to peer* que infringen derechos de propiedad intelectual. En este sentido, pueden verse las resoluciones de la *High Court of Justice, Chancery Division* de Inglaterra y Gales en los casos *Universal Island Records Ltd. et al. v. NTL Group et al.* (Orden de de 14 de octubre de 2004) y *Polydor Limited et al. v. Brown et. Al* (Sentencia de 28 de noviembre de 2005, que parte de la identificación del infractor a través de una orden judicial de 11 de marzo de 2005, que cita). Pueden verse también las resoluciones de la *Commercial Court* de Irlanda del Norte en los casos *EMI Records (Ireland) Ltd., Sony BMG Music Entertainment (IRL) Ltd, Universal Music (Ireland) Ltd, Warner Music Ireland Ltd v. Eircom Ltd, BT Telecommunications Ireland Ltd*. (Orden de 8 de julio de 2005); *EMI Records (Ireland) Ltd., Sony BMG Music Entertainment (IRL)*

Francia[53], Holanda[54] o Dinamarca[55] mantener la obligación de los prestadores de servicios de revelar la identidad de sus abonados en el marco de procedimientos civiles por infracción de la propiedad intelectual. Y permite también que Estados que restringen la comunicación de los datos de identificación de los usuarios de Internet al ámbito penal modifiquen su posición.

Ltd, Universal Music (Ireland) Ltd, Warner Music Ireland Ltd v. Eircom Ltd., NT Communications Ireland Ltd. y Irish Broadband Internet Services Ltd. (Orden de 24 de enero de 2006)*;* y *EMI Records (Ireland) Ltd., Sony BMG Music Entertainment (IRL) Ltd, Universal Music (Ireland) Ltd, Warner Music Ireland Ltd v. Eircom Ltd., Irish Broadband Internet Services Ltd., NTL Communications (Ireland) Ltd., Imagine Telecommunications Ltd., Digiweb Ltd. Y Smart Telecom Holdings Ltd.* (Orden de 8 de junio de 2007). Es importante destacar cómo las resoluciones citadas insisten en que los derechos de privacidad (intimidad y protección de datos) de los usuarios de redes *peer to peer* deben ceder cuando existen indicios claros de que han infringido derechos de propiedad intelectual. Señalan, además, que la perturbación que sufren estos usuarios en sus derechos de privacidad a resultas de estas órdenes es mínima.

[53] En Francia, el art. 6 de la Ley 2004/575, para la Confianza en la Economía Digital (modificado por la Ley 2007/297, de 5 de marzo, obliga a los prestadores de servicios a conservar los datos de sus abonados, a fin de permitir la identificación de quien haya contribuido a la creación de los contenidos comunicados a través de ese servicio. Asimismo faculta a la autoridad judicial, que puede ser civil, para requerir a los prestadores de servicios la comunicación de esos datos. Además, para facilitar la defensa de la propiedad intelectual, el art. 9.4.º de la Ley 78-17, relativa a la Informática, a los Ficheros y a las Libertades, tras su modificación en 2004, en relación con los arts. L. 321-1 y L. 331-1 del Código de la Propiedad Intelectual, faculta a las entidades de gestión y a las asociaciones de defensa profesional de los titulares de derechos de propiedad intelectual para tratar datos de carácter personal a fin de proteger estos derechos frente a infracciones. Para ello requieren la autorización de la Comisión Nacional de la Informática y las Libertades (CNIL). Al amparo del citado art. 9.4.º, la CNIL concedió al Sindicato de Editores de Programas de Ordenador, mediante resolución de 24 de marzo de 2005, autorización para recopilar las direcciones IP de los supuestos infractores de sus derechos de propiedad intelectual a través de redes *peer to peer*. Unos meses más tarde, en cuatro resoluciones fechadas el 18 de octubre de 2005, la CNIL denegó a cuatro entidades de gestión representantes de autores y productores de música la preceptiva autorización para utilizar dispositivos permanentes de detección automatizada de infracciones de sus derechos de propiedad intelectual a través de redes *peer to peer*. Esos dispositivos automáticos estaban dirigidos a enviar mensajes disuasorios a los supuestos infractores y a recoger sus direcciones IP. Posteriormente, sin embargo, el Consejo de Estado, mediante resolución fechada el 23 de mayo de 2007, anuló esas cuatro resoluciones de la CNIL. Considera el Consejo de Estado que el tratamiento de datos que pretenden hacer las entidades de gestión solicitantes de la autorización no es desproporcionado, teniendo en cuenta que una de sus funciones es proteger la propiedad intelectual y que ésta se encuentra hoy en día especialmente amenazada por el intercambio ilícito de obras y prestaciones protegidas a través de Internet. Por consiguiente, entiende que debe concederse a las entidades de gestión la autorización para recoger por medios automáticos las direcciones IP de los infractores de derechos de propiedad intelectual a través de redes *peer to peer*.

[54] En Holanda, la CBP (*College Bescherming Persoonsgegevens*, o Comisión para la Protección de Datos Personales) ha declarado la licitud de la recogida por una entidad de gestión (BREIN) de las direcciones IP de quienes infringen sus derechos de propiedad intelectual a través de redes *peer to peer* (Resolución de 16 de abril de 2004). La CBP no se planteó si BREIN necesitaba el consentimiento de los supuestos infractores para el tratamiento de sus direcciones IP a fin de defender los derechos de propiedad intelectual vulnerados. Lo dio por sentado, probablemente porque el art. 8 f) de la Ley de Protección de Datos Personales holandesa, reproduciendo lo dispuesto por el art. 7 f) de la Directiva 95/46/CE, establece que no hace falta el consentimiento del afectado cuando prevalece un interés legítimo del responsable del tratamiento. Por su parte, el Tribunal de Primera Instancia de Utrecht, en auto de 12 de julio de 2005 (asunto *Brein contra UPC Nederland y otros*), declaró que los tribunales civiles pueden requerir a los prestadores de servicios de la sociedad de la información, a instancia de los titulares de derechos de propiedad intelectual, para que revelen la identidad de quienes infringen estos derechos a través de redes *peer to peer*, siempre que los titulares de derechos hayan respetado las disposiciones legales sobre protección de datos personales al recopilar la información sobre la infracción.

[55] En Dinamarca, la Agencia de Protección de Datos (*Datatilsynet*), en su resolución de 23 de abril de 2003, reconoció al Grupo Antipiratería (*Antipiratgruppen*), una asociación para la defensa pro-

La segunda conclusión que se extrae de la lectura de la Sentencia del TJCE en el caso *Promusicae* es que los Estados miembros no están obligados a imponer el deber de comunicar datos personales en el marco de un procedimiento civil con objeto de garantizar una protección efectiva de los derechos de propiedad intelectual, y ello sobre la base de que las disposiciones de la DCE, la DDASI y la DRDPI que exigen que los Estados miembros garanticen una protección efectiva de la propiedad intelectual en la sociedad de la información no pueden ir en perjuicio de las exigencias relativas a la protección de los datos personales[56]. Ya he expuesto con anterioridad mi opinión con respecto a la relación existente entre las Directivas sobre propiedad intelectual y las Directivas sobre protección de datos, que no es de subordinación, sino de coordinación, por lo que, para evitar reiteraciones, me remito a lo dicho entonces.

La tercera conclusión, que tiene su plasmación no sólo en la fundamentación jurídica de la sentencia, sino incluso en la respuesta que el TJCE da a la cuestión prejudicial, es que «el Derecho comunitario exige que los Estados miembros, a la hora de adaptar su ordenamiento jurídico interno a estas Directivas, procuren basarse en una interpretación de éstas que garantice un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario. A continuación, en el momento de aplicar las medidas de adaptación del ordenamiento jurídico interno a dichas Directivas, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con estas mismas Directivas, sino también no basarse en una interpretación de éstas que entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad»[57].

Esta afirmación es plenamente consecuente con la argumentación seguida por el TJCE a lo largo de la sentencia, que parte de la base de que los derechos en conflicto, regulados en las diversas Directivas aplicables al caso, se encuentran a un mismo nivel. Hemos visto, en efecto, que según el TJCE las Directivas sobre protección de datos no exigen que se ciña al ámbito penal la obligación de los prestadores de servicios de revelar la identidad de sus abonados infractores de la propiedad intelectual, pero que tampoco las Directivas sobre comercio electrónico y propiedad intelectual imponen a estos prestadores de servicios la obligación de identificar a sus abonados en el marco de procedimientos civiles. ¿Por qué? Porque no existe una relación jerárquica entre los derechos en conflicto, ni entre unas Directivas y otras. Ello da libertad a los Estados

---

fesional de titulares de derechos de propiedad intelectual, la facultad de tratar direcciones IP usuarios de Internet que infringían derechos de propiedad intelectual a través de la red, a fin de emprender las acciones legales pertinentes para la defensa de estos derechos. En opinión de la Agencia de Protección de Datos, los titulares de derechos de propiedad intelectual no podrían defender esos derechos si no pudieran tratar los datos personales de los infractores. Por ello, teniendo en cuenta que los datos que trata o son accesibles al público, o los ha obtenido a través de órdenes judiciales de revelación de esos datos, llega a la conclusión de que el tratamiento de datos efectuado por el Grupo Antipiratería es lícito.

[56] Vid. parágrafos 57 a 60 de la Sentencia.

[57] Parágrafo 70 de la sentencia y respuesta a la cuestión prejudicial.

miembros para buscar soluciones a esta colisión de derechos que sean equilibradas, proporcionadas, y que garanticen la máxima efectividad tanto de los derechos afectados como de las Directivas que los desarrollan[58].

