InDret
REVISTA PARA EL
ANÁLISIS DEL DERECHO

WWW. INDRET.COM

Direcciones IP y presunto anonimato. Tras la identidad del usuario infractor de derechos de propiedad intelectual en Internet

Patricia Llopis Nadal

Universitat de València

BARCELONA, OCTUBRE 2018

Abstract[1]

Quienes utilizan Internet para cometer actos ilícitos se benefician del presunto anonimato que ofrece la Red, sin embargo, en el estado actual de desarrollo de la tecnología es posible identificar al usuario que actuó tras una determinada dirección IP.

En el marco de un proceso civil para la tutela de los derechos de propiedad intelectual, la base legal para obtener los datos del presunto infractor la proporciona el art. 256.1.11.º de la LEC; esta disposición permite al titular de los derechos solicitar a los prestadores de servicios el nombre y apellidos de quien, careciendo de autorización, ha puesto a disposición del público sus obras.

Si bien esta diligencia pone fin al obstáculo que suponía para el acceso a la justicia desconocer la identidad del infractor, su práctica no está exenta de problemas. Así, a la restricción de las conductas tipificadas y a los requisitos impuestos por la propia norma –circunstancias que limitan su campo de aplicación-, debe añadirse la necesidad de que el tratamiento de las IPs –datos personales- sea conforme a derecho, la complejidad de saber a qué prestador pedir la información o la posibilidad de que quien contrató la línea no coincida con el autor de las infracciones.

Con el propósito de ofrecer una solución a todas estas cuestiones, el presente trabajo tiene por objeto clarificar el régimen jurídico de la diligencia preliminar dirigida a obtener la identidad del usuario que infringe derechos de propiedad intelectual en Internet.

Those who use Internet to commit unlawful acts take advantage of the presumed anonymity offered by the Net. However, in the current state of the technology, to identify the user that acted behind an IP address is possible.

Within the framework of a civil procedure in order to protect copyrights, the legal basis to obtain the alleged infringer data is given by article 256.1.11th of the Civil Procedure Act. This provision enables the copyrights holder to request to the Internet service providers the name and forenames of those who, without authorization, have made his works available to the public.

Even though this preliminary proceeding puts an end to an obstacle to the access to justice –created by ignoring the identity of the infringer, its practice is not trouble-free. The limitation of the conducts that can be pursued and the requirements issued by the norm are circumstances that narrow the field of application of this proceeding. The need to process the IP addresses, which are personal data, in accordance with the law, the complexity of knowing the service provider to whom request the information, besides the possibility that the owner of the Internet connection is not in line with the author of the infringements constitute, as well, some of the above mentioned problems.

For the purpose of providing an answer to all these issues, this paper is aimed at clarifying the legal regime of the preliminary proceeding used to discover the identity of the user that is infringing copyrights on the Internet.

[1] El presente trabajo toma como punto de partida la investigación realizada en el marco del programa de ayudas pre-doctorales UV-Atracció de Talent de VLC-CAMPUS, siendo completado posteriormente durante una estancia en el Max Planck Institute Luxembourg for International, European and Regulatory Procedural Law, gracias a la ayuda concedida por la "Fundación Privada Manuel Serra Domínguez".

Title: IP addresses and presumed anonymity. Going after the identity of the infringer user of copyrights on the Internet.

Palabras clave: diligencias preliminares, propiedad intelectual, Internet, usuario, dirección IP, intermediarios.

Keywords: preliminary proceedings, copyrigths, Internet, user, IP address, intermediaries.

Sumario

1. Introducción

El anonimato con el que es posible actuar en Internet ha constituido, tradicionalmente, un impedimento para la tutela judicial efectiva de los derechos de propiedad intelectual. El motivo de esta indefensión era que, si bien el titular de los derechos infringidos conocía la dirección IP desde la que se cometían los ilícitos, no podía obtener el nombre y apellidos del presunto infractor, por lo que, más allá de los números de su conexión a la Red, era incapaz de identificar al sujeto contra quien presentaba la demanda.

Esta situación mejora cuando, en virtud de la Ley 21/2014[2], se introduce en nuestro ordenamiento jurídico una diligencia preliminar dirigida a averiguar la identidad del usuario autor de la infracción[3]. De este modo, cuando los derechos de propiedad intelectual han sido infringidos en Internet, el art. 256.1.11.º de la Ley de Enjuiciamiento Civil[4] (en adelante LEC) permite al titular de los mismos preparar el proceso civil solicitando al prestador de servicios los datos de quien, careciendo de la preceptiva autorización, pone a disposición del público o difunde de manera directa o indirecta contenidos protegidos por la Ley de Propiedad Intelectual[5] (en adelante LPI)[6].

Si bien es cierto que esta previsión supone un notable avance respecto de la regulación precedente, la ley impone unos requisitos que, según el modo en que se interpreten, pueden restringir la aplicación –y, en consecuencia, la utilidad- de esta diligencia preliminar. Así, además de la existencia de indicios razonables de la infracción, será necesario que se trate de actos que no puedan considerarse realizados por meros consumidores finales de buena fe y sin ánimo de obtener beneficios económicos y

[2] Ley 21/2014, de 4 de noviembre, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, *B.O.E.*, núm. 268, de 5 de noviembre de 2014.

[3] Las diligencias preliminares son actuaciones de carácter pre-procesal realizadas por el futuro demandante, estas se solicitan ante los órganos jurisdiccionales con el objetivo de obtener la información necesaria para preparar la demanda (ORTELLS, 2015, p. 249).

[4] Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, *B.O.E.*, núm. 7, de 8 de enero de 2000.

[5] Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, *B.O.E.*, núm. 97, de 22 de abril de 1996.

[6] La referida disposición establece "1. Todo juicio podrá prepararse: […] 11.º Mediante la solicitud, formulada por el titular de un derecho de propiedad intelectual que pretenda ejercitar una acción por infracción del mismo, de que un prestador de servicios de la sociedad de la información aporte los datos necesarios para llevar a cabo la identificación de un usuario de sus servicios, con el que mantengan o hayan mantenido en los últimos doce meses relaciones de prestación de un servicio, sobre el que concurran indicios razonables de que está poniendo a disposición o difundiendo de forma directa o indirecta, contenidos, obras o prestaciones objeto de tal derecho sin que se cumplan los requisitos establecidos por la legislación de propiedad intelectual, y mediante actos que no puedan considerarse realizados por meros consumidores finales de buena fe y sin ánimo de obtención de beneficios económicos o comerciales, teniendo en cuenta el volumen apreciable de obras y prestaciones protegidas no autorizadas puestas a disposición o difundidas".

comerciales. Adicionalmente, al decidir sobre su concesión, el tribunal habrá de tener en cuenta si el usuario ha puesto a disposición o difundido un volumen apreciable de obras.

La utilidad de esta diligencia preliminar regulada en el ordinal 11.º reside en que, en el marco de un proceso civil para la protección de los derechos de propiedad intelectual, desvirtúa el presunto anonimato que proporciona Internet permitiendo conocer la identidad de quien actuó tras una dirección IP. No obstante, esto plantea una serie de problemas adicionales, como el hecho de sea necesario el tratamiento de un dato de carácter personal, la necesidad de saber a qué prestador de servicios solicitar la información o la posibilidad de que no coincida el titular de la línea con el autor material de las infracciones.

Conscientes de que todas estas circunstancias pueden dificultar el recurso a la diligencia del art. 256.1.11.º de la LEC, el objetivo del presente trabajo es clarificar las cuestiones esenciales de su régimen jurídico. Para ello, en primer lugar, se intenta justificar la oportunidad de limitar la solicitud de la diligencia preliminar al titular de los derechos infringidos –solicitante de la diligencia-; en segundo lugar, se expone quién será en cada caso concreto el prestador de servicios que habrá de comunicar los datos del usuario –sujeto pasivo de la diligencia-; en tercer lugar, se interpretan los requisitos que ha de reunir la conducta del infractor evitando que la disposición quede vacía de contenido –usuario a identificar mediante la diligencia-; y, finalmente, se incide en el uso de los datos proporcionados y el posible carácter reservado de las actuaciones –límites a la información obtenida con la práctica de la diligencia-.

2. Solicitante y sujeto pasivo de la diligencia preliminar del art. 256.1.11.º de la LEC

2.1. El titular de derechos de propiedad intelectual como único legitimado para solicitar la diligencia preliminar del art. 256.1.11.º

El art. 256.1.11.º de la LEC atribuye legitimación activa para solicitar la diligencia preliminar únicamente al "titular de un derecho de propiedad intelectual que pretenda ejercitar una acción por infracción del mismo". Destaca la limitación que introduce esta diligencia respecto de los legitimados para su solicitud, haciendo uso de una redacción que nos obliga a cuestionar si cabe entender en sentido amplio la referencia al titular de derechos o, por el contrario, si debe restringirse exclusivamente a este sujeto.

La primera interpretación implicaría sostener, en relación con esta diligencia preliminar, la legitimación activa prevista para el resto de diligencias en materia de propiedad intelectual –conforme a los ordinales 7.º, 8.º y 10.º del art. 256.1-, de modo que, además del titular de los derechos, podrían solicitar los datos sobre el usuario tanto los cesionarios en régimen de exclusividad como las entidades de gestión colectiva. En cambio, los dos grupos de sujetos indicados quedarían excluidos si realizamos una interpretación literal de la norma tal y

como ha sido aprobada por nuestro legislador –esto es, si restringimos únicamente al titular del derecho infringido la posibilidad de solicitar esta diligencia-.
Siendo el objetivo de la diligencia preliminar del ordinal 11.º hacer posible el ejercicio de las acciones de los arts. 138 y ss. de la LPI, todos los sujetos activamente legitimados deberían poder solicitar los datos del usuario contra quien va a dirigirse la demanda (MONTESINOS, 2015, p. 55). Ayuda a defender esta idea el hecho de que, de no ser así, se generaría una situación de desigualdad no solo en función de quien sea el futuro demandante, sino también respecto del hipotético demandado como responsable de la infracción. Lo indicado es debido a que, conforme al art. 256.1.10.º de la LEC, la identidad del prestador presunto infractor podría ser requerida por cualquiera que ostentara legitimación activa[7], mientras que según el art. 256.1.11.º de la LEC la identificación del usuario únicamente sería posible a petición del titular del derecho de autor, afín o conexo presuntamente infringido.