De acuerdo con la sentencia, esa realización de una adecuada ponderación de los derechos en conflicto se exige no sólo a los legisladores nacionales, a la hora de incorporar las Directivas comunitarias aplicables, sino también, y esto es muy importante, a las autoridades y órganos jurisdiccionales nacionales que deben aplicar estas disposiciones. Por consiguiente, tanto los tribunales como los órganos administrativos competentes (por ejemplo las autoridades nacionales que velan por la protección de los datos personales) deben interpretar y aplicar las normas sobre protección de datos de tal forma que se garantice el requerido equilibrio de este derecho con otros derechos fundamentales comunitarios, así como el respeto al principio de proporcionalidad. No caben, en consecuencia, leyes nacionales que otorguen una primacía absoluta al derecho a la protección de datos sobre la propiedad intelectual o el derecho a la tutela judicial efectiva, igualmente merecedores de protección. Tampoco caben interpretaciones o aplicaciones de las leyes nacionales que conduzcan a resultados igualmente desequilibrados. Al contrario, tanto el legislador nacional como los órganos administrativos y jurisdiccionales que aplican la Ley han de tratar de conjugar los diversos derechos en conflicto, y alcanzar soluciones ponderadas[59].

IV. LAS CLAVES DEL CONFLICTO A NIVEL ESPAÑOL

En España resultan igualmente relevantes para la resolución del conflicto varias normas jurídicas. Por un lado, las disposiciones relativas a la protección de la propiedad intelectual, que, por lo que aquí nos interesa, son básicamente el art. 256.1.7.º de la Ley de Enjuiciamiento Civil (LEC) y los arts. 138, 139.1.h) y 141.6 del Texto Refundido de la Ley de Propiedad Intelectual (TRLPI), tras su modificación por las leyes 19/2006 y 23/2006. Por otro lado, las disposiciones en materia de protección de datos, constituidas por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD), con su Reglamento de desarrollo[60], los arts. 33 y siguien-

---

[58] En el mismo sentido, KUNER, «Data Protection and Rights Protection on the Internet: The Promusicae Judgement of the European Court of Justice», *cit.*, pp. 201-202.

[59] LASARTE hace una lectura más pesimista de la sentencia, que en absoluto comparto, en LASARTE ALVAREZ, C., «Comunicaciones Electrónicas *peer to peer* (P2P) *versus* derechos de autor», en *Diario La Ley*, núm. 6951, 22 de mayo de 2008, cuando afirma: «La interpretación realizada de la normativa vigente por el Tribunal de Justicia, sin duda alguna, resulta acorde con los parámetros tradicionales de la hermenéutica jurídica y con el conjunto de los mandatos contendido en las disposiciones a tener en cuenta, pero llega a una conclusión absolutamente insatisfactoria para todos los autores y creadores, cuyas reclamaciones judiciales en vía civil son condenadas, irremisiblemente, al fracaso, de manera tal que cualesquiera infracciones y conductas contrarias a la propiedad intelectual que no merezcan la calificación de delito propiamente dicho quedarán absolutamente impunes ante la imposibilidad de prueba de las descargas masivas y de la identificación de las personas que las realizan».

[60] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, publicado en el BOE núm. 17, de 19 de enero de 2008.

tes de la Ley 32/2003, General de Telecomunicaciones, desarrollados por el Reglamento sobre condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios[61], y la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (Ley de Conservación de Datos). Veámoslas separadamente.

1. La protección de la propiedad intelectual en la Ley de Propiedad Intelectual y en la Ley de Enjuiciamiento Civil

1. Las diligencias preliminares de la Ley de Enjuiciamiento Civil

El derecho de información reconocido por el art. 8 DRDPI a los titulares de propiedad intelectual fue introducido en nuestro ordenamiento por la Ley 19/2006, de 5 de junio, por la que se amplían los medios de tutela de los derechos de propiedad intelectual e industrial y se establecen normas procesales para facilitar la aplicación de diversos reglamentos comunitarios. Esta Ley vino a incluir en el art. 256.1.7.º LEC una nueva diligencia preliminar para preparar procedimientos por la vulneración de derechos de propiedad intelectual e industrial, dirigida a obtener información sobre el origen de la infracción[62].

De acuerdo con el art. 256.1.7.º LEC, quien esté legitimado para ejercitar una acción por infracción de un derecho de propiedad intelectual cometida mediante actos desarrollados a escala comercial[63], podrá solicitar frente a quien, a escala comercial, haya prestado los servicios que pudieran haber lesionado la propiedad intelectual, la adopción de diligencias de obtención de datos sobre el origen de la infracción, incluida la identidad de los supuestos infractores, con vistas a emprender contra ellos las oportunas acciones legales. Aunque el tenor del precepto es menos claro que el del art. 8 DRDPI, el legitimado pasivo de esta diligencia preliminar es el intermediario que presta al infractor, a escala comercial, los servicios de los que éste se vale para cometer la infracción.

Como ya he explicado en otro lugar[64], tal y como está redactado el art. 256.1.7.º podría no resultar conforme con el art. 8 DRDPI. De acuerdo con éste, en caso de vulneración de la propiedad intelectual, los titulares de los derechos lesionados pueden solicitar a las autoridades competentes que requieran a quienes prestan a escala comercial servicios utilizados por los in-

---

[61] Real Decreto 424/2005, de 15 de abril.

[62] Sobre esta diligencia preliminar vid. Bercovitz, Garrote, González Gozalo y Sánchez Aristi, *Las reformas de la Ley de Propiedad Intelectual*, Tirant lo Blanch, Valencia, 2006, pp. 205 y ss. En una vertiente más procesal, vid. Armengot Vilaplana, A., «La tutela judicial civil de los derechos de propiedad intelectual tras las reformas introducidas por las Leyes 19/2006 y 23/2006». *Revista Jurídica de Deporte y Entretenimiento*, núm. 18, año 2006-3, pp. 535 y ss.

[63] El concepto de acto desarrollado a escala comercial aparece definido en el último párrafo del art. 256.1.8.º LEC, entendiendo por tal aquel acto realizado para obtener beneficios económicos o comerciales directos o indirectos.

[64] Cfr. Bercovitz, Garrote, González Gozalo y Sánchez Aristi, *Las reformas de la Ley de Propiedad Intelectual*, *cit.*, pp. 209-211.

fractores para cometer la infracción para que revelen la identidad de éstos, con independencia de que la infracción en sí sea o no a escala comercial. En cambio, el tenor literal del art. 256.1.7.º LEC parece limitar este derecho de información a aquellos casos en que las infracciones se hayan cometido a escala comercial, lo que deja fuera de su ámbito de aplicación las infracciones que no tengan esa escala comercial, aun cuando se hayan cometido utilizando servicios prestados a escala comercial. Como semejante interpretación reduciría el mínimo nivel de protección exigido por el art. 8 DRDPI, en relación con el art. 2.1 DRDPI, no puede mantenerse. Debemos entender, en consecuencia, que cuando el art. 256.1.7.º LEC hace referencia a infracciones «cometidas mediante actos desarrollados a escala comercial» comprende aquellas infracciones que se hayan cometido utilizando servicios prestados por terceros a escala comercial, aun cuando la infracción en sí no tenga esa entidad.

De acuerdo con esta interpretación del art. 256.1.7.º LEC conforme con el art. 8 DRDPI, parece que los titulares de derechos de propiedad intelectual están legitimados para solicitar a los proveedores de acceso a Internet, en el marco de un procedimiento civil, la revelación de la identidad del destinatario de ese servicio que se vale del mismo para infringir los derechos de aquellos a través de redes *peer to peer*. Revelada la información, el art. 259.4 LEC dispone que «la información obtenida se utilizará exclusivamente para la tutela jurisdiccional de los derechos de propiedad intelectual del solicitante de las medidas, con prohibición de divulgarla o comunicarla a terceros». Y continúa: «a instancia de cualquier interesado, el tribunal podrá atribuir carácter reservado a las actuaciones, para garantizar la protección de los datos e información que tuvieran carácter confidencial». Obsérvese, por tanto, que el legislador español optó, a la hora de incorporar el art. 8 DRDPI, por una solución perfectamente equilibrada entre las necesidades derivadas de la tutela judicial efectiva de la propiedad intelectual y el derecho a la protección de datos, permitiendo implícitamente el tratamiento de esos datos por los titulares de derechos y los proveedores de acceso (no se establece en la LEC ninguna limitación a la obligación de los prestadores de servicios de revelar la identidad de los destinatarios de los mismos fundada en el derecho a la protección de datos), con vistas exclusivamente a identificar a los infractores en el marco de un procedimiento civil por vulneración de la propiedad intelectual, y asegurando en lo demás la confidencialidad de esos datos[65].

---

[65] En el momento de la promulgación de la Ley 19/2006, que introdujo el nuevo art. 256.1.7.º LEC, estaba vigente el antiguo art. 12 LSSI, cuyo apartado 3 establecía que los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios debían conservar los datos de conexión y tráfico de sus usuarios «para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública o la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así lo requieran». Este artículo 12.3 LSSI debía entenderse desplazado por el art. 256.1.7.º LEC para el caso concreto regulado en éste, por aplicación de los principios de especialidad y temporalidad. La posterior promulgación de la Ley de Conservación de Datos, sin embargo, volvió a complicar las cosas para los titulares de derechos, como veremos más adelante.

2. La acción de cesación, cautelar y definitiva, de la Ley de Propiedad Intelectual

El TRLPI (arts. 138 a 141) reconoce a los titulares de derechos de propiedad intelectual la facultad de solicitar la adopción de medidas cautelares o definitivas de cesación de toda actividad infractora. Asimismo les legitima para ejercitar acciones indemnizatorias contra los infractores.

Según el art. 138.III TRLPI, los titulares de derechos no sólo podrán ejercitar acciones de cesación definitiva o cautelar contra los infractores, sino también contra los intermediarios a cuyos servicios recurra un tercero para infringir derechos de propiedad intelectual, aunque los actos de dichos intermediarios no constituyan en sí mismos una infracción. Este precepto es desarrollado por los arts. 139.1.h), para la tutela definitiva, y 141.6, para la tutela cautelar[66].

De acuerdo con el art. 139.1.h) TRLPI el cese de la actividad ilícita que puede solicitar el titular de los derechos infringidos puede comprender «la suspensión de los servicios prestados por intermediarios a terceros que se valgan de ellos para infringir derechos de propiedad intelectual», sin perjuicio de lo dispuesto en la LSSI. En el mismo sentido, el art. 141.6 TRLPI establece que en caso de infracción o cuando exista temor racional y fundado de que ésta va a producirse, la autoridad judicial podrá decretar, a instancia del titular de derechos afectado, «la suspensión de los servicios prestados por intermediarios a terceros que se valgan de ellos para infringir derechos de propiedad intelectual», sin perjuicio de lo dispuesto en la LSSI. Lo dispuesto en la LSSI son las exenciones de responsabilidad (puertos seguros) de que disfrutan los prestadores de servicios de la sociedad de la información intermediarios en diversos casos, y que les pone a salvo de eventuales reclamaciones de daños y perjuicios por las víctimas de actos ilícitos cometidos a través de la red.

Evidentemente, si los preceptos citados prevén la posibilidad de pedir, como medida cautelar o definitiva, que los intermediarios, entre los que se encuentran los proveedores de acceso a Internet, suspendan el servicio del que se vale un tercero para infringir la propiedad intelectual ajena, es obvio que implícitamente está autorizando todo tratamiento de datos que sea imprescindible para que pueda solicitarse por el titular de los derechos infringidos y ejecutarse por el prestador de servicios intermediario dicha medida cautelar o definitiva de suspensión, máxime cuando ningún precepto de la Ley de Propiedad Intelectual prevé limitación alguna relacionada con el derecho a la protección de datos personales.

---

[66] Sobre la posibilidad de solicitar la suspensión cautelar o definitiva del servicio de acceso a Internet prestado por un proveedor de acceso a un usuario de redes *peer to peer*, vid. GARROTE FERNÁNDEZ-DÍEZ, I., *Pe. i.*, núm. 27, septiembre-diciembre de 2007, pp. 13 y ss.

2. La legislación española en materia de protección de datos.

1. La Ley Orgánica de Protección de Datos de Carácter Personal y su Reglamento de desarrollo

Como es sabido, el derecho a la protección de datos de carácter personal constituye en España un derecho fundamental reconocido en el art. 18.4 de la Constitución y desarrollado en la Ley Orgánica de Protección de Datos de Carácter Personal.

Para el tratamiento (incluyendo la obtención, utilización y comunicación) de datos personales, como lo son la dirección IP que una persona utiliza para conectarse a Internet, su nombre o su domicilio (datos que sirven para identificar a quien comete una infracción a través de Internet), es preciso, como regla general, su consentimiento, salvo que la ley disponga otra cosa (art. 6.1 LOPD). Como excepción que podría aplicarse a nuestro caso, no será necesario el consentimiento cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. El concepto de fuente accesible al público es retrictivo, según se desprende del art. 3.j) LOPD, que contiene una lista cerrada de fuentes accesibles al público[67], dentro de la cual se encuentran los medios de comunicación.

El Reglamento de desarrollo de la LOPD ha venido a precisar en su art. 10 los supuestos que legitiman el tratamiento de los datos conforme al art. 6 LOPD. De acuerdo con el art. 10.2 del Reglamento, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado en dos casos. Primero, cuando lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes: que el tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 LOPD; o que el tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas. Segundo, cuando los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado. El concepto de fuente accesible al público es todavía más estricto que el del art. 3.j) LOPD, al haber clarificado que la mención en éste de los medios de comunicación se refiere a los medios de comunicación social.

---

[67] Vid. en este sentido, entre las más recientes, las sentencias de la Audiencia Nacional (Sala de lo Contencioso-Administrativo) de 24 de abril de 2007 (JUR 2007/136405), 30 de mayo de 2007 (JUR 2007/199490) ó 3 de septiembre de 2007 (JUR 2007/276044).

Lo primero que debemos señalar a la vista de los artículos anteriores es que no se ha incorporado correctamente a nuestro ordenamiento el art. 7.f) de la Directiva sobre Protección de Datos Personales, que, como antes hemos visto, permite el tratamiento no consentido de datos personales ajenos cuando sea necesario para la satisfacción de un interés legítimo prevalente del responsable del tratamiento. En la LOPD se condiciona esa excepción a que los datos se extraigan de una fuente accesible al público. En el Reglamento se añade una segunda condición alternativa: que exista una habilitación legal[68]. Ninguna de estas condiciones se encuentra en la Directiva, de acuerdo con la cual basta con que el tratamiento sea necesario para satisfacer un interés legítimo preponderante. Por ello, una lectura de la legislación nacional conforme con el Derecho comunitario impone una interpretación suficientemente amplia de esas condiciones. Semejante interpretación sería consecuente, además, con la doctrina de nuestro Tribunal Constitucional sobre el carácter limitado del derecho a la protección de datos personales, derivado de su relación con los demás derechos fundamentales reconocidos por nuestra Constitución[69].

Así las cosas, para que entendamos que los titulares de derechos o los proveedores de acceso pueden tratar en España datos de los usuarios de redes *peer to peer* a fin de proteger la propiedad intelectual es necesario que consideremos bien que la red *peer to peer* constituye un medio de comunicación social (en sentido amplio) o bien que existe una habilitación legal que legitima ese tratamiento.

Respecto a la primera alternativa, ha de ponerse de manifiesto que la Agencia Española de Protección de Datos se ha mostrado hasta el momento reacia a considerar Internet como un medio de comunicación, cuánto más una red *peer to peer*. Sin embargo, la Audiencia Nacional (Sala de lo Contencioso-Administrativo) ha mantenido la tesis contraria en su sentencia de 24 de abril de 2007[70], donde consideró que una página *web* en la que una persona publica deliberadamente sus datos personales constituye un medio de comunicación[71]. Si aplicamos esta doctrina a las redes *peer to peer*, podríamos mantener que constituyen medios de comunicación en la medida en que, a través de ellas, los usuarios ponen voluntariamente a disposición del público la información disponible en la carpeta com-

---

[68] En el art. 6.1 LOPD la habilitación legal se establece como excepción a la regla del consentimiento sin condicionarla a la satisfacción de un interés legítimo preponderante de un tercero. Sin embargo, está implícito que la habilitación legal se debe justificar por la existencia de tal interés prevalente, pues de lo contrario se estaría conculcando el contenido esencial del derecho fundamental del art. 18.4 de la Constitución.

[69] Cfr. STC 292/2000, de 30 de noviembre.

[70] JUR 2007/276044.

[71] Señala la Audiencia nacional: «Por tanto, a los efectos que aquí nos interesan y en un caso como el presente, en el que una persona publica conscientemente sus datos de carácter personal en su página web, sin establecer ninguna limitación (es más, señala expresamente en la página web en cuestión, bajo la denominación de nota alegal «no hay copyright que valga y todo lo que aparece en estas páginas es de uso público…») y a la que puede acceder cualquier usuario de la red sin ningún tipo de cortapisa, debe considerarse esa información publicada voluntariamente por el propio afectado en su página web de Internet, como divulgada en un «medio de comunicación», a los efectos del artículo 3.j) LOPD que comentamos».

partida de sus ordenadores, así como determinados datos personales, como por ejemplo su dirección IP. Siendo así, el tratamiento de esos datos no requeriría consentimiento si fuera necesario para la satisfacción de un interés legítimo preponderante. De esta manera, un titular de derechos estaría legitimado para recoger y tratar los datos personales de los usuarios infractores difundidos por éstos a través de la red, siempre que fuera necesario para ejercitar acciones para la defensa de su propiedad intelectual[72]. Es dudoso, sin embargo, si puede mantenerse esta interpretación tras la aprobación del Reglamento de desarrollo de la LOPD, dado que, como hemos visto, restringe el concepto de «medios de comunicación» a los «medios de comunicación social»[73].