En principio, es posible pensar que no hay motivos para introducir esta distinción entre la diligencia preliminar del ordinal 10.º y la del ordinal 11.º; sin embargo, es cierto que averiguar la identidad del usuario exige realizar un tratamiento previo de un dato personal como es su dirección IP[8]. Como se expone a continuación, a partir de los números que identifican el protocolo de Internet podrá obtenerse el nombre, apellidos y dirección de quien ha contratado la conexión desde la que se cometen las infracciones, por lo que la legitimación restringida al titular del derecho infringido podría contribuir a respetar que la misma fuera objeto de un tratamiento individualizado y manual, evitando la monitorización de IPs a gran escala, mediante la realización de un tratamiento automatizado cuya legalidad resulta cuestionable.

a. Las diferencias entre el tratamiento manual e individualizado y el tratamiento monitorizado y a gran escala de direcciones IP

Para proporcionar mayor claridad a nuestra exposición deviene necesario concretar las diferencias existentes entre el tratamiento manual e individualizado y el tratamiento monitorizado y a gran escala de las direcciones IP, a tal efecto, los programas de intercambio entre pares representan el modelo de explotación ilícita que mejor permite ilustrar en qué consiste cada una de las distintas formas de tratamiento.

> El modelo de explotación ilícita basado en el intercambio mediante redes de pares –también denominado intercambio P2P por la terminología inglesa *peer to peer* (de igual a igual)-, se caracteriza por que la descarga de contenidos protegidos se articula previa instalación de un programa de ordenador (*software* P2P) que permite, a partir de un enlace (link), embeber el archivo desde los dispositivos de los usuarios que están conectados a la red de pares[9].

Lo indicado se justifica por la habitual configuración de los *softwares* P2P, caracterizados

[7] A propósito de la legitimación activa para ejercer las acciones reguladas en los arts. 138 y ss. de la LPI cuando los derechos de propiedad intelectual son infringidos en Internet, véase LLOPIS (2018b, Capítulo II, Sección I).

[8] Sobre las direcciones IP, véase MARTÍNEZ (2006, p. 5); PUERTO (2015, pp. 27 y 28).

[9] Para una exposición detallada sobre esto, véase LLOPIS (2018a, pp. 11 y ss.).

por dejar a la vista del resto de usuarios los números que identifican los protocolos de Internet desde los que están siendo compartidos los archivos que se descargan, y, con ello, determina que el principal uso de la diligencia preliminar regulada en el art. 256.1.11.º de la LEC sea averiguar la identidad de los pares que están poniendo obras a disposición del público a través de estos programas.

Así, para conocer de forma manual e individualizada la dirección IP de quien comete el ilícito será necesario seguir tres pasos. Primero, el titular del derecho debe conectarse a la red P2P y buscar la obra de su titularidad. Segundo, ha de anotar la IP desde la que su obra está siendo puesta a disposición del público; asimismo, puesto que se trata de direcciones dinámicas, debe tomar nota del día y hora en que el contenido protegido es objeto de explotación ilícita. Tercero, y a efectos probatorios, habrá de descargar los archivos para demostrar que se trata de su obra[10].

> En el asunto *Breyer*, el TJUE distingue las IPs *dinámicas*, definiéndolas como direcciones "provisionales, que se atribuyen a cada conexión a Internet y que son sustituidas en conexiones posteriores", de las direcciones IP *estáticas*, "invariables y que permiten la identificación permanente del dispositivo conectado a la red" [STJUE *Breyer*, 2.ª, 19.10.2016 (C-582/14; MP: A. Rosas), especialmente, punto 36].

Por su parte, monitorizar implica recurrir a aparatos o programas que permitan recabar, de forma automática y en grandes cantidades, información sobre las direcciones IP desde las que se infringen los derechos de propiedad intelectual. Este mecanismo puede ser utilizado por parte de los cesionarios, de las entidades de gestión o de terceros profesionales con quienes estos hayan contratado a fin de averiguar las direcciones desde las que se cometen los ilícitos[11], y, de este modo, conocer las direcciones IP de todos aquellos usuarios que están compartiendo obras a través de un programa P2P.

> En el asunto que dio lugar a la sentencia *Promusicae* del TJUE, la asociación española obtuvo las direcciones IP de los usuarios que estaban compartiendo contenidos a través del programa de intercambio *Kazaa* previa monitorización de la búsqueda, en otras palabras, no descubrió las IPs desde las que se cometían los ilícitos previo tratamiento manual e individualizado de cada una de las obras puestas a disposición del público [STJUE *Promusicae*, Gran Sala, 29.01.2008 (C-275/06;

[10] Son varios los autores que han explicado, en relación con los programas de intercambio entre pares, el modo de obtener de forma manual la dirección IP desde la que se ponen a disposición del público los contenidos protegidos, entre otros, GONZÁLEZ GOZALO (2008, pp. 17 y 18); GARROTE (2011, pp. 35 y 36); LÓPEZ (2016, pp. 368 y 369).

[11] Como explica LÓPEZ (2016, p. 369), "En la práctica, los titulares de derechos no realizan estas tareas de investigación por sí mismos, sino que recurren a empresas especializadas, que utilizan potentes equipos informáticos y programas especialmente diseñados para recoger información relativa al tráfico de contenidos a través de redes P2P con el fin de poder identificar a quienes infringen los derechos de autor a gran escala. Estas aplicaciones, conocidas como *webs robots* o simplemente *bots*, se introducen en las redes P2P haciéndose pasar por un usuario más y realizan de manera incesante y a mucha más velocidad de lo que podría hacer un ser humano peticiones de archivos que contengan contenidos protegidos por derechos de autor, incorporando a una base de datos la información relevante de aquellos usuarios que ofrecen dichos archivos, básicamente la dirección IP, la fecha y hora de conexión y una muestra de los contenidos descargados".

MP: J. Malenovský)].

b. Los límites a la legitimación para solicitar la diligencia del ordinal 11.º como forma de alcanzar el justo equilibro entre derechos fundamentales

Las características que distinguen el tratamiento manual del tratamiento monitorizado nos conducen a concluir que la reserva exclusiva de legitimación a favor del titular del derecho infringido podría haber sido prevista para conseguir, en relación con la diligencia destinada a obtener datos sobre el usuario, el equilibrio entre dos grupos de derechos fundamentales: de una parte, la tutela judicial efectiva y la propiedad intelectual –conforme a los arts. 47 y 17 de la CEDF, respectivamente-, y, de otra parte, la intimidad y la protección de datos personales –de acuerdo con los arts. 7 y 8 de la CEDF-; siendo este el modo elegido por el legislador español para respetar la jurisprudencia *Promusicae*, *LSG* y *Bonnier* del TJUE [STJUE *Promusicae*, Gran Sala, 29.01.2008 (C-275/06), puntos 61 a 70 (especialmente, punto 68); Auto *LSG*, 8.ª, 19.02.2009 (C-557/07; MP: J. Malenovský), puntos 26 a 29 (especialmente, punto 29); STJUE *Bonnier*, 3.ª, 19.04.2012 (C-461/10; MP: J. Malenovský), puntos 55 a 60 (especialmente, punto 56)].

En estas sentencias, respondiendo a cuestiones prejudiciales sobre la posibilidad de comunicar datos del internauta que utiliza determinada dirección IP a efectos de su identificación en el marco de un proceso civil, el Tribunal de Luxemburgo considera que los Estados Miembros, al adaptar su ordenamiento jurídico interno a las Directivas de la Unión, deben garantizar *un justo equilibrio* entre los derechos fundamentales protegidos por la Unión Europea; asimismo, mantiene que los órganos jurisdiccionales, cuando interpreten su legislación interna, deben respetar los principios generales de este ordenamiento supranacional, entre ellos, el principio de proporcionalidad.

> En el asunto *Bonnier*, para emitir un requerimiento judicial de comunicación de datos a partir de una dirección IP en el marco de un proceso civil, la ley sueca exigía tres requisitos: la existencia de indicios reales de infracción del derecho de propiedad intelectual, la necesidad de los datos para facilitar la investigación del ilícito y que el fin perseguido por el requerimiento fuera más importante que el daño que su práctica causaba al afectado o a otros intereses. El TJUE consideró que Suecia no solo había previsto una normativa que garantizaba el justo equilibrio entre los distintos derechos fundamentales que pueden verse afectados, sino que, además, permitía a sus tribunales nacionales ponderar, atendiendo a las circunstancias del caso concreto y respetando el principio de proporcionalidad, los distintos intereses contrapuestos [STJUE *Bonnier*, 3.ª, 19.04.2012 (C-461/10), puntos 58 y 59].

Por ello, el establecimiento de un régimen jurídico diferente en materia de legitimación activa en función de las características del infractor cuya identidad se pretende conocer –prestador de servicios o usuario- podría estar justificado por dos razones vinculadas a alcanzar este *justo equilibrio*: la necesidad de tratar las direcciones IP de manera individualizada –en cuanto han sido consideradas datos de carácter personal-, y el hecho de que la identidad del usuario no sea información general de fácil acceso para los internautas –como sí sucede respecto de los prestadores de servicios titulares de páginas web-.

- Las direcciones IP como datos de carácter personal y la necesidad de que sean objeto de tratamiento lícito.

A efectos de averiguar la identidad del usuario es necesario que, previamente, el solicitante de la diligencia disponga de su dirección IP, lo que supone llevar a cabo un tratamiento de datos personales; en consecuencia, puede existir cierto interés en que este tratamiento, si bien legalmente permitido, se realice de forma individual respecto de cada derecho por su propio titular. No obstante, mantener esta afirmación exige demostrar dos extremos: que las direcciones IP son datos de carácter personal y que el propio art. 256.1.11.º de la LEC es habilitación legal suficiente para su tratamiento.

Acerca de si las direcciones IP debían ser consideradas datos de carácter personal al ser tratadas por terceros distintos a los prestadores de servicios de acceso, la doctrina ha mantenido opiniones contrapuestas, siendo la postura mayoritaria la de atribuirles la condición de datos personales[12]. También nuestros órganos jurisdiccionales han tenido la ocasión de pronunciarse al respecto, confirmando el propio TS en casación el carácter de datos personales de las direcciones IP –en el sentido del art. 3.a) de la Ley Orgánica de Protección de Datos[13] (en adelante LOPD)-, puesto que contienen información de personas físicas identificadas o identificables: "no cabe duda que, a partir de la dirección IP puede identificarse directa o indirectamente la identidad del interesado, ya que los proveedores de acceso a internet tienen constancia de los nombres, teléfono y otros datos identificativos de los usuarios a los que han asignado las particulares direcciones IP" [STS, 3.ª, 3.10.2014 (Roj: STS 3896/2014; MP: José María del Riego Valledor), FJ 4º].

Asimismo, el TJUE ha confirmado a través de la sentencia *Breyer* que, incluso cuando son terceros quienes tratan esta información, las direcciones IP constituyen datos de carácter personal. A este propósito, los jueces de Luxemburgo han señalado que respecto del *proveedor de servicios de medios en línea* –esto es, un tercero distinto del intermediario que facilita el acceso- la dirección IP constituye un dato personal "cuando este disponga de medios legales que le permitan identificar a la persona interesada" [STJUE *Breyer*, 2.ª, 19.10.2016 (C-582/14), punto 49]. Lo que conduce al TJUE a esta conclusión es que el tercero que ha obtenido la dirección IP dispone de instrumentos que pueden utilizarse *razonablemente* para identificar al internauta mediante la ayuda de otros agentes, en particular, de la autoridad competente y del proveedor de acceso a Internet [STJUE *Breyer*, 2.ª, 19.10.2016 (C-582/14), especialmente, puntos 45 a 49]. De este modo, el tribunal confirma lo que ya sostuvo en el asunto *Scarlet* sobre las direcciones IP, ampliando su campo de aplicación más allá de los prestadores de servicios de acceso [STJUE *Scarlet*, 3.ª, 24.11.2011 (C-70/10; MP: J. Malenovský), especialmente, punto 51].

[12] Destaca la exposición al respecto realizada por GARROTE (2011, pp. 37 a 50), defendiendo su postura contraria a atribuir la condición de datos de carácter personal a las direcciones IP (especialmente, pp. 47 y ss.).

[13] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, *B.O.E.*, núm. 298, de 14 de diciembre de 1999.

Tomando como referencia la jurisprudencia del TJUE en respuesta a la cuestión prejudicial del asunto *Breyer*, el mismo carácter de datos personales debemos conceder a las direcciones IP cuando el recurso al art. 256.1.11.º de la LEC permite obtener la identidad de quien contrató la conexión a Internet. La afirmación realizada se fundamenta en el hecho de que el titular del derecho infringido es un tercero que, con la colaboración del Juzgado de lo Mercantil –quien ordena la práctica de la diligencia- y del prestador de servicios de acceso –quien proporciona la información del usuario con quien mantiene o ha mantenido una relación contractual- puede identificar a la persona que ha actuado en Internet tras esa dirección IP.

En relación con esta jurisprudencia, debemos recordar que el art. 3.a) de la LOPD ya definía los datos personales como "cualquier información concerniente a personas físicas identificadas o identificables", mientras que el art. 2.a) de la recientemente derogada Directiva 95/46[14] especificaba "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación". Asimismo, lo anterior se ha visto reforzado por el art. 4 del nuevo Reglamento General de Protección de Datos[15] (RGPD), que incluye en el concepto *datos personales* toda la información no solo de las personas físicas identificadas, sino también de las personas físicas identificables. En este sentido, los números de la dirección IP dinámica, junto a la fecha y hora en que tuvo lugar la actividad en la Red, constituyen los medios que permiten determinar, previa colaboración del prestador de servicios de acceso por orden del tribunal competente, la identidad de la persona que ha contratado la conexión a Internet.

En cuanto a la existencia de habilitación legal suficiente que nos permita afirmar que estamos ante un tratamiento lícito, si bien el art. 256.1.11.º de la LEC no hace referencia expresa a las direcciones IP, consideramos que esta norma permite que el prestador de servicios aporte los datos necesarios para identificar al usuario infractor a partir de la información que le proporciona el titular del derecho infringido –la dirección IP desde la que se realizaron los actos de puesta a disposición o de difusión directa o indirecta de su obra, así como la fecha y la hora en que los mismos tuvieron lugar-. Para ello, el tratamiento de la dirección IP por parte del titular del derecho infringido deviene imprescindible puesto que, de lo contrario, carece de medios para fundamentar la diligencia que solicita: designar al presunto infractor cuyo nombre y apellidos necesita conocer a efectos de presentar la demanda, así como acreditar que existe adecuación respecto de la finalidad perseguida y que concurre justa causa e interés legítimo para pedir

[14] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *D.O.C.E.*, n.º L 281, de 23 de noviembre de 1995, pp. 31 a 50.

[15] Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), *D.O.U.E.*, n.º L 119, de 4 de mayo de 2016, pp. 1 a 88.

la diligencia.

> Estas exigencias, impuestas en virtud del art. 258.1 de la LEC, impiden solicitar en abstracto la diligencia preliminar dirigida averiguar la identidad del usuario; en consecuencia, no cabe realizar peticiones genéricas ni desproporcionadas, siendo necesario demostrar tanto su intención de perseguir en vía civil estos ilícitos como el carácter imprescindible de la información para poder iniciar este proceso (GARCÍA y VENDRELL, 2013, p. 5).

De esta forma, entendemos que el subapartado 11.º contiene la previsión legal necesaria para el tratamiento de un dato de carácter personal, como es la dirección IP, en el marco de las infracciones de derechos de propiedad intelectual cometidas en Internet. Así, delimitando las características que ha de reunir la infracción y restringiendo la solicitud de la diligencia al titular del derecho infringido, esta norma jurídica contiene una excepción al necesario consentimiento del interesado para el tratamiento de sus datos que respeta las exigencias impuestas por el TC español[16]: se trata de una limitación al derecho fundamental que es proporcionada, está fundada en una previsión legal con base constitucional y expresa con precisión todos los presupuestos materiales de la medida limitadora [STC, Pleno, 30.11.2000 (STC 292/2000, *B.O.E.* n.º 4, 4.01.2001; MP: Julio Diego González Campos), FJ 16º]. En consecuencia, podemos afirmar que se respeta lo establecido en el art. 6.1 de la LOPD: en defecto de consentimiento del afectado, el tratamiento habrá de ser autorizado por la ley[17].

> A propósito de la existencia de un consentimiento tácito e inequívoco –como permite y exige la LOPD-, el TS ha mantenido: "A la hora de analizar si existe un consentimiento tácito del titular de los datos para su tratamiento, debe tenerse en cuenta la finalidad de los actos de los que se deduce esa voluntad, que en este caso están encaminados a operar en las redes P2P, sin que sea razonable deducir de dicho propósito el consentimiento para el tratamiento de los datos […] El hecho de que un usuario de red P2P conozca que su dirección IP es visible y puede ser conocida, no significa que acepte de forma inequívoca su uso y tratamiento por terceros, ni que consienta de forma específica el tratamiento de sus datos […] Por tanto, no puede equipararse el conocimiento por el titular de que su dirección IP es visible en las redes P2P, con su consentimiento para su tratamiento automatizado junto con otros datos de su tráfico" [STS, 3.ª, 3.10.2014 (Roj: STS 3896/2014), FJ 6º].

Adicionalmente, según el RGPD –y al margen de que el art. 256.1.11.º de la LEC constituya habilitación legal suficiente-, el tratamiento de datos será lícito si deviene necesario para satisfacer intereses legítimos del responsable del mismo o de un tercero, siempre que sobre estos no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de sus datos personales. Esta balanza, impuesta por el art. 6.1.f)

[16] Para un análisis detallado sobre nuestra doctrina constitucional a propósito de "La legitimidad de la injerencia en el derecho a la protección de datos" en relación con la tutela de los derechos de propiedad intelectual, véase el estudio realizado por DURÁN (2011, pp. 5 y ss.).

[17] Antes de la Ley 21/2014, LETAI (2012, p. 189) planteaba, ante la falta de habilitación expresa, la existencia de una habilitación "tácita, en el derecho constitucional a la tutela judicial efectiva ya que, mientras en España no se pueda formular una demanda […] contra una dirección IP, será de primera necesidad el obtener los datos del eventual infractor […] se podría incluso entender que hablamos de habilitaciones especificas si nos remitimos a las diligencias preliminares del artículo 256.1.7º de la LEC".

del RGPD, puede convertirse en un argumento más a favor de limitar la legitimación activa para pedir la diligencia preliminar al titular del derecho de propiedad intelectual infringido, quien presentará su solicitud tras realizar un tratamiento manual e individualizado de la dirección IP como dato de carácter personal[18].

- Las dificultades de acceder a la información que permite identificar al usuario presunto infractor.

El acceso a la información de las dos categorías de infractores cuya identidad puede obtenerse mediante las diligencias preliminares –prestadores de servicios o usuarios- presenta cierta asimetría. Estas diferencias a la hora de obtener los datos que permitan identificarles también pueden justificar que se restrinja la legitimación activa para solicitar la diligencia que permite conocer el nombre y apellidos del usuario presunto infractor.

Así, el prestador de servicios al que se refiere la petición de diligencia preliminar realizada con base en el subapartado 10.º está obligado, por el art. 5.1 de la Directiva 2000/31[19], a permitir un fácil acceso a la *información general* sobre el mismo[20] –que incluye, entre otros, los datos necesarios para demandarle: nombre, dirección y un medio de contacto-. Estos datos deberán constar en la página web titularidad del prestador de servicios, lo que podría reducir la aplicación práctica de la diligencia preliminar regulada en el art. 256.1.10.º de la LEC –si bien es cierto que únicamente están sujetos a esta exigencia aquellos prestadores de servicios que tengan su establecimiento permanente en el territorio de un Estado Miembro de la Unión Europea-.

A lo indicado debe añadirse que, para la solicitud de información sobre el prestador, no es necesario realizar ningún tratamiento previo de sus datos personales –basta con conocer su sitio de Internet y la persona que le presta servicios de alojamiento, de pago electrónico o le retribuye a cambio de explotar sus espacios publicitarios-, de ahí que quepa entender que otros legitimados activos, diferentes al titular del derecho de propiedad intelectual infringido, puedan pedir al Juzgado de lo Mercantil la práctica de la diligencia –estos serían los cesionarios en régimen de exclusividad y las entidades de gestión-.

---

[18] También con carácter previo a la reforma de 2014, GONZÁLEZ GOZALO (2008, pp. 52 a 56) mantenía que del art. 6.1 de la LOPD "se desprende que el derecho de protección de datos ha de ceder cuando sea necesario para lograr un fin legítimo perseguido por la ley" [p. 52], y, a partir de esta premisa consideraba como fines legítimos legalmente reconocidos la protección de la propiedad intelectual y el derecho fundamental a la tutela judicial efectiva, para cuyo ejercicio el titular necesita conocer la identidad del infractor, algo que solo podrá obtener a partir de su dirección IP y de otros datos relativos a la infracción.

[19] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), *D.O.U.E.*, n.º L 178, de 17 de julio de 2000, pp. 1 a 16.