En cuanto a la segunda alternativa, la habilitación legal, se acomoda con mayor facilidad a las exigencias del art. 7.f) de la Directiva sobre Protección de Datos Personales. Del art. 6.1 LOPD (como también del art. 10.2 de su Reglamento de desarrollo) se desprende que el derecho de protección de datos ha de ceder cuando sea necesario para lograr un fin legítimo perseguido por la ley. El concepto de ley comprende la Constitución, como norma superior jerárquica. Excluye, en cambio, los reglamentos[74]. En este sentido, cabe traer a

---

[72] Esta tesis viene corroborada por la reciente sentencia del Tribunal Supremo (Sala Segunda) de 9 de mayo de 2008, recurso de casación núm. 1797/2007 (todavía no incluida en ningún repertorio), en relación con un rastreo hecho por la Guardia Civil en una red *peer to peer* (eMule) para detectar delitos relacionados con la pornografía infantil. A través de dicho rastreo, efectuado sin autorización judicial, la Guardia Civil obtuvo un listado de direcciones IP a través de las cuales, en fechas y horas determinadas, se habían efectuado descargas o intercambios de archivos de fotografías y vídeos con contenido de pornografía infantil. Dicho listado se presentó con posterioridad en el Juzgado de Instrucción núm. 7 de Sevilla, solicitando una orden judicial dirigida a los correspondientes proveedores de acceso a Internet para que identificasen a los abonados que, en las fechas y horas indicadas, tenían asignadas esas concretas direcciones IP. En cumplimiento de dicho mandamiento judicial un prestador de servicios identificó a la acusada como usuaria de una de esas direcciones IP. En base a dicha información, y tras las oportunas diligencias de investigación, se enjuició el caso, donde la Audiencia Provincial de Tarragona absolvió a la acusada mediante sentencia de 2 de mayo de 2007, por entender, entre otras razones, que la prueba presentada era nula por haberse vulnerado gravemente en su obtención el derecho al secreto a las comunicaciones de la procesada. Interpuesto recurso de casación por el Ministerio Fiscal, la Sala de lo Penal del Tribunal Supremo lo estimó, declarando que «el acceso a dicha información (las IPs a través de las cuales se había intercambiado pornografía infantil), calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa 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 —como puntualiza con razón el Ministerio Fiscal— queda registrada siempre y ello lo sabe el usuario». Interesa destacar que, aunque aparentemente esta sentencia se enfrenta al caso desde el punto de vista de los derechos a la intimidad y al secreto de las comunicaciones, sí menciona y tiene en cuenta la normativa en materia de protección de datos, citando expresamente, aunque sea *obiter dicta*, la LOPD y su Reglamento de desarrollo, la Ley General de Telecomunicaciones y su Reglamento e incluso, aunque no era temporalmente aplicable, la Ley de Conservación de Datos. De ahí que resulte especialmente ilustrativo, a los efectos que aquí nos interesa, que califique de pública y accesible para cualquier usuario la información difundida voluntariamente por los usuarios de redes *peer to peer*. En definitiva, viene a reconocer que se trata de una fuente accesible al público.

[73] No puede dejar de apuntarse, sin embargo, la posible ilegalidad del Reglamento en cuanto a este extremo, pues, al acotar el concepto legal de medio de comunicación, limita el alcance de una de las excepciones al consentimiento del afectado previstas por el art. 6.2 LOPD, alejándolo más, si cabe, del art. 7.f) de la Directiva sobre Protección de Datos Personales que transpone.

[74] No basta, por tanto, una habilitación reglamentaria para excluir la regla general del consentimiento, como declara la resolución de la AEPD de 3 de abril de 2006 (expediente 174/2005).

colación numerosas resoluciones de la Agencia Española de Protección de Datos (AEPD) que han encontrado en preceptos legales o constitucionales la habilitación legal requerida por el art. 6.1 LOPD para el tratamiento de datos personales sin el consentimiento del afectado[75].

En nuestro caso, el fin legítimo legalmente reconocido que legitima el tratamiento de datos personales de los infractores de la propiedad intelectual es doble: por un lado, la protección de la propiedad intelectual, que constituye un derecho constitucional conforme al art. 32.1 de la Constitución. Por otro lado, el derecho fundamental a la tutela judicial efectiva, consagrado en el art. 24 de la Constitución.

La protección de la propiedad intelectual puede llevarse a cabo por la vía penal o por la vía civil.

Para que los titulares de derechos puedan defenderse por la vía penal frente a las infracciones de su propiedad intelectual que tienen lugar a través de redes *peer to peer*[76] es presupuesto necesario que puedan presentar las correspondientes denuncias, lo que no es sino consecuencia de su derecho a la tutela judicial efectiva, tal y como ha señalado repetidamente el Tribunal Constitucional[77]. Pues bien, el derecho a la tutela judicial efectiva del art. 24.1 CE, en su modalidad de derecho a promover la actividad jurisdiccional en el ámbito penal mediante la correspondiente denuncia, puede constituir la habilitación legal que, conforme al art. 6.1 LOPD, de acuerdo con la interpretación dada al mismo por la AEPD[78], legitima el tratamiento de direcciones

---

[75] Así, además de las abundantes resoluciones que encuentran dicha habilitación en el derecho a la tutela judicial efectiva reconocido por el art. 24 de la Constitución, a las que me referiré con posterioridad, cabe citar, por ejemplo, la Resolución de 27 de julio de 2006 (expediente 111/2005), según la cual la comunicación a la Comisión del Mercado de las Telecomunicaciones de determinados datos personales de los clientes de los proveedores de servicios telefónicos a los que se asignan números de teléfono está amparada por el principio de libre competencia consagrado en el art. 38.6 de la Ley General de las Telecomunicaciones y las normas que lo desarrollan; o la Resolución de 8 de enero de 2007 (expediente 164/2004), que declara que la Ley del Contrato de Seguro y la Ley de Ordenación y Supervisión de los Seguros Privados habilitan a las entidades aseguradoras para tratar los datos personales relativos a la salud de los perjudicados que deban ser indemnizados por aquéllas como consecuencia de un seguro de responsabilidad civil, en la medida en que sin tratar esos datos no pueden determinar la indemnización a pagar.

[76] Aunque no puede pasarse por alto que, en el supuesto que nos ocupa, la vía penal se encuentra con el obstáculo que supone la Circular 1/2006 de la Fiscalía General, de 5 de mayo, sobre los delitos contra la propiedad intelectual e industrial tras la reforma de la Ley Orgánica 15/2003, que ha declarado que el intercambio de archivos a través de redes P2P no reúne, en principio, los requisitos para su incriminación pena.

[77] Por todas, puede verse la STC 111/1995, de 4 de julio, que señala: «Cuando el denunciante fuere el ofendido por los hechos, y con independencia de que desee o no adquirir la condición procesal de parte, la denuncia no es sólo una obligación, sino también un derecho que por lógica forma parte del contenido esencial del derecho a la tutela judicial efectiva y mediante cuyo ejercicio el ofendido pone de manifiesto su deseo de promover la actividad jurisdiccional».

[78] Vid. Resoluciones de 26 de noviembre de 2004 [expediente 18/2004], 11 de abril de 2005 [expediente 114/2004], 27 de abril de 2006 [expediente 310/2005], 23 de mayo de 2006 [expediente 953/2004], 7 de julio de 2006 [expediente 519/2006], 2 de octubre de 2006 [expediente 961/2004], 20 de septiembre de 2006 [expediente 36/2005] ó 16 de marzo de 2007 [expediente 386/2006].

IP por los titulares de los derechos infringidos a través de una red *peer to peer*. En efecto, para poder iniciar mediante la pertinente denuncia un procedimiento penal por los eventuales delitos contra la propiedad intelectual que se puedan cometer a través de estas redes, los titulares de derechos deben tratar necesariamente las direcciones IP de los supuestos infractores. Sólo recabando las direcciones IP de estos usuarios y tomando nota de las obras o prestaciones protegidas que ponen a disposición del público a través de sus carpetas compartidas en un momento dado puede el titular de derechos presentar una denuncia suficientemente concreta como para que pueda dar inicio a un procedimiento penal viable. Sin el tratamiento de esas direcciones IP, la denuncia resultaría tan genérica («a través de las redes P2P se cometen delitos contra la propiedad intelectual») que sería archivada inmediatamente (de igual manera que si lo que se denunciara fuera, por ejemplo, que en el metro de Madrid se producen hurtos todos los días), pues para que una denuncia tenga algún valor como motor de arranque de un procedimiento penal debe concretar suficientemente los hechos supuestamente delictivos, de modo que puedan ser convenientemente investigados.

Evidentemente, la Ley no obliga a los titulares de derechos a obtener pruebas de la comisión del delito que denuncia (vid. art. 264 de la Ley de Enjuiciamiento Criminal), pero el art. 24.2 CE les otorga el derecho fundamental a utilizar los medios de prueba pertinentes para su defensa. Si ponemos en relación los dos apartados del art. 24 CE podemos colegir que los titulares de propiedad intelectual tienen derecho a probar los hechos que consideren constitutivos de delitos contra la propiedad intelectual en la medida en que sea pertinente para hacer viable la denuncia a través de la cual pretenden iniciar los correspondientes procedimientos penales. Este derecho constituye, entiendo, habilitación suficiente conforme al art. 6.1 LOPD para que los titulares de derechos de propiedad intelectual traten las direcciones IP de los supuestos infractores a través de redes *peer to peer*. Ese tratamiento servirá para presentar una denuncia suficientemente concreta de los hechos supuestamente delictivos, a partir de la cual podrán realizarse las diligencias judiciales oportunas para esclarecer los hechos y averiguar la identidad de los presuntos infractores.

En cuanto a la tutela civil de la propiedad intelectual, hemos visto que el TRLPI reconoce a los titulares de derechos de propiedad intelectual la facultad de solicitar medidas cautelares para la protección urgente de sus derechos, de instar el cese definitivo de las actividades ilícita de los infractores y de reclamar las indemnizaciones de daños y perjuicios correspondientes.

Para hacer uso de estas facultades, el titular de los derechos de propiedad intelectual infringidos necesita conocer la identidad del infractor. Así se desprende del art. 399.1 de la Ley de Enjuiciamiento Civil (LEC). En el caso de infracciones cometidas por usuarios de redes *peer to peer*, el titular de los derechos infringidos no puede por medios propios averiguar la identidad del infractor, pues éste actúa de forma anónima. Lo único que puede hacer, como

hemos visto, es recoger su dirección IP, así como otros datos relevantes relativos a la infracción, y con esos datos, acudir a la autoridad judicial para que ordene al proveedor de acceso a Internet que ha proporcionado esa dirección IP al infractor bien que revele la identidad de éste, en el ámbito de unas diligencias preliminares del art. 256.1.7.º LEC, o bien que suspenda el servicio del que se vale el abonado para cometer la infracción.