[20] Esta norma ha sido transpuesta a nuestro ordenamiento jurídico mediante el art. 10.1 de la Ley de Servicios de la Sociedad de la Información (en adelante LSSI) [Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, *B.O.E.*, núm. 166, de 12 de julio de 2002].

c. Conocer la dirección IP desde la que se cometen los ilícitos como requisito para solicitar al proveedor de acceso que identifique al usuario

A pesar de lo que ha sido señalado en los apartados precedentes, *a priori*, averiguar la dirección IP desde la que se cometen los ilícitos no es una tarea complicada –especialmente cuando el modelo de explotación utilizado son los programas P2P[21]-; sin embargo, el titular del derecho de propiedad intelectual infringido puede tener dificultades al intentar descubrir la IP del usuario –debido a la falta de medios y de conocimientos-. Esta dificultad se incrementa cuando debe demostrar ante el Juzgado de lo Mercantil que el usuario comparte un *volumen apreciable de obras*, lo que no solo implica probar que está poniendo a disposición o difundiendo contenidos cuya titularidad ostenta el solicitante de la diligencia preliminar, sino, adicionalmente, demostrar que realiza las mismas actividades con contenidos que pertenecen a otros titulares de derechos.

No obstante, ha de entenderse imprescindible que quien pide la diligencia disponga de la dirección IP antes de dirigirse al prestador de servicios de acceso para que le comunique los datos de quien actuó tras ese código numérico –no sucede lo mismo, como se expone más adelante, cuando la diligencia preliminar tenga como sujeto pasivo al prestador de servicios de alojamiento 2.0-. En consecuencia, debemos mantener que no cabe solicitar al proveedor de acceso la IP desde la que se están infringiendo los derechos de propiedad intelectual –es decir, la dirección a partir de la cual se ponen a disposición o se difunden los contenidos protegidos-.

La postura defendida encuentra su fundamento en el hecho de que, para facilitar esa información, el prestador debería controlar las comunicaciones que se llevan a cabo haciendo uso de su red, una actividad de control que deviene contraria, de una parte, al tipo de datos que estos prestadores tienen la obligación de conservar –que excluye, conforme al art. 3.2 de la Ley 25/2007[22], aquellos que revelen el contenido de las comunicaciones[23]-; y, de otra parte, a la prohibición de supervisión general de las transmisiones –prevista en el considerando 47 y en el art. 15.1 de la Directiva 2000/31[24], y

[21] Afirman la facilidad con que se puede obtener la dirección IP en el caso de los programas de intercambio entre pares, GONZÁLEZ DE ALAIZA CARDONA (2004, p. 60); LETAI (2012, p. 187); LÓPEZ (2016, p. 368).

[22] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, *B.O.E.*, núm. 151, de 19 de octubre de 2007.

[23] Como indican PEGUERA y TARRÉS (2010, p. 343), "Los datos que los operadores deberán conservar y, en su caso, ceder son exclusivamente los datos de tráfico y localización, así como los datos relacionados que permitan identificar al abonado o usuario registrado. En cambio, no es objeto de conservación el contenido de las comunicaciones electrónicas ni tampoco la información consultada utilizando la Red".

[24] El art. 15.1 de la Directiva 2000/31 establece "Los Estados Miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto a los servicios contemplados en los artículos 12, 13 y 14" –entre los que se incluyen los proveedores de acceso-. Si bien no hay ninguna disposición en la LSSI que de manera expresa haya transpuesto esta norma de derecho de la Unión, los efectos propios de las Directivas exigen que la misma sea respetada en el ordenamiento jurídico nacional, de modo que queda prohibido imponer a estos prestadores una

confirmada por el Tribunal de Luxemburgo respecto de los proveedores de acceso en el asunto *Scarlet* [STJUE *Scarlet*, 3.ª, 24.11.2011 (C-70/10), especialmente, puntos 39 y 40]-.

Es interesante recordar que, en el litigio principal que dio origen a la jurisprudencia *Scarlet*, se pretendía obligar al prestador de servicios de acceso a establecer un *sistema de filtrado* de todas las comunicaciones electrónicas realizadas a través de su red para, de esta forma, controlar el intercambio de contenidos protegidos por la propiedad intelectual que tuviera lugar utilizando su servicio –especialmente, mediante redes de pares-. Se trataba de una supervisión prevista para hacer frente a cualquier lesión, ilimitada en el tiempo y relativa a todas la obras presentes y futuras, por lo que el TJUE entendió que dicha medida no era respetuosa con la exigencia de garantizar un justo equilibrio entre la protección de la propiedad intelectual y la libertad de empresa de los operadores de Internet. Asimismo, también consideraron los jueces de Luxemburgo que, un sistema de tales características, podría vulnerar derechos fundamentales de los usuarios del proveedor de acceso, como la protección de datos de carácter personal y la libertad de recibir o comunicar informaciones [STJUE *Scarlet*, 3.ª, 24.11.2011 (C-70/10), especialmente, puntos 47 a 53].

Lo expuesto en los párrafos precedentes nos permite concluir que no es posible, ni siquiera mediante requerimiento adoptado por el tribunal competente para decidir sobre la diligencia, solicitar al prestador de servicios de acceso que verifique y facilite las direcciones IP desde las que se han cometido los ilícitos, ya que esto únicamente podría conseguirlo mediante un *sistema de filtrado* de las informaciones transmitidas. Por tanto, el titular del derecho infringido que pretenda obtener la identidad del usuario infractor deberá conocer la dirección IP y proporcionársela al proveedor de acceso como requisito para solicitarle los datos de la persona que contrató esa conexión a Internet.

2.2. El sujeto pasivo de la diligencia preliminar del art. 256.1.11.º de la LEC

Conforme a lo establecido por el art. 256.1.11.º de la LEC, los prestadores de servicios de la sociedad de la información son los únicos sujetos pasivos a quienes puede dirigirse la petición de datos sobre el usuario infractor. Es necesario, en todo caso, que el usuario que se pretende identificar haya sido cliente de los servicios prestados por el sujeto requerido dentro del margen de los últimos doce meses, puesto que los datos que se solicitan habrán de extraerse de la relación contractual que el prestador mantenga o haya mantenido con el presunto infractor. A este propósito, resulta irrelevante que la relación entre el prestador y el usuario persista cuando se solicite la diligencia, así como el tiempo que la misma haya durado.

---

obligación de supervisión general respecto del contenido que se transmite por su red para poder facilitar las direcciones IP desde las que se ofrecen obras protegidas. En este sentido, señala GARROTE (2014, p. 22) "Hay que acudir por tanto a la interpretación conforme del Derecho nacional con el comunitario y a la jurisprudencia del TJUE para defender la inexistencia de una obligación general de supervisión en España".

A diferencia de lo previsto en la diligencia preliminar del ordinal 10.º[25], la LEC no impone para este supuesto que la información pueda extraerse a partir de los datos que el prestador conserve como resultado de la relación mantenida con el usuario; asimismo, tampoco excluye los datos que exclusivamente estuvieran siendo objeto de tratamiento por el prestador de servicios en cumplimiento de lo dispuesto en la Ley 25/2007. No obstante, en cuanto el sujeto pasivo coincide –un prestador de servicios de la sociedad de la información-, el origen de la información de que dispone se corresponde –el contrato celebrado con un cliente, en este caso, un usuario- y sus obligaciones son las mismas –ceder los datos al órgano competente en caso de indicios de comisión de delito grave- no hay motivos para excluir la necesidad de que también esta condición y esta excepción se mantengan respecto del prestador cuando se trate de facilitar los datos relativos a un usuario –esto es, se extiendan a la diligencia preliminar del art. 256.1.11.º de la LEC- (MONTESINOS, 2015, p. 57).

La solicitud de diligencias preliminares deberá designar como sujeto pasivo al prestador de servicios que pueda facilitar la información sobre el usuario, este será, en todo caso, un intermediario proveedor de acceso a Internet y/o un intermediario prestador de servicios de alojamiento. El recurso a uno u otro –o incluso a ambos- estará en función del modelo de explotación utilizado para cometer las infracciones, de la información de la que disponga el solicitante de la diligencia y de los datos que pueda facilitar el prestador de servicios requerido. En este sentido, podemos encontrarnos con dos situaciones distintas en función de si el titular del derecho de propiedad intelectual infringido dispone de la dirección IP utilizada para cometer los ilícitos.

a. El sujeto pasivo de la diligencia preliminar cuando el titular del derecho conoce los números de la dirección IP utilizada para infringir

En el momento de solicitar la diligencia preliminar, es posible que el titular del derecho de propiedad intelectual infringido conozca los números de la dirección IP del usuario presunto infractor. Esta situación será habitual cuando el modelo de explotación utilizado es el intercambio mediante redes de pares puesto que, como ha sido expuesto *supra*, el programa P2P que articula las descargas se caracteriza por hacer visibles al resto de usuarios los números que identifican los protocolos de Internet desde los que se comparten los archivos.
En el supuesto descrito, el prestador de servicios de acceso –definido en el art. 14 de la LSSI-, es quien deberá facilitar los datos del usuario de su servicio que, en un momento concreto –día y hora-, estaba actuando en Internet bajo esa dirección –siendo imprescindible concretar el momento exacto ya que, en estos supuestos, las IPs serán

[25] La referida disposición establece "Los citados prestadores proporcionarán la información solicitada, siempre que ésta pueda extraerse de los datos de que dispongan o conserven como resultado de la relación de servicio que mantengan o hayan mantenido con el prestador de servicios objeto de identificación, salvo los datos que exclusivamente estuvieran siendo objeto de tratamiento por un proveedor de servicios de Internet en cumplimiento de lo dispuesto en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones".

direcciones dinámicas-. El proveedor de acceso a Internet debe ser capaz de proporcionar esa información, puesto que, en virtud del art. 3.1.2.º.iii) de la Ley 25/2007, ha de conservar el nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección IP.

Ahora bien, no podemos descartar que, a partir de la configuración del *software* P2P, el titular de los derechos infringidos solo conozca el nombre o pseudónimo (*nickname*) mediante el cual el infractor ha actuado en la Red. De ser el caso, en cuanto el responsable del programa de intercambio no es un prestador de servicios de la sociedad de la información, existen dudas a propósito de si se le podrá pedir que facilite los datos necesarios para identificar al usuario que pone obras a disposición del público desde su carpeta compartida –su IP u otras informaciones de las que disponga-. Una interpretación en sentido estricto del art. 256.1.11.º de la LEC nos conduce a afirmar que esto no será posible, puesto que los responsables de este *software* no pertenecen a la categoría de los sujetos pasivos previstos en la referida disposición.

> La excepción a lo que ha sido apuntado la constituyen los programas P2P centralizados –programas P2P de primera generación-, caracterizados por ofrecer instrumentos de búsqueda a los contenidos protegidos, lo que permite calificarlos de intermediarios e incluirlos en la categoría de prestadores de servicios de la sociedad de la información regulada en el art. 17 de la LSSI (DE NOVA 2010, pp. 308 y 309); (SÁNCHEZ, 2007, p. 195). No obstante, el uso de estos programas ha decaído –siendo sustituidos por los que presentan una estructura descentralizada-, de ahí que en la actualidad tenga escasa relevancia la posibilidad de considerarlos prestadores de servicios.

b. El sujeto pasivo de la diligencia preliminar cuando el titular del derecho desconoce los números de la dirección IP utilizada para infringir

Más compleja es la situación que se produce cuando el titular del derecho de propiedad intelectual infringido no dispone de la dirección IP del usuario, sino que únicamente puede acceder su *nickname*. Esto será frecuente cuando el usuario pone a disposición o difunde contenidos desde una página web en formato 2.0 –es decir, cuando actúa como proveedor de contenidos en páginas web que son titularidad de un tercero, p. ej., en redes sociales o en foros- ya que, a diferencia de lo que sucede con las redes de pares, la dirección IP no suele ser visible al público. En este caso la información relativa al usuario deberá solicitarse al alojador 2.0 –una categoría de prestador de servicios de alojamiento o de almacenamiento de datos de los regulados en el art. 16 de la LSSI-[26].

En principio, el titular de la web 2.0 que presta servicios de alojamiento deberá contar con un registro de su sitio de Internet que le permita conocer, como mínimo, el momento –día y hora- en que los contenidos fueron puestos a disposición del público por uno de sus usuarios y la IP desde la que se realizaron esas actuaciones. Este tratamiento de datos lo

[26] El término alojador 2.0, utilizado para designar al titular de las páginas web donde son los usuarios quienes ponen a disposición los contenidos, fue acuñado por nuestros órganos jurisdiccionales en el asunto *Telecinco c. Youtube* [SJM Madrid, Sec. 7.ª, 20.09.2010 (Roj: SJM M 84/2010; MP: Andrés Sánchez Magro); SAP Madrid, Civil Sec. 28.ª, 14.01.2014 (Roj: SAP M 4/2014; MP: Ángel Galgo Peco)].

realiza el propio prestador de servicios de alojamiento 2.0, con carácter previo y sin que sea necesaria la existencia de una diligencia preliminar. Ahora bien, en todo caso, puesto que deviene imprescindible el registro en el sitio de Internet que este gestiona para poder publicar información, cabe presuponer que en la inscripción se exige al usuario que autorice la recogida y la utilización de sus datos de carácter personal –entre los que se incluye la dirección IP- por parte del alojador y como requisito para utilizar su sitio de Internet. De este modo, se obtiene el consentimiento del afectado, exigido por el art. 6.1 de la LOPD –así como el 6.1.a) del RGPD-, para que sea posible el tratamiento de sus datos personales.

La exigencia de mantener un registro de los contenidos que son puestos a disposición por terceros desde su sitio de Internet –que le permita, entre otros, dar respuesta a la diligencia del art. 256.1.11.º de la LEC- difiere, sustancialmente, del *sistema de filtrado* que se intentó imponer al prestador de servicios de alojamiento en el asunto *SABAM*, y que fue considerado contrario al derecho de la Unión por el Tribunal de Luxemburgo [STJUE *SABAM*, 3.ª, 16.02.2012 (C-360/10; MP: J. Malenovský)]. Esto es así puesto que, al pedir los datos sobre el usuario infractor, el propio solicitante de la diligencia es quien proporciona al alojador 2.0 la información que el *sistema de filtrado* le hubiera permitido conocer: le facilitará el nombre bajo el cual el usuario actúa en su plataforma –como único requisito para obtener la dirección IP desde la que este internauta está generando el tráfico- y, adicionalmente, los contenidos que han sido puestos a disposición –a fin de acreditar que hay indicios razonables que justifican la solicitud de la diligencia-.

A este propósito debemos recordar que, en el litigio principal que dio origen a la jurisprudencia *SABAM* se pretendía, mediante requerimiento judicial, ordenar a *Netlog* –plataforma de red social en la que los usuarios podían publicar, entre otros, contenidos protegidos por la propiedad intelectual- el establecimiento de un *sistema de filtrado* con el que identificara, entre la totalidad de archivos almacenados en sus servidores por los usuarios, aquellos que contuvieran obras o prestaciones protegidas, que concretara cuales estaban siendo puestos a disposición de forma ilícita y que bloqueara su comunicación pública. La petición realizada al órgano jurisdiccional suponía, en realidad, imponer a un alojador 2.0 la obligación de supervisar toda la información subida por sus usuarios para hacer frente a cualquier lesión, ilimitada en el tiempo y relativa tanto a las obras presentes como futuras.

El TJUE, en respuesta a la cuestión prejudicial planteada, entendió que la medida no podía garantizar el justo equilibrio entre, de una parte, el respeto de la propiedad intelectual y, de otra parte, la libertad de empresa de los prestadores de servicios y la protección de datos de carácter personal de los usuarios de Internet, así como su libertad de recibir y comunicar informaciones [STJUE *SABAM*, 3.ª, 16.02.2012 (C-360/10), puntos 44 a 51]. Sin embargo, como hemos defendido, cuando el titular de derechos es quien recaba la información sobre el usuario infractor: nombre que utiliza en su sitio de Internet y contenidos que comparte desde el mismo, estamos ante una situación diferente al sistema de filtrado que fue prohibido por el Tribunal de Luxemburgo.

Por último, si la única información que puede proporcionar el prestador de servicios de alojamiento titular de la web 2.0 son los números de la dirección IP de quien puso a disposición los contenidos, será necesario solicitar una segunda diligencia preliminar sobre la base del art. 256.1.11.º de la LEC –en esta ocasión, dirigida al proveedor de servicios de acceso-, a fin de que informe sobre el nombre, apellidos y dirección del cliente de su servicio que actuó en un determinado momento detrás de esa dirección IP. En caso contrario, el titular de los derechos infringidos podrá iniciar un proceso civil y ejercer las acciones de los arts. 138 y ss. a partir de los datos que le ha proporcionado el alojador 2.0.

3. El usuario cuya identidad se solicita sobre la base del art. 256.1.11.º de la LEC

La diligencia preliminar del art. 256.1.11.º de la LEC se establece con el propósito de identificar al usuario sobre el que concurren indicios razonables de que pone a disposición o difunde, de forma directa o indirecta, materiales protegidos por la propiedad intelectual; en consecuencia, su solicitud únicamente será posible cuando el usuario realiza una de estas dos actuaciones, quedando excluidos los actos de reproducción ilícitos. Adicionalmente, la LEC añade una serie de requisitos para solicitar la información que permita conocer la identidad del usuario: que los actos no puedan considerarse realizados por meros consumidores finales de buena fe y sin ánimo de obtener beneficios económicos y comerciales, así como la obligación de tener en cuenta el volumen apreciable de obras no autorizadas puestas a disposición o difundidas.

Regulada en el art. 20.2.i) de la LPI, la puesta a disposición es una modalidad de comunicación pública caracterizada por permitir, mediante procedimientos inalámbricos, que cualquier persona acceda a los contenidos desde el lugar y en el momento que elija –algo que se produce cuando el usuario ofrece al resto de internautas obras protegidas a través de un programa P2P o de una página web 2.0-. Por lo que respecta a la difusión, directa o indirecta, la misma no se corresponde con ninguno de los actos de explotación regulados en los arts. 18 a 21 de la LPI –siendo imposible incluirla en alguna de sus diferentes modalidades-. No obstante, en la medida en que el término *difundir* es sinónimo de *propagar* o *divulgar*[27], cabe pensar que la intención del legislador ha sido la de comprender en esta actividad la provisión de enlaces que dirigen a contenidos protegidos.

Si bien es cierto que el Tribunal de Luxemburgo ha interpretado que enlazar a contenidos protegidos constituye un acto de comunicación pública en su modalidad de puesta a disposición[28], no es menos cierto que para ello impone dos requisitos: que el enlace

[27] Así lo define el diccionario de la Real Academia Española en su tercera acepción: "Propagar o divulgar conocimientos, noticias, actitudes, costumbres, modas, etc.".

[28] El TJUE ha configurado el régimen jurídico de los enlazadores en materia de propiedad intelectual mediante las siguientes sentencias: STJUE *Svensson*, 4.ª, 13.02.2014 (C-466/12; MP: J. Malenovský); STJUE

conduzca a obras protegidas ampliando el público inicialmente considerado por el titular de derechos y que el enlazador tenga conocimiento del carácter ilícito del contenido al que dirige. El primero de los requisitos concurre en todo supuesto de piratería en Internet, puesto que la primera puesta disposición de la obra nunca fue autorizada por quienes ostentan derechos de propiedad intelectual sobre la misma; por su parte, el segundo requisito ha sido concretado por el TJUE estableciendo la presunción de que, si el enlace se proporciona con ánimo de lucro, el enlazador conocía, o debía conocer, que estaba conduciendo a obras publicadas de manera ilícita[29].

Ahora bien, cuando los enlaces son proporcionados por usuarios –haciendo uso para ello de páginas web en formato 2.0-, es habitual que estos carezcan de ánimo de lucro –el cual pertenecerá, en todo caso, al titular del sitio de Internet desde el que se ofrecen los hipervínculos-. Esta falta de ánimo de lucro determina que no pueda aplicarse la presunción *iuris tantum* de que quien facilitó el enlace sabía, o podía saber, la ilicitud del contenido enlazado, por lo que corresponde al titular del derecho infringido demostrar la concurrencia del conocimiento necesario para considerar que el usuario realizó un acto de comunicación pública no autorizado.

De este modo, será posible solicitar la diligencia dirigida a averiguar la identidad del usuario que enlaza a obras protegidas sin necesidad de demostrar que, en el supuesto concreto, se ha realizado un acto de puesta a disposición –es decir, que aun careciendo de ánimo de lucro, el usuario conocía o debía conocer la ilicitud del contenido enlazado-; esto es posible siempre que se justifique la petición de la diligencia preliminar en la idea de que el usuario, mediante su enlace, difunde directa o indirectamente contenidos protegidos por la propiedad intelectual.