El art. 256.1.7.º LEC pretende justamente facilitar a los titulares de derechos de propiedad intelectual la averiguación, por vía judicial, de la identidad de los infractores, a fin de preparar el posterior procedimiento declarativo o cautelar en el orden jurisdiccional civil. De acuerdo con el citado artículo, en caso de infracción de derechos de propiedad intelectual, los titulares de los derechos infringidos podrán solicitar al juez, en el marco de un procedimiento de diligencias preliminares, que interrogue a quien ha prestado al infractor a escala comercial el servicio del que éste se ha valido para cometer la infracción, a fin de que revele la identidad del infractor.

Para que esta solicitud de diligencias preliminares pueda prosperar, el titular de los derechos infringidos está obligado a justificar que se cumplen los requisitos legalmente exigidos (art. 256.2 LEC). Ello implica acreditar la concurrencia de justa causa e interés legítimo en la solicitud, así como la adecuación de la diligencia solicitada con la finalidad perseguida (art. 258.1 LEC). La única forma de probar estos extremos es presentando a la autoridad judicial los datos relativos a la infracción recogidos con anterioridad. Sólo si se muestra al Juez que un usuario, cuya identidad se desconoce, se conectó a Internet en una fecha y a una hora concretas a través de una determinada dirección IP, y puso a disposición del público sin autorización obras o prestaciones protegidas del solicitante de las diligencias preliminares, podrá el juez acordar las diligencias solicitadas y exigir al proveedor de acceso a Internet que proporcionó al infractor esa dirección IP que revele la identidad del infractor. Para ello se precisa, indudablemente, el tratamiento previo de los datos relativos a la infracción por parte del titular de los derechos infringidos, pues sólo así se pueden obtener las pruebas que deberá presentar ante el Juez para que éste acceda a su petición. Sin ese tratamiento previo, por tanto, no podría el titular de los derechos de propiedad intelectual infringidos solicitar las diligencias preliminares del art. 256.1.7.º LEC. No podría, por consiguiente, demandar a los usuarios infractores conforme al art. 138 TRLPI, lo que conllevaría no sólo un menoscabo a su propiedad intelectual, sino también a su derecho fundamental a la tutela judicial efectiva, tanto en su modalidad de acceso a los tribunales para el ejercicio de sus derechos e intereses legítimos (art. 24.1 CE), como en su modalidad de utilizar todos los medios de prueba pertinentes para la defensa de sus pretensiones (art. 24.2 CE).

Además, el propio art. 256.1.7.º legitima el tratamiento de datos por parte de los proveedores de acceso cuando sea necesario para cumplir una orden judicial de revelación de la identidad de sus abonados infractores dictada en el marco de un procedimiento de diligencias preliminares.

De ahí que entendamos que todos estos preceptos de rango legal o constitucional habilitan tanto a los titulares de propiedad intelectual como a los proveedores de acceso para tratar los datos de quienes infringen sus derechos, siempre que ese tratamiento sea indispensable para poder ejercitar las acciones legales oportunas para la defensa de esos derechos.

Por otro lado, los titulares de derechos pueden iniciar también procedimientos civiles de cesación contra los prestadores de los servicios intermediarios de los que se valen los usuarios de Internet para cometer las infracciones, al amparo del último párrafo del art. 138 de la Ley de Propiedad Intelectual. Las medidas a las que se refiere el art. 138 son «la suspensión [definitiva] de los servicios prestados por intermediarios a terceros que se valgan de ellos para infringir derechos de propiedad intelectual, sin perjuicio de lo dispuesto en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico» —art. 139.1.h)— y «la suspensión [cautelar] de los servicios prestados por intermediarios a terceros que se valgan de ellos para infringir derechos de propiedad intelectual, sin perjuicio de lo dispuesto en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico» —art. 141.6 LPI—.

En el marco de estos procesos civiles, el tratamiento de datos no va dirigido a identificar al usuario para que pueda ser demandado por el titular de los derechos infringidos. La finalidad del tratamiento por el titular de la propiedad intelectual no es otra que especificar la conducta supuestamente ilícita y el servicio cuya suspensión se insta, para que el órgano jurisdiccional pueda resolver lo que proceda y, en su caso, ordenar la medida cautelar o definitiva solicitada. Sin ese tratamiento no podría determinarse ni la conducta ilícita ni el servicio que se pretende suspender, con lo que los arts. 138 *in fine*, 139.1.h) y 141.6 LPI quedarían vacíos de contenido. La finalidad del tratamiento por el proveedor de acceso, por su parte, es poder ejecutar una eventual orden judicial de suspensión del servicio utilizado por un abonado para infringir la propiedad intelectual ajena. Necesita, en efecto los datos suministrados por el órgano jurisdiccional (que serán los proporcionados por el titular de los derechos) para contrastarlos con sus registros, determinar quién es el titular de la cuenta de acceso en cuestión y poder suspenderle el acceso a Internet. Estos preceptos, por consiguiente, contienen una habilitación legal implícita para el tratamiento de aquellos datos del infractor necesarios para ejercitar la correspondiente acción contra el prestador de servicios intermediario y para que éste, en su caso, pueda cumplir la orden judicial correspondiente.

La anterior argumentación viene avalada por las numerosas resoluciones de la AEPD en las que, fundándose en la excepción del art. 6.1 LOPD, reconoce la licitud de un tratamiento de datos no consentido por el afectado, sobre la base de que, de lo contrario, se vulneraría el derecho a la tutela judicial efectiva del responsable de dicho tratamiento[79].

[79] Que el derecho a la protección de datos entra en conflicto con el derecho a la tutela judicial efectiva cuando para preparar una demanda es preciso tratar datos personales del demandado lo

2. La Ley General de Telecomunicaciones

Los arts. 5 y 6 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas han sido incorporados por los arts. 33 y siguientes de la Ley General de Telecomunicaciones y los arts. 61 y siguientes del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

La transposición del art. 5 de la Directiva se ha llevado a cabo a través de los arts. 33 y 35 de la Ley General de Telecomunicaciones. De acuerdo con estos preceptos, quienes prestan servicios de comunicaciones electrónicas disponibles al público (entre ellos los proveedores de acceso a Internet) deben garantizar el secreto de las comunicaciones, adoptando a tal efecto las medidas técnicas necesarias, así como asegurar la protección de los datos de carácter personal conforme a la legislación vigente y «sin perjuicio de la restante nor-

---

ha declarado la AEPD, por ejemplo, en sus Resoluciones de 2 de junio de 2006 (expediente 856/2005) y 7 de julio de 2006 (expediente 519/2006). Partiendo de esa base, las Resoluciones de 26 de noviembre de 2004 (expediente 18/2004), 11 de abril de 2005 (expediente 114/2004), 27 de abril de 2006 (expediente 310/2005), 23 de mayo de 2006 (expediente 953/2004), 7 de julio de 2006 (expediente 519/2006), 2 de octubre de 2006 (expediente 961/2004), 20 de septiembre de 2006 (expediente 36/2005) ó 16 de marzo de 2007 (expediente 386/2006), por citar algunas de las más recientes, han permitido el tratamiento no consentido de datos personales del demandado para su aportación como medios de prueba a los procesos judiciales seguidos contra él por el responsable del tratamiento. De forma similar, las Resoluciones de 2 de diciembre de 2004 (expediente 239/2004), 30 de diciembre de 2004 (expediente 664/2004), 14 de enero de 2005 (expediente 292/2004), 28 de febrero de 2005 (expediente 354/2004), 7 de marzo de 2005 (expediente 360/2004) ó 27 de julio de 2005 (expediente 166/2005), por ejemplo, facultan a los abogados y procuradores para tratar datos personales de los oponentes de sus clientes en el ejercicio de sus cometidos. De las resoluciones citadas puede colegirse que cuando el tratamiento de datos es esencial para preparar una demanda contra el afectado por ese tratamiento, el artículo 24 CE habilita para realizar ese tratamiento, sin necesidad de contar con el consentimiento del titular de esos datos. En nuestro caso, la recogida y el almacenamiento de las direcciones IP de los infractores son necesarios para el ejercicio de las acciones de defensa de los derechos de propiedad intelectual vulnerados. Por tanto, debe entenderse que el art. 24 CE, en relación con los arts. 138 LPI y 256.1.7.º LEC, faculta a los titulares de los derechos infringidos para recoger esos datos personales de sus infractores, sin los cuales sería imposible presentar la correspondiente demanda. Este tratamiento no podría constituir en ningún caso una vulneración del derecho a la protección de datos personales de los infractores, en la medida en que, según una jurisprudencia constante del Tribunal Constitucional, lo que persigue el derecho a la protección de datos es «garantizar a las personas un poder de control sobre sus datos personales y sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado» (cfr. SSTC 292/2000, de 30 de noviembre; 85/2003, de 8 de mayo; 99/2004, de 25 de mayo; 110/2007, de 10 de mayo), mientras que el tratamiento pretendido por los titulares de derechos ni conlleva el tráfico ilícito de datos ni menoscaba la dignidad de su titular. La posterior comunicación de esos datos personales al órgano jurisdiccional competente tampoco requeriría el consentimiento de los afectados, en cuanto que está amparada por el art. 11.2.d) LOPD, según tiene declarado la AEPD. Pueden verse en este sentido las Resoluciones de 11 de abril de 2005 (expediente 114/2004), 21 de marzo de 2006 (expediente 595/2004), 27 de abril de 2006 (expediente 310/2005), 23 de mayo de 2006 (expediente 1122/2005), 2 de junio de 2006 (expediente 856/2005) ó 17 de octubre de 2006 (expediente 51/2006). Finalmente, la comunicación de esos datos por la autoridad judicial al proveedor de acceso y su posterior tratamiento por parte de éstos se justifica, igualmente, por la existencia de una habilitación legal implícita —arts. 6.1 y 11.2.a) LOPD— en los arts. 138.III, 139.1.h) y 141.6 TRLPI, que establece un deber de conducta tanto para el tribunal como para el prestador de servicios (cfr. art. 10.2 del Reglamento de desarrollo de la LOPD).

mativa específica aplicable». Ahora bien, como exponíamos antes, la puesta a disposición del público a través de una red *peer to peer* de una determinada información no está amparada por el secreto de las comunicaciones, ya que dicha comunicación es pública[80]. Y, por otro lado, aunque una vez que se inicia la conexión punto a punto entre los ordenadores de quien pone a disposición del público la información y quien pretende descargársela pudiera hablarse de una comunicación privada, el secreto de las comunicaciones no afecta a los participantes en ese acto de comunicación[81]. Por ello, los arts. 33 y 35 de la Ley General de Telecomunicaciones no son aplicables a nuestro caso.