3.1. La imposibilidad de solicitar la diligencia del ordinal 11.º para identificar al usuario que se limita a realizar actos de reproducción ilícitos

Como ha sido indicado en la introducción a este epígrafe, los actos de reproducción de contenidos protegidos quedan fuera del campo de aplicación de la diligencia preliminar del art. 256.1.11.º de la LEC, siendo este, en realidad, el acto de explotación ilícito que con mayor frecuencia cometen los usuarios. Por tanto, no será posible solicitar que sea identificado el internauta que se limita a descargar contenidos protegidos –ni siquiera cuando esta descarga se realice de forma masiva-; en consecuencia, salvo que se obtenga su identidad por otras vías, no podrán ejercerse contra él las acciones de los arts. 138 y ss. de la LPI y sus conductas ilícitas quedarán exentas de reproche civil. Esta circunstancia impide disuadir las conductas de aquellos usuarios que solo realizan actos de reproducción –en cuanto garantiza la preservación de su anonimato-, y, dado que no elimina la intención de seguir consumiendo materiales ilícitos, potencia que quienes obtienen beneficios

GS Media, 2.ª, 8.09.2016 (C-160/15; MP: M. Ilešič); STJUE *Stichting Brein II*, 2.ª, 14.06.2017 (C-610/15; MP: M. Ilešič).

[29] Para una exposición sobre el tratamiento jurídico de los enlaces en materia de propiedad intelectual a partir de las sentencias del TJUE, véase LLOPIS (2018a, pp. 13 y ss.).

económicos a partir de estas infracciones continúen buscando formas alternativas de proporcionar contenidos y de eludir su persecución.

Es importante incidir en que lo expuesto en el párrafo anterior ha de entenderse sin perjuicio de que se ejerza la acción de cese contra el intermediario proveedor de acceso –conforme al art. 138.IV de la LPI-, reclamándole que ponga fin al servicio prestado a la dirección IP desde la que se están descargando obras o prestaciones en grandes cantidades. Esto será posible sin necesidad de conocer el nombre y apellidos de quien actúa tras esa IP –en cuanto la legitimación pasiva respecto de la acción de cese corresponde al intermediario-, si bien los efectos de la interrupción del servicio sí que recaen sobre el usuario infractor –quien será, en realidad, un tercero interesado en el proceso civil- (LLOPIS, 2018b, Capítulo III, Sección I).

3.2. Los requisitos adicionales impuestos a la actividad del usuario infractor y la necesidad de interpretarlos de manera flexible

El art. 256.1.11.º de la LEC incorpora una serie de condiciones adicionales que debe reunir el usuario presunto infractor: de una parte, es necesario que se trate de actos que no puedan considerarse realizados por consumidores finales de buena fe y sin ánimo de obtener beneficios económicos; de otra parte, para la concesión de la diligencia se atenderá al volumen de obras y prestaciones que son facilitadas sin el preceptivo consentimiento de su titular, siendo necesario que se trate de un volumen *apreciable*. La existencia de estos requisitos ha de ser probada por el solicitante ante el tribunal competente ya que, de no ser así, no podrá imponerse al sujeto pasivo de la diligencia la obligación de proporcionar tales informaciones. En los siguientes apartados se analizan las exigencias que introduce la LEC para la concesión de esta diligencia preliminar, así como los problemas que plantea la identificación del usuario a partir de lo previsto en el ordinal 11.º.

a. Actos que no puedan considerarse realizados por meros consumidores finales de buena fe y sin ánimo de obtener beneficios económicos o comerciales

Para poder solicitar los datos que permitan identificar al usuario, el art. 256.1.11.º de la LEC impone como requisito que las actividades tipificadas –poner a disposición o difundir contenidos protegidos- no sean realizadas por meros consumidores finales de buena fe y sin ánimo de obtener beneficios económicos o comerciales. Si bien es cierto que esta condición introducida respecto de los usuarios limita el campo de aplicación de la diligencia, no es menos cierto que la mayor o menor amplitud de la restricción depende del modo en que se interprete la norma; a este propósito, debemos defender aquella interpretación que no vacíe de contenido la solución adoptada por el legislador español a fin de hacer frente a la laguna que existía en nuestro ordenamiento jurídico respecto de la identificación del usuario.

La redacción literal del art. 256.1.11.º establece "y mediante actos que no puedan considerarse realizados por meros consumidores finales de buena fe y sin ánimo de

obtención de beneficios económicos o comerciales"; se trata de una redacción que copia, para el subapartado 11.º, el texto introducido por la Ley 21/2014 respecto de la diligencia preliminar del art. 256.1.7.º de la LEC, reemplazando el antiguo requisito "actos desarrollados a escala comercial", por la exigencia de "actos que no puedan considerarse realizados por meros consumidores finales de buena fe y sin ánimo de obtención de beneficios económicos o comerciales".

La segunda conjunción *y* utilizada por el legislador en este fragmento del art. 256.1.11.º de la LEC para enlazar el concepto "meros consumidores finales de buena fe" con la actitud "sin ánimo de obtención de beneficios económicos o comerciales" puede ser interpretada de dos formas distintas.

Una primera interpretación consiste en considerar que la palabra *y* enlaza dos oraciones, por ello, la condición "sin ánimo de obtención de beneficios económicos o comerciales" va referida al sustantivo "actos"; en consecuencia, son dos las *conductas* que quedan excluidas del ámbito de la diligencia preliminar del ordinal 11.º, de una parte, los actos realizados por usuarios que son meros consumidores finales de buena fe y, de otra parte, los actos realizados por usuarios sin ánimo de obtener beneficios económicos o comerciales.

Una segunda interpretación implica reconocer que la finalidad del término *y* es unir dos complementos circunstanciales utilizados para caracterizar al sustantivo "consumidores finales"; de modo que son dos las características que ha de reunir el *consumidor final* para que no quepa ejercer una diligencia dirigida a averiguar su identidad: tener buena fe y carecer de ánimo de obtener beneficios económicos y comerciales.

Finalmente, debemos señalar que el recurso a la conjunción *y* al principio de la frase ("y mediante actos…") nos obliga a considerar la oración en su integridad como constitutiva de una única condición o exigencia. Por este motivo, debemos rechazar una tercera interpretación en la que la expresión "y sin ánimo de obtención de beneficios" represente, por sí misma, un requisito para que sea posible la concesión de la diligencia preliminar, y, en consecuencia, no esté influenciada por el sentido negativo de la oración en su conjunto ("no puedan considerarse realizados por meros consumidores finales de buena fe y sin ánimo de obtención de beneficios").

Esta última interpretación, que hemos descartado, facilitaría la utilización de la diligencia preliminar del subapartado 11.º, y, bajo nuestro punto de vista, debería haber sido el carácter concedido por el legislador español a la norma, puesto que permitiría su solicitud incluso frente a quienes ponen a disposición o difunden contenidos careciendo de ánimo de lucro, es decir, contra todos los usuarios ya que ninguno de ellos desarrolla una actividad económica –en cuanto son los proveedores de contenidos, esto es, una categoría de prestadores de servicios de la sociedad de la información, quienes ponen a disposición o difunden materiales en Internet realizando una actividad económica, en otras palabras, actuando con ánimo de obtener beneficios-. No obstante, la redacción dada al art. 256.1.11.º de la LEC nos obliga a descartar que hubiera podido ser esta la intención del legislador,

puesto que, de lo contrario, hubiera concedido otro orden y sentido a las frases que integran la mencionada disposición.

- La exclusión de dos tipos de conductas: las realizadas de buena fe y las realizadas sin ánimo de obtener beneficios económicos o comerciales (primera interpretación).

Si se interpreta el art. 256.1.11.º de la LEC en el sentido de que se trata de dos conductas distintas es necesario concretar en qué consiste cada una de ellas: las realizadas de buena fe y las que se llevan a cabo sin ánimo de obtener beneficios. A propósito de los actos realizados por meros consumidores finales de buena fe debemos destacar dos cosas. En primer lugar, existen dudas acerca de si cabe considerar como consumidor final al usuario que comparte contenidos en redes de pares, así como al que pone a disposición o difunde materiales protegidos a través de plataformas 2.0. En segundo lugar, y en todo caso, deviene difícil afirmar que este actúa con buena fe, puesto que se trata de un usuario que carece de la preceptiva autorización y es –o, al menos, todo consumidor medio informado debería ser- consciente de que, con su actividad, facilita que otros internautas disfruten de las obras de forma gratuita, y sin que el titular de los derechos perciba contraprestación alguna. A pesar de lo señalado, es cierto que la buena fe se presume, por tanto, corresponde al solicitante de la medida desvirtuar esta presunción ante el Juzgado de lo Mercantil[30].

Respecto de la segunda conducta, su exclusión implica que, para poder solicitar la diligencia preliminar, deberá acreditarse que el usuario realizó los actos tipificados con ánimo de obtener beneficios económicos o comerciales. Sin embargo, parece difícil distinguir este tipo de actos de los realizados "a escala comercial", máxime cuando el art. 256.1.8.º.II de la LEC, actualmente en vigor, define los actos desarrollados a escala comercial como "aquellos que son realizados para obtener beneficios económicos o comerciales directos o indirectos".

La situación existente deviene todavía más compleja si recordamos que el requisito "actos desarrollados a escala comercial" –ahora suprimido del ordinal 7.º, pero vigente en el 8.º del art. 256.1 de la LEC-, fue criticado por la doctrina; estas críticas defendían que en el art. 8.1.c) de la Directiva 2004/48 –transpuesto al ordenamiento jurídico nacional mediante estas disposiciones de la LEC-, la exigencia "a escala comercial" no era referida a las actividades ilícitas cometidas, sino a las características del servicio de la sociedad de la información a través del cual se llevaba a cabo la infracción (GONZÁLEZ GOZALO, 2008, pp. 47 y 48; GARROTE, 2011, pp. 54 a 56). Lo indicado nos lleva a concluir que, en realidad, carece de sentido seguir manteniendo un requisito equivalente a la expresión "a escala comercial" respecto de los usuarios, especialmente, cuando la propia Directiva prevé que tal exigencia sea aplicada al prestador del servicio utilizado para cometer la infracción.

[30] Por esta razón, CASTÁN (2016, p. 147) considera que "la solicitud de diligencias frente a los usuarios requerirá una carga extra de aportación argumental y probatoria en cuanto a los indicios que revelan que no estamos ante utilizaciones ingenuas, ocasionales, económicamente neutras, inocuas o anecdóticas de obras o prestaciones ajenas".

A lo indicado debe añadirse que quienes ponen a disposición del público o difunden contenidos protegidos son, fundamentalmente, dos categorías de sujetos: los usuarios o los proveedores de contenidos; la diferencia entre ambos, de acuerdo con lo establecido en la LSSI, radica en que los segundos desarrollan una actividad económica[31]. En consecuencia, la diligencia preliminar del ordinal 11.º estaría reservada para usuarios de Internet que, sin llevar a cabo una actividad económica –pues, de ser así, su condición sería la de proveedor de contenidos-, obtengan o tengan ánimo de obtener un beneficio económico o comercial –algo que parece difícil de imaginar- (LÓPEZ, 2016, p. 394; MINERO, 2015, p. 383).