Sí resultan aplicables, en cambio, por referirse al tratamiento de datos de tráfico, los preceptos que adaptan al ordenamiento nacional el art. 6 de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, en concreto las letras a) y b) del art. 38.3 de la Ley General de Telecomunicaciones. De conformidad con estas disposiciones, los abonados a servicios de comunicaciones electrónicas tienen derecho a que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación, sin perjuicio de lo dispuesto por la Ley de Conservación de Datos (cfr. art. 38.5.III de la Ley General de Telecomunicaciones), aunque no pueden evitar el tratamiento por el operador de los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones; o que esos datos de tráfico sólo sean utilizados con fines comerciales o para la prestación de servicios de valor añadido si media su consentimiento.

El art. 38.3 ha sido desarrollado por el art. 65 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios. De este desarrollo interesa destacar que, según el art. 65.5, el tratamiento de los datos de tráfico sólo podrá realizarse por las personas que actúen bajo la autoridad del operador prestador del servicio o explotador de la red que tengan ciertos cometidos, entre los que se encuentran el de suministrar la información requerida por los jueces y tribunales, por el Ministerio Fiscal o por los órganos o entidades que pudieran reclamarla en virtud de las competencias atribuidas por la Ley General de Telecomunicaciones. De donde podría colegirse que, en principio, sólo el proveedor de acceso puede tratar los datos de tráfico de un usuario sin su con-

---

[80] Vid. en este sentido la reciente STS (Sala Segunda) de 9 de mayo de 2008, recurso de casación núm. 1797/2007 (todavía no incluida en ningún repertorio), que resuelve que los datos que se difunden a través de una red *peer to peer* (eMule, en el caso concreto) no están protegidos ni por el derecho a la intimidad ni por el derecho al secreto de las comunicaciones. En concreto, el Tribunal Supremo declara 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 en Internet, no se hallaban protegidos por el artículo 18-1.º ni por el 18-3 de la Constitución».

[81] Cfr. STC 114/1984. Téngase en cuenta que el derecho al secreto de las comunicaciones no protege el contenido de la comunicación (que podrá estar amparado por otros derechos, como el derecho a la intimidad), sino el proceso de comunicación. Por ello, quien no intercepta la comunicación porque ya es parte de la misma no puede vulnerar este derecho.

sentimiento, y únicamente para los fines legal o reglamentariamente previstos, entre los que se encuentra, según el propio art. 65.5, el suministro de información requerida por los jueces y tribunales[82].

Ahora bien, debe tenerse en cuenta que el art. 65 de este Reglamento regula el tratamiento de datos de tráfico por los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, no por terceros usuarios de la red. Y ese es el contexto en que ha de interpretarse el art. 65.5, que, por lo tanto, regula qué personas que actúen bajo la autoridad de esos operadores pueden tratar los datos de tráfico de los abonados. Y ello precisamente porque desde dentro de la empresa prestadora de servicios de comunicaciones electrónicas es factible conocer la identidad del abonado cuyos datos de tráfico se están tratando, algo que, desde fuera, es imposible.

Si el tratamiento de los datos de tráfico por terceros ajenos al prestador de servicios no se rige por el art. 65 del Reglamento, ni tampoco por el art. 38 de la Ley General de Telecomunicaciones, debemos recurrir, en la medida en que esos datos constituyan al mismo tiempo datos personales, a la LOPD[83]. Me remito, por consiguiente, a lo que expuse en relación con ésta.

3. La Ley de Conservación de Datos

La Directiva sobre Conservación de Datos ha sido incorporada al derecho español por la Ley 25/2007. De acuerdo con el art. 1.º de esta Ley, su objeto es «la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados, siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación o enjuiciamiento de delitos graves».

Los sujetos obligados por la Ley son los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones (art. 2 de la Ley). Entre ellos se encuentran los proveedores de acceso a Internet. Los datos que han de conservar en relación con las conexiones a Internet son, entre otros, la dirección IP asignada al usuario, la

---

[82] En este sentido, señala el Tribunal Supremo (Sala Segunda) en su sentencia de 9 de mayo de 2008, recurso de casación núm. 1797/2007 (todavía no incluida en ningún repertorio), si bien lo hace *obiter dicta*, que de la LOPD y su Reglamento de desarrollo, así como de la Ley General de Telecomunicaciones y su Reglamento, «parece desprenderse que sin el consentimiento del titular de unos datos reservados, contenidos en archivos informáticos, no pueden facilitarse a nadie, salvo los casos especiales que autorizan sus propias normas, entre las que se halla la autorización, judicial, que lógicamente estaría justificada en un proceso de investigación penal».

[83] De conformidad con el art. 63 del Reglamento, en lo no previsto por él ni por el art. 38 de la Ley General de Telecomunicaciones se aplicará lo dispuesto por la legislación vigente sobre protección de los datos de carácter personal.

fecha y hora de la conexión y desconexión y el nombre y la dirección de Internet del abonado (art. 3 de la Ley). El plazo de conservación es de doce meses, si bien puede reducirse hasta seis o ampliarse hasta veinticuatro reglamentariamente (art. 5.1 de la Ley). De ello cabe colegir que los proveedores de acceso están obligados a retener durante doce meses los datos que permiten identificar al abonado que en un momento dado se conectó a Internet. La cuestión es si los datos así conservados pueden ser tratados con vistas a proteger la propiedad intelectual. Y a primera vista, la respuesta parece negativa.

En efecto, la Ley parece tajante cuando restringe al ámbito de la detección, investigación o enjuiciamiento de los delitos graves el deber de retención de datos que se impone a los prestadores de servicios. Ello podría interpretarse no sólo en el sentido de que se excluye el tratamiento de estos datos en el marco de un procedimiento civil[84], sino que incluso queda vedado en relación con delitos que no sean graves. Delitos graves son, según el art. 13.1 del Código Penal (CP), aquellos sancionados con una pena grave de las enumeradas en el art. 33.2 CP[85]. Los delitos contra la propiedad intelectual (arts. 270 y ss. del Código Penal) no constituyen delitos graves, pues en ningún caso tienen aparejadas penas graves. Por consiguiente, cabría mantener que no es posible tratar los datos conservados con fines de detección, investigación o enjuiciamiento de infracciones contra la propiedad intelectual.

Ello vendría confirmado por otros artículos de la Ley de Conservación de Datos. Así, el art. 4.1.II prohíbe a los sujetos obligados aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el art. 38 de la Ley General de Telecomunicaciones. El art. 6, por su parte, establece que los datos retenidos sólo podrán ser cedidos de acuerdo con lo dispuesto en la propia Ley de Conservación de Datos, para los fines que se determinan y previa autorización judicial (apartado 1), y que la cesión se efectuará únicamente a los agentes facultados, que son los miembros de las Fuerzas y Cuerpos de Seguridad del Estado, los funcionarios de la Dirección Adjunta de Vigilancia Aduanera y el personal del Centro Nacional de Inteligencia, cuando corresponda (apartado 2). Finalmente, el art. 7.2 dispone que mediante resolución judicial se determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los

[84] De hecho, en el apartado II de la Exposición de Motivos se señala que en el Capítulo I de la Ley «se precisan los fines que, *exclusivamente*, justifican la obligación de conservación, y que se limitan a la detección, investigación y enjuiciamiento de un delito contemplado en el Código Penal o las leyes penales especiales, con los requisitos y cautelas que la propia Ley establece».

[85] En concreto, la prisión superior a cinco años, 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 y 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.

datos conservados que habrán de cederse a los agentes facultados. De estas disposiciones parece colegirse que el único tratamiento de los datos retenidos que pueden hacer los proveedores de acceso, fuera de los previstos en el art. 38 de la Ley General de Telecomunicaciones, es consultarlos a fin de cumplir una orden judicial dictada en el ámbito de la detección, investigación o enjuiciamiento de delitos graves, y cederlos a los agentes facultados, que son los que realizan funciones de policía judicial.

Semejante interpretación, no obstante, conlleva la creación de un ámbito de impunidad en Internet en relación con múltiples conductas ilícitas, incluso tipificadas como delitos (siempre que no sean delitos graves). No me estoy refiriendo únicamente a infracciones de la propiedad intelectual. También a lesiones del derecho al honor, a la intimidad[86], a la propia imagen, incluso cuando constituyan delitos. En definitiva, ningún acto ilegal realizado a través de Internet podría ser perseguido si no estuviera tipificado como delito grave, con la consiguiente indefensión de la víctima, lo que, desde mi punto de vista, es inconstitucional. Por ello, pienso que ha de hacerse una lectura menos literal de la Ley de Conservación de Datos, que pondere adecuadamente los diversos intereses en conflicto. Y creo verdaderamente que esa lectura es posible, aunque, sin duda, sería más aconsejable una modificación legislativa que aclarara la cuestión.

Hemos visto, en efecto, que la sentencia del TJCE en el caso *Promusicae* señala que los derechos a la protección de datos, por un lado, y a la propiedad intelectual y a la tutela judicial efectiva, por otro, se encuentran al mismo nivel, sin que ninguno de ellos sea prevalente. En el mismo sentido se ha manifestado nuestro Tribunal Constitucional, por ejemplo en la STC 292/2000, de 30 de noviembre, en la que declara que el derecho a la protección de datos personales no es un derecho absoluto, sino que encuentra límites en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos[87]. Ello obliga a interpretar y aplicar la Ley de Conservación de datos de forma tal que

---

[86] Se produce el absurdo de que el derecho a la intimidad, emparentado con el derecho a la protección de datos (aun cuando se trate de un derecho fundamental distinto) cedería ante este último en Internet. De modo que se estaría imponiendo a la víctima de una intromisión ilegítima en el derecho a la intimidad la obligación de soportar dicha injerencia en aras de la protección de los datos del infractor.

[87] Afirma el Tribunal Constitucional: «Este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que ha de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7; 196/1987, de 11 de diciembre, F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ce-

se alcancen soluciones ponderadas, que reflejen un adecuado equilibrio entre los derechos en conflicto.

La interpretación literal de la Ley de Conservación de Datos anteriormente expuesta no es ponderada en absoluto, pues deja a los titulares de derechos de propiedad intelectual en la máxima indefensión frente a infracciones cometidas a través de Internet. Por ello, a la espera de una deseable modificación legislativa, es preciso encontrar una interpretación alternativa. La única vía que asegura una equilibrada protección de los distintos intereses en conflicto parte de la base de entender que el objeto de la Ley de Conservación de Datos, de acuerdo con su artículo 1.º, es simplemente (a) garantizar que esos datos estén disponibles para la detección, investigación y enjuiciamiento de los delitos graves y (b) regular el deber de cesión de los datos a las autoridades competentes para detectar, investigar y enjuiciar esos delitos graves. Quedaría, por tanto, fuera de su objeto la utilización de los datos conservados en el marco de un procedimiento civil. Esto no quiere decir que esa utilización esté excluida (prohibida) por la Ley de Conservación de Datos, sino que, simplemente, queda fuera de su ámbito objetivo de aplicación. Deja, por tanto, abierta la puerta a que otras normas, incluso anteriores, permitan la utilización de los datos conservados en el marco de procedimientos civiles. Entre esas normas se encuentran el art. 256.1.7.º LEC, o los arts. 138.III, 139.1.h) y 141.6 TRLPI. Es más, cabría entender que, estando ya en vigor estos artículos cuando se tramitó la Ley de Conservación de Datos, para que pudiera entenderse que ésta excluye el uso de los datos conservados por los prestadores de servicios en el marco de procedimientos civiles por infracción de derechos de propiedad intelectual tendría que haberse establecido así expresamente, lo que no se ha hecho.

Interpretando la Ley de Conservación de Datos a través de ese prisma, podrían solventarse los problemas que presentan sus arts. 4 y 6. El art. 4.1, según el cual «en ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38» de la Ley General de Telecomunicaciones, vendría a significar que los prestadores de servicios no pueden utilizar en beneficio propio los datos conservados, salvo en los supuestos contemplados en el mentado artículo 38. Pero tal no es el caso cuando el prestador de servicios trata los datos conservados a fin de cumplir una orden judicial de identificación del usuario proveniente de un tribunal civil, o de suspensión del servicio de acceso a Internet prestado a ese usuario.

En cuanto al art. 6, que establece que «los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dis-

---

der, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero, F. 6; 18/1999, de 22 de febrero, F. 2)». En el mismo sentido, el Tribunal Constitucional, en sus Autos 197/2003, de 16 de junio, y 212/2003, de 30 de junio, que no existe un derecho incondicionado y absoluto a la reserva de datos económicos, al amparo del derecho a la intimidad, pues tal derecho haría inoperante el deber constitucional de contribuir a los gastos públicos (art. 31.1 CE).

puesto en ella par los fines que se determinan y previa autorización judicial» y «únicamente a los agentes facultados», cabría entender que se refiere exclusivamente a las cesiones de datos reguladas por la Ley de Conservación de Datos, que son las relacionadas con la detección, investigación y enjuiciamiento de delitos graves, pero no a las cesiones reguladas en otras normas, como pueda ser el art. 256.1.7.º LEC. En cualquier caso, este precepto no impediría el tratamiento de los datos por el propio proveedor de acceso, sin cesión a terceros, con vistas a suspender el servicio prestado al infractor.

En definitiva, podría defenderse, aun cuando, desde luego, es una cuestión problemática, que, pese a la promulgación de la Ley de Conservación de Datos, los titulares de derechos de propiedad intelectual pueden recurrir a los tribunales civiles para que, en el marco del procedimiento de diligencias preliminares regulado en la Ley de Enjuiciamiento Civil, ordenen a los proveedores de acceso que identifiquen a los usuarios que se valgan de sus servicios para infringir derechos de propiedad intelectual, previa constatación de que hay indicios razonables de que se ha producido la infracción. O, cuando menos, que pueden solicitar a los tribunales civiles que ordenen a estos prestadores de servicios la suspensión del acceso a Internet del infractor, aunque para ello tenga que tratar los datos conservados de acuerdo con la Ley de Conservación de Datosl. Con esta interpretación se garantiza el equilibrio pretendido no sólo por el TJCE, sino también por nuestro Tribunal Constitucional, en la medida en que siempre será precisa la intervención de un órgano jurisdiccional, que deberá valorar, antes de dictar la orden que proceda, si el tratamiento de datos que conlleva está justificado.

V. SOLUCIONES AL CONFLICTO CONFORME AL DERECHO ESPAÑOL

Analizadas las claves del conflicto entre la propiedad intelectual y el derecho a la protección de datos, estamos en condiciones de exponer, a modo de síntesis, las soluciones a los problemas que el derecho a la protección de datos plantea a la hora de recabar la tutela judicial de la propiedad intelectual. En concreto, son tres las cuestiones que se suscitan. Si pueden los titulares de derechos recopilar datos relativos a las infracciones de su propiedad intelectual que se producen a través de redes *peer to peer*, si pueden los proveedores de acceso tratar esos datos con vistas a suspender o terminar la conexión a Internet de sus abonados infractores de la propiedad intelectual ajena y, finalmente, si están obligados los proveedores de acceso a revelar la identidad de sus abonados en el marco de procedimientos judiciales para la defensa de la propiedad intelectual.

1. La recogida de datos relativos a la infracción por parte de los titulares de derechos de propiedad intelectual

En mi opinión, los titulares de derechos están legitimados para recoger los siguientes datos relativos a las infracciones de su propiedad intelectual que se producen a través de redes *peer to peer*: fecha y hora de comisión de la infrac-

ción, dirección IP utilizada y obras o prestaciones protegidas compartidas[88]. Pueden recoger los datos por sí mismos o por un tercero contratado a tal efecto, siempre que se cumplan los requisitos del art. 12.2 LOPD.

Ese tratamiento se justifica por la existencia de un interés legítimo preponderante (tutela judicial de la propiedad intelectual), que sólo puede ser satisfecho mediante la recogida de los datos y su comunicación a la autoridad judicial (art. 6 LOPD y 10 de su Reglamento de desarrollo). Ese interés legítimo encuentra su reconocimiento en diversas normas que, de forma implícita, autorizan el tratamiento que los titulares de derechos pretenden llevar a cabo. Así, el derecho a recabar la tutela judicial efectiva del art. 24 de la Constitución, que en el ámbito penal se plasma en la posibilidad de presentar una denuncia suficientemente detallada como para que no sea archivada de plano. En el ámbito civil, son varios los preceptos de los que se colige una habilitación legal tácita para el tratamiento de datos por los titulares de derechos de propiedad intelectual. Así, el art. 256.1.7.º LEC prevé diligencias preliminares de averiguación de la identidad del infractor, consistentes en interrogar sobre su identidad a quien le ha prestado a escala comercial los servicios utilizados para cometer la infracción. Por su parte, los art. 138.III, 139.1.h) y 141.6 TRLPI facultan a los tribunales para ordenar, a instancia de los titulares de derechos, la suspensión cautelar o definitiva de los servicios de los que se vale el infractor para cometer la infracción contra la propiedad intelectual. Para que tanto las diligencias preliminares del art. 256.1.7.º LEC como las medidas cautelares o definitivas de los arts. 138.III, 139.1.h) y 141.6 puedan ser concedidas por el órgano judicial y atendidas por los proveedores de acceso (para que puedan resultar efectivas, en definitiva), y teniendo en cuenta el principio de justicia rogada y la carga de la prueba en el procedimiento civil, es obvio que los titulares de derechos deben estar legitimados para tratar los datos de los infractores única y exclusivamente con vistas a iniciar estos procedimientos civiles para la defensa de su propiedad intelectual.