Con base en lo que ha sido señalado, esto es, incluyendo los beneficios directos e indirectos, pero excluyendo los actos vinculados al desarrollo de una actividad económica, debe concretarse cuándo cabe entender que un usuario realiza actos con ánimo de obtener beneficios económicos o comerciales. Debemos rechazar que el usuario obtenga beneficios directos, ya que estos solo podrían proceder de las descargas realizadas por terceros e implicarían, en todo caso, el desarrollo de una actividad económica en calidad de proveedor de contenidos –agente que, dada su condición de prestador de servicios, es identificado mediante la diligencia preliminar regulada en el subapartado 10.º-.

Asimismo, si el beneficio económico indirecto se entiende como limitado, únicamente, a generar ingresos a partir de actividades vinculadas a la infracción –p. ej., publicidad, venta de datos…-, debemos descartarlo ya que, en tal supuesto, el usuario también llevaría a cabo una actividad económica. De este modo, parece que la única forma de atribuir al usuario la realización de actividades que reúnan estas características es la existencia de cierta vinculación –p. ej., capacidad de control o que se trate de la misma persona- entre quien pone a disposición o difunde los contenidos y quienes obtienen beneficios económicos o comerciales, directos o indirectos, a partir de las infracciones facilitadas por el usuario a identificar –p. ej., los responsables del *software* P2P o el prestador de servicios de alojamiento 2.0 desde el que se ofrecen las obras o los enlaces a estas-.

A lo señalado debemos añadir una manifestación adicional de la imposibilidad de obtener beneficios por parte del usuario: mientras en la diligencia dirigida a averiguar la identidad del prestador de servicios presunto infractor, el ordinal 10.º del art. 256.1 de la LEC incluye como sujetos pasivos a los prestadores de pago electrónico y a los prestadores de servicios de publicidad; en el caso de la diligencia preliminar destinada a averiguar la identidad del usuario, el ordinal 11.º limita la condición de sujeto pasivo a los prestadores de servicios de la sociedad de la información (CASTÁN, 2016, p. 147). Por tanto, mantener la interpretación de que solo cabe solicitar la diligencia cuando los actos del usuario se realicen con ánimo de obtener beneficios económicos o comerciales, deviene contradictorio con el hecho de que

[31] Si bien se trata de definiciones previstas a los solos efectos de aplicar la LSSI, el Anexo de esta norma, en su apartado a), define *servicio de la sociedad de la información* como aquel que es prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario, incluyendo los servicios que no son remunerados por el destinatario pero que representan una actividad económica para el prestador.

no se pida la información a quienes se encargan de gestionar estos rendimientos.

No obstante, una interpretación amplia de la idea de beneficio económico indirecto, podría llevarnos a considerar que este también existe como consecuencia de la ventaja o el ahorro que suponen, para el propio usuario, las actividades que realiza. Si bien depende de las características del modelo de explotación, las ventajas como beneficio económico indirecto pueden darse en los programas de pares y en los sitios web 2.0 cuando estos premian a sus usuarios en función de la cantidad de materiales que ponen a disposición del público –p. ej., más velocidad de descarga, cuota de abonado gratuita o acceso a contenidos *premium*-.

Sin embargo, el beneficio económico indirecto generado por el ahorro de no pagar a cambio de las obras no casa con la actividad de poner a disposición o de difundir contenidos protegidos, puesto que únicamente se produce como consecuencia de realizar los actos de reproducción necesarios para llevar a cabo la descarga de contenidos –y estos actos, como se ha indicado, quedan fuera del ámbito de aplicación de la diligencia preliminar del ordinal 11.º-. Por tanto, únicamente en el caso de las ventajas indicadas en el párrafo precedente, podría afirmarse que el usuario actúa con ánimo de obtener beneficios y podrían solicitarse los datos que permitan su identificación[32].

Por último, conviene diferenciar el beneficio económico indirecto –al que se ha hecho referencia *supra*- del beneficio comercial indirecto; a propósito del segundo, GARROTE FERNÁNDEZ-DIEZ ofrece como ejemplo lo que él mismo denomina "usuarios «profesionales»" definiéndolos como aquellos "que ofrecen archivos a otros con la finalidad de captar su atención respecto de un determinado sitio web (por ejemplo, añadiendo en el nombre del archivo la dirección de la página)" (GARROTE, 2011, p. 55). No obstante, tras la sentencia *Mc Fadden* del TJUE, incluso estos usuarios "profesionales" podrían ser considerados prestadores de servicios de la sociedad de la información, siempre que la publicidad que realicen de su sitio de Internet a través del servicio que prestan –en este caso, como proveedores de contenidos- se desarrolle en el marco de su actividad económica –de ser así, cabría conocer su identidad haciendo uso de la diligencia del subapartado 10.º, en lugar de recurrir a la del ordinal 11.º- [STJUE *Mc Fadden*, 3.ª, 15.09.2016 (C-484/14; MP: J. Malenovský), puntos 41 a 43].

A partir de lo que ha sido expuesto debemos concluir que, el hecho de que ambas conductas –la actuación de buena fe y la ausencia de ánimo de obtener beneficios-, excluyan la posibilidad de solicitar la diligencia preliminar del subapartado 11.º para conocer la identidad del usuario, limita, notablemente, el ámbito de aplicación de esta norma. En particular, esta restricción se ve agravada por la circunstancia de que la segunda de las excepciones se base en unos criterios que, por definición, concurren en la mayoría de

[32] Otra interpretación de esto es la que propone MINERO (2015, p. 383), quien considera que el juez "habrá de estar a la entidad económica del propio acto, más que a la finalidad comercial o a la calificación que pueda merecer el supuesto infractor".

usuarios que ponen a disposición o difunden contenidos protegidos en Internet[33].

Mantener la interpretación del art. 256.1.11.º de la LEC que se ha apuntado en este epígrafe, junto al resto de requisitos y limitaciones previstos en la citada norma para hacer posible el recurso a esta diligencia preliminar –legitimación activa, indicios razonables, volumen apreciable…-, provocará, como consecuencia, que el interesado en ejercer las acciones de indemnización, cese o publicación de la sentencia, se plantee la oportunidad de dirigirlas contra el usuario, especialmente ahora que la nueva regulación del art. 138.II de la LPI, y la jurisprudencia de la Unión en materia de enlaces, han ampliado las posibilidades de legitimación pasiva más allá del tradicional infractor –aquel que pone a disposición del público los contenidos protegidos-.

- La exclusión de los consumidores finales que actúan de buena fe y sin ánimo de obtener beneficios económicos o comerciales (segunda interpretación).

La segunda interpretación del art. 256.1.11.º de la LEC implica considerar que las dos características –buena fe y sin ánimo de obtener beneficios-, se refieren a una única conducta del consumidor final, de modo que será necesaria la concurrencia de ambas sobre la actividad desarrollada por el usuario para que se aplique la excepción –y, por tanto, para que no sea posible obtener su identidad mediante la diligencia preliminar del ordinal 11.º-. En nuestra opinión, esta es la interpretación que debe mantenerse –aun cuando pueda parecer forzada-, de una parte, porque la norma tampoco ofrece suficiente claridad para imponer la primera interpretación, y, de otra parte, porque si se interpreta la excepción del modo en que ha sido expuesto en el apartado precedente, existe el riesgo de que la diligencia preliminar restrinja de tal manera su ámbito de aplicación que ni siquiera pueda tener valor disuasorio respecto de los usuarios.

Es posible reforzar esta interpretación con base en los siguientes argumentos. En primer lugar, el pronunciamiento por el que el tribunal civil declare que los actos de explotación son ilícitos tendrá en cuenta la inexistencia de autorización por parte del titular del derecho, pero no, en cambio, si quien cometió las infracciones lo hizo con la intención de obtener beneficios económicos o comerciales.

En segundo lugar, porque es precisamente el ánimo de obtener un beneficio económico directo o indirecto uno de los requisitos que, tras la reforma operada en virtud de la LO 1/2015[34], el art. 270 del Código Penal exige para que la infracción de la propiedad

[33] "En realidad, si lo que se quería era evitar que el precepto quedase privado de toda utilidad práctica, lo que se debería haber suprimido no era el requisito de que la puesta a disposición o difusión de obras o prestaciones protegidas se haya producido a gran escala, sino el de que la infracción persiga la obtención de beneficios económicos o comerciales" (LÓPEZ, 2016, p. 393).

[34] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, *B.O.E.*, núm. 77, de 31 de marzo de 2015.

intelectual sea constitutiva de delito[35], pudiendo existir ilícito civil en el caso de que el infractor no desarrolle una actividad económica a partir de sus actuaciones.

En tercer lugar, el considerando 14 *in fine* de la Directiva 2004/48 establece: "Los actos llevados a cabo a escala comercial son los realizados para obtener beneficios económicos o comerciales directos o indirectos; esto excluye normalmente los actos realizados por los consumidores finales de buena fe"; por ello, si bien el consumidor final de buena fe, como regla general, carece de ánimo de lucro, para que se le aplique la excepción –esto es, para que no pueda ejercerse una diligencia preliminar dirigida a conocer su identidad- será necesario que, adicionalmente, concurra el requisito de no pretender obtener un beneficio económico.
Por último, estableciendo un paralelismo con la jurisprudencia *GS Media* del TJUE –si bien limitada a los enlaces como actos de puesta a disposición-, es constitutiva de infracción la conducta que reúne dos condiciones: se realiza sin ánimo de lucro y conociendo o debiendo conocer su carácter ilícito –siendo este segundo requisito equiparable a la mala fe del usuario-; de modo que, si concurren la buena fe y la falta de ánimo de obtener beneficios, el consumidor que ha realizado la puesta a disposición o difusión no podrá ser identificado [STJUE *GS Media*, 2.ª, 8.09.2016 (C-160/15), puntos 47 a 50].

Como se ha desarrollado a propósito de la primera interpretación, son limitados los supuestos en que el usuario actúa con ánimo de obtener beneficios económicos o comerciales; en este sentido, el consumidor final cuya actividad ha consistido en la puesta a disposición del público o en la difusión, directa o indirecta, de contenidos protegidos mediante redes de pares o páginas web 2.0, reunirá, en la mayoría de ocasiones, el requisito de realizar actos que carezcan de interés económico o comercial. Lo anterior permite mantener que, como regla general, no será frecuente la práctica de esta diligencia preliminar, por lo que deviene necesario –como única vía para evitar que se den las dos condiciones que impiden la concesión de la diligencia-, que el solicitante de los datos pruebe que el usuario realizó sus actuaciones sin buena fe.

Si bien la buena fe se presume, no deja de ser una presunción *iuris tantum*, por lo que los esfuerzos de quien solicite la diligencia habrán de centrarse en demostrar lo contrario. No obstante, tratándose de una demostración dirigida a que se conceda la práctica de una diligencia preliminar, la carga probatoria impuesta al solicitante en este momento previo al inicio del proceso civil no debe ser la misma que la exigida para obtener un pronunciamiento favorable –especialmente, en la medida en que, para que el tribunal dicte una sentencia estimatoria, no es necesario acreditar ante el mismo que el usuario que cometió los ilícitos actuó con mala fe-. En todo caso, debemos plantear nuestras dudas a propósito de la existencia de buena fe por parte de quien, careciendo del consentimiento del titular de derechos, pone a disposición del público o difunde contenidos protegidos –bien mediante su carpeta compartida en redes de pares, o bien a través de páginas web en formato 2.0-, ya que este usuario es, o al menos debería ser, conocedor de que está

[35] Sobre los requisitos que deben reunir las conductas tipificadas como constitutivas de delito contra la propiedad intelectual tras la reforma de 2015, véase LLORIA (2016); TOMÁS Y VALIENTE (2015, pp. [843] a 890).

realizando actos de explotación ilícita y, con ello, permite que terceros accedan a obras o prestaciones sin retribuir a su titular[36].

b. La necesidad de un volumen apreciable de obras y prestaciones protegidas por la propiedad intelectual ofrecidas sin autorización

Para que sea concedida la práctica de la diligencia preliminar, el art. 256.1.11.º de la LEC exige atender al volumen apreciable de contenidos puestos a disposición o difundidos sin el consentimiento de su titular. La norma hace uso de la expresión *teniendo en cuenta*, de modo que, si bien el juez competente, antes de decidir sobre su concesión, habrá de prestar atención al número de obras o prestaciones que son ofrecidas por el usuario, se trata de una redacción que parece prevista para rebajar el carácter imperativo de esta exigencia. En particular, esto puede ser relevante para evitar que la obligación de demostrar que el usuario comparte –en una cantidad significativa-, contenidos protegidos por la propiedad intelectual, se convierta en una carga excesiva para el solicitante de la diligencia en fase pre-procesal –especialmente, en cuanto necesitará probar la falta de autorización para explotar obras cuya titularidad corresponde a otros sujetos-.

En todo caso, a pesar de que este volumen apreciable solo *ha de tenerse en cuenta,* se trata de un requisito adicional que restringe el ámbito de aplicación de la diligencia, puesto que excluye la posibilidad de solicitar información sobre aquellos usuarios que cometan actos ilícitos en una cantidad que no merezca el adjetivo de *apreciable* (CASTÁN, 2016, p. 147)[37]. Sin embargo, esta definición constituye un concepto jurídico indeterminado y deja en manos del Juzgado de lo Mercantil la facultad de apreciar, con discrecionalidad y a efectos de decidir sobre la concesión o denegación de la práctica de la diligencia, si la cantidad de contenidos puestos a disposición o difundidos por el usuario puede ser calificada como *apreciable*.

Sin que se exija que las actividades se realicen a gran escala –pues no ha de entenderse así este adjetivo-, la necesidad de que el volumen sea apreciable supone descartar la posibilidad de recurrir a la diligencia del subapartado 11.º cuando se trate de infracciones puntuales –o cometidas a título individual-. Esto será así, aunque sea posible probar el (elevado) número de reproducciones no autorizadas que han tenido lugar a partir de ese acto de puesta a disposición o esa actividad de difusión, puesto que, lo relevante es que el usuario haya facilitado otros contenidos.

[36] GARROTE (2011, p. 55) mantiene una postura escéptica al plantear "es muy dudoso que los usuarios de redes P2P sean en todo caso consumidores de buena fe". LÓPEZ (2016, p. 392) es más contundente al respecto, al entender que, en relación con los usuarios de programas P2P, la exigencia de buena fe "no plantea ningún obstáculo, pues no parece que quien almacena en su carpeta de archivos compartidos contenidos protegidos por derechos de propiedad intelectual merezca la condición de «usuario final de buena fe»".

[37] Asimismo, considera el autor que el requisito consistente en tener en cuenta el *volumen apreciable* de contenidos ofrecidos por el presunto infractor, provoca que la vía civil solo pueda utilizarse para las "grandes infracciones" (CASTÁN, 2016, p. 149).

En otras palabras, según la redacción prevista, queda fuera del ámbito de aplicación de la diligencia del ordinal 11.º aquel usuario que ha puesto a disposición del público o difundido una única obra –incluso haciéndolo con ánimo de obtener un beneficio económico o comercial-. Por tanto, aun cuando la repercusión económica de su infracción sea elevada –p. ej., cuando la obra todavía no ha sido difundida o publicada por cualquier otro medio o, simplemente, cuando el interés generado sea tal que un gran número de internautas han disfrutado en línea o han descargado copias de la misma sin remunerar a los titulares de derechos- no será posible identificar al usuario presunto infractor, por lo que solo podrán ejercerse las acciones de los arts. 138 y ss. de la LPI contra los otros sujetos pasivamente legitimados.

A esto debe añadirse que la facilidad con la que, *a priori*, el titular del derecho puede averiguar la IP del internauta, contrasta con lo compleja que puede ser la tarea de demostrar ante el tribunal la existencia de un volumen *apreciable* de contenidos objeto de infracción, pues para ello no solo debe buscar otros materiales protegidos que estén siendo proporcionados por un mismo usuario desde ese modelo de explotación –obras o prestaciones cuya titularidad corresponderá a terceras personas-, sino que, además, habrá de demostrar que carecía del consentimiento de los titulares para realizar esa puesta a disposición o difusión. Respecto de la diligencia preliminar dirigida a conocer la identidad del usuario, debemos mantener que ha de regir la idea de *indicios razonables* de que, al igual que sucede con su obra o prestación, estos contenidos también están siendo ofrecidos sin la preceptiva autorización para ello –y no, en cambio, la necesidad de probar la falta de consentimiento para explotarlos, tratándose de contenidos cuya titularidad no le corresponde-.

A lo señalado debe añadirse que, para el titular del derecho, deviene más difícil acreditar la existencia de un volumen apreciable de contenidos cuando es un usuario quien los pone a disposición o los difunde. Lo afirmado se debe a que la visibilidad al público de los materiales protegidos que ofrece no es la misma que la publicidad de los contenidos facilitados por los prestadores de servicios; p. ej., si el titular de la página actúa como el único sujeto que pone obras a disposición del público desde el sitio de Internet que administra, el total de contenidos provistos por este –que justifique la existencia de un volumen apreciable-, podrá comprobarse con una simple visita a su web ya que todo lo que allí se ofrezca habrá sido proporcionado por este prestador de servicios.

Como ha sido expuesto *supra*, conocer la IP del usuario facilita las actuaciones, pues únicamente obliga al titular del derecho infringido a solicitar una diligencia preliminar que tendrá como sujeto pasivo al prestador de servicios de acceso. Ahora bien, en el caso de que la puesta a disposición o la difusión se realice desde un sitio web 2.0, salvo que la página haga pública la IP desde la que han sido subidas las obras –situación menos frecuente en estas plataformas-, el solicitante de la diligencia ha de tener en cuenta el nombre (*nickname*) con el que actúa el usuario y comprobar cuantos archivos son ofrecidos por este. Por su parte, cuando el modelo utilizado sea un programa de intercambio entre pares, quien

pretenda solicitar la diligencia prestará atención a los contenidos que son facilitados desde una misma dirección IP –algo que, habitualmente, es posible en este tipo de *software*, sin perjuicio de que también pueda conocer el nombre ficticio con el que actúa el usuario en este sistema de intercambio-.

En ambos supuestos –la web 2.0 y el *software* P2P-, la mayor o menor dificultad de la búsqueda depende de la configuración del sitio de Internet o del programa de intercambio; a veces es suficiente con hacer clic sobre el nombre del usuario para que nos dirija a todos los materiales ofrecidos por este –p. ej., así funciona la página web 2.0 *ThePirateBay*, que ofrece enlaces que permiten la ubicación de las obras-, en cambio, en otros modelos es necesaria una búsqueda individual y manual en la que el titular del derecho vaya tomando nota de los distintos contenidos facilitados por un *nickname* o una dirección IP en un determinado momento –p. ej., las redes de descarga entre pares tradicionales, como es el caso de *Kazaa*-.

3.3. Los problemas que surgen al intentar identificar al usuario presunto infractor a partir de la diligencia preliminar del art. 256.1.11.º

Conforme a lo que ha sido expuesto, los usuarios que pueden identificarse haciendo uso de la diligencia prevista en el subapartado 11.º reúnen las siguientes características. Primero, deben poner a disposición o difundir contenidos protegidos por la propiedad intelectual –lo que excluye a quienes únicamente reproducen contenidos-; segundo, no ha de tratarse de consumidores finales que actúen de buena fe y carezcan de ánimo de obtener beneficios económicos o comerciales –siendo suficiente, para evitar que se aplique esta excepción, demostrar que el usuario actuó con mala fe-; tercero, la cantidad de obras o prestaciones ofrecidas sin autorización debe cumplir el requisito de ser apreciable –un volumen que será valorado por el tribunal pero que no puede constituir una carga probatoria excesiva para el solicitante-.

La necesidad de que concurran los requisitos expuestos reduce los usuarios de Internet cuya identidad puede solicitarse conforme al art. 256.1.11.º de la LEC, a esto debe añadirse que disponer de la dirección IP desde la que se cometen las infracciones no siempre conduce a descubrir la identidad del autor de las mismas (GONZÁLEZ GOZALO, 2005, p. 82). Solicitada la diligencia preliminar frente al proveedor de acceso, este proporcionará el nombre y apellidos del cliente que contrató el servicio de conexión a Internet y actuaba en el momento indicado bajo esa dirección IP; sin embargo, la persona indicada no necesariamente coincidirá con el autor material de las infracciones (GARROTE, 2011, p. 60). Esta situación puede darse en los tres tipos de redes utilizadas para acceder a Internet: las redes públicas, las redes privadas y las redes locales, siendo diferentes las consecuencias a efectos de identificar al usuario, de exigirle responsabilidad y de ejercer el derecho a la tutela judicial efectiva.

a. Redes públicas: las diferentes consecuencias de proporcionar acceso gratuito, previa retribución o en el marco de una actividad económica

Son *redes públicas* aquellas que permiten el acceso a Internet de gran cantidad de personas, bien de forma abierta sin exigir que se identifiquen, o bien previo registro controlado por el titular –siendo, lo segundo, menos frecuente-. La principal característica de estas redes es que todos los dispositivos que se conectan lo hacen desde la misma IP pública proporcionada