La respuesta es especialmente clara en el segundo supuesto (ejercicio de acciones de cesación contra los proveedores de acceso), donde el titular de derechos no pretende averiguar la identidad del usuario, porque no le va a demandar. Es más, cabría incluso dudar que los datos recogidos por el titular de derechos constituyan datos personales cuando no van a servir para identificar al infractor, pues en este caso para él se trata de datos disociados, referidos a una persona no identificable por medios razonables.

Por otro lado, no debe olvidarse que los titulares de derechos obtienen los datos de la propia red *peer to peer*, y que ésta puede calificarse como una fuente accesible al público, en su condición de medio de comunicación, en tanto en

[88] Estas últimas no son datos personales, porque no sirven para identificar al infractor. Tampoco están amparadas por el derecho a la intimidad, dado que se trata de una información puesta voluntariamente a disposición del público por el propio infractor. Lo mismo ocurre con los nombres de usuario, que normalmente no son datos personales porque no son aptos para identificar al infractor. Por ello mismo, su recopilación por los titulares de derechos no plantea ningún problema.

cuanto es utilizada voluntariamente por sus usuarios para poner a disposición del público cualquier información. Por tanto, al amparo del art. 6.2 LOPD, los datos extraídos de la red *peer to peer* pueden ser utilizados por los titulares de derechos para defender su propiedad intelectual.

2. El tratamiento de esos datos por los proveedores de acceso para suspender o terminar la conexión a internet de los usuarios infractores

Como hemos visto, para que un proveedor de acceso pueda cumplir una eventual orden civil de suspensión del servicio que presta a un abonado, a través del cual éste infringe la propiedad intelectual ajena, es necesario que trate sus datos personales. Sólo consultando los datos relativos a la infracción (dirección IP, fecha y hora de la conexión a Internet) y cotejándolos con los que figuran en sus archivos puede identificar al abonado titular de la cuenta de acceso a Internet mediante la cual se ha cometido la infracción y suspender la prestación de este servicio.

Ese tratamiento de los datos de tráfico relativos a la infracción no está previsto en el art. 38 de Ley General de Telecomunicaciones, ni en el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios. Si a ello unimos que, según se desprende del art. 4 de la Ley de Conservación de Datos, los proveedores de acceso sólo pueden utilizar los datos de identificación del usuario de una red de comunicaciones electrónica que hayan retenido para los fines previstos en el art. 38 de la Ley General de Telecomunicaciones o para cederlos a los agentes facultados para la detección, investigación y enjuiciamiento de delitos graves, podría parecer que estos prestadores de servicios no están legitimados para tratar estos datos con vistas a cumplir una eventual orden de suspensión de los servicios prestados al infractor dictada al amparo del TRLPI.

Ahora bien, los arts. 138.III, 139.1.h) y 141.6 son claros cuando establecen entre las medidas cautelares y definitivas de cesación la suspensión de los servicios prestados al infractor por un intermediario. Hemos visto que para que esas medidas puedan adoptarse es imprescindible tratar los datos del infractor. Y dicho tratamiento también es indispensable para que esas medidas puedan ser ejecutadas por el proveedor de acceso. Por tanto, si la efectividad de dichas medidas previstas por la Ley de Propiedad Intelectual requiere el tratamiento de los datos del infractor, es claro que la propia previsión legal de estas medidas conlleva una habilitación tácita para el preceptivo tratamiento de datos. De lo contrario, las disposiciones legales que las establecen serían inútiles.

El necesario equilibrio entre el derecho a la protección de datos y la tutela judicial de la propiedad intelectual exige una interpretación de las distintas normas aplicables que asegure la máxima efectividad de los derechos en liza. Esa interpretación pasa por entender que el art. 4 de la Ley de Conservación de

Datos prohíbe a los proveedores de acceso utilizar en beneficio propio («aprovechar», dice la Ley) los datos que la Ley les obliga a retener. Pero no les prohíbe tratar esos datos para cumplir una orden judicial dictada en un procedimiento por infracción de la propiedad intelectual al amparo de los arts. 138.III, 139.1.h) y 141.6 TRLPI. En este caso, el tratamiento estaría justificado por el cumplimiento de una obligación jurídica prevista por la Ley, tal y como se desprende del art. 10 del Reglamento de desarrollo de la LOPD.

3. La revelación de la identidad de los usuarios infractores por los proveedores de acceso a internet.

La tercera cuestión es si, tras la promulgación de la Ley de Conservación de Datos, pueden los titulares de derechos de propiedad intelectual, en el marco del procedimiento civil de diligencias preliminares del art. 256.1.7.º LEC, solicitar que los proveedores de acceso sean obligados a revelar la identidad de los usuarios que infringen la propiedad intelectual de aquéllos a través de redes *peer to peer*.

La respuesta, a bote pronto, debería ser negativa. Si los proveedores de acceso sólo pueden retener los datos de sus abonados, aparte de por razones de facturación, para garantizar su disponibilidad para la detección, investigación y enjuiciamiento de delitos graves, no parece que esos datos puedan ser utilizados para identificar al usuario infractor de la propiedad intelectual en el marco de un procedimiento civil.

Ahora bien, semejante respuesta, como ya he señalado, es más que dudosa. Significaría que quien, al amparo del anonimato que le proporciona Internet, realiza un acto ilícito que no esté tipificado como delito grave (como por ejemplo ocurre con las infracciones contra la propiedad intelectual, que en ningún caso pueden constituir delitos graves) no puede ser perseguido, ni por la vía civil ni por la vía penal; que es impune, en definitiva. Significaría que la víctima de una infracción cometida a través de una red *peer to peer* no puede ser resarcida, porque sólo conociendo la identidad del infractor puede ejercitar una acción indemnizatoria. Significaría, en suma, que Internet es como una ciudad sin Ley, donde cualquier tropelía es posible, siempre que no constituya un delito grave. Un «puerto seguro» sin condiciones para los infractores de la propiedad intelectual. Un paraíso para los piratas. Algo inimaginable en un Estado democrático.

Por ello, creo que la Ley de Conservación de Datos ha de ser interpretada en el sentido de que no impide que los datos retenidos sean utilizados para fines distintos de la detección, investigación y enjuiciamiento de delitos graves, siempre que ese uso esté previsto legalmente. Y en nuestro caso, tal previsión se encuentra en el art. 276.1.7.º LEC, que obliga a los prestadores de servicios a revelar la identidad de sus abonados cuando infringen la propiedad intelectual.

VI. CONCLUSIÓN

Los usuarios de Internet tienen derecho a que se respeten sus derechos fundamentales en la red. Es más, el derecho de protección de datos, el derecho al secreto de las comunicaciones, el derecho a la intimidad o la libertad de expresión, exigen que se preserve la posibilidad de usar anónimamente Internet. Pero ello no supone ninguna especialidad con respecto a otros ámbitos de comunicación y expresión. También debe asegurarse la posibilidad de expresarse anónimamente fuera de Internet, o de comunicarse secretamente por cualquier otro medio, o de mantener dentro de la esfera privada, también fuera de la red, todo cuanto pertenezca a la intimidad personal o familiar. No podemos olvidar que Internet no es sino uno de los muchos medios de expresión y comunicación que tenemos a nuestra disposición. Por tanto, el nivel de protección de las personas en Internet ha de ser el mismo que en cualquier otro medio, ni más ni menos.

No debemos caer en el error de sobreproteger al usuario de Internet, de concederle derechos que van más allá de los que se reconocen en otros ámbitos, en detrimento de los derechos de los terceros. Un exceso de protección contribuiría a generar en el ciberespacio un ámbito de impunidad injustificado. En este sentido, un derecho de protección de datos personales mal entendido, que asegurara en todo caso a todo usuario de Internet el más absoluto anonimato a efectos civiles, e incluso a determinados efectos penales, o que dificultara el ejercicio de acciones de cesación dirigidas contra los intermediarios, fomentaría la comisión de actos ilícitos en Internet y generaría indefensión a los perjudicados.

En este contexto, la sentencia del TJCE de 29 de enero de 2008 en el asunto *Promusicae* ha venido a recordarnos que el derecho a la protección de datos no es un derecho absoluto. Es preciso ponerlo en relación con otros derechos constitucionales, como los derechos al honor, a la intimidad, a la propia imagen, a la tutela judicial efectiva… y a la propiedad intelectual. O lo que es lo mismo, es preciso ponerlo en relación con aquellos derechos de terceros con los que puede entrar en colisión, y ponderarlos, con vistas a alcanzar un adecuado equilibrio entre los derechos en conflicto. Esa labor le compete al legislador en primer lugar, pero también a quienes aplican la Ley.

La legislación española es deficitaria en este sentido, sobre todo por lo que respecta a la Ley de Conservación de Datos. El legislador no ha sido todo lo cuidadoso que cabría esperar y ha producido un texto normativo que, aparentemente, crea un ámbito de impunidad en Internet, no ya para las infracciones de la propiedad intelectual, sino para cualquier acto ilícito que no esté tipificado como delito grave. Sería deseable que el propio legislador enmendara su error, clarificando que el derecho de información previsto en el art. 256.1.7.º LEC puede ejercitarse también frente a infracciones ocurridas en Internet[89] y

[89] En el mismo sentido Lasarte Alvarez, «Comunicaciones Electrónicas *peer to peer* (P2P) *versus* derechos de autor», *cit.*

que los proveedores de acceso pueden tratar los datos de sus abonados para cumplir órdenes de cesación dictadas por los tribunales civiles. Mientras tanto, los tribunales y las autoridades competentes en materia de protección de datos tienen abierta la vía interpretativa para asegurar el necesario equilibrio entre este derecho a la protección de datos y los demás. Se trata, simplemente, de garantizar que no haya ámbitos de impunidad en nuestro ordenamiento, ni siquiera en Internet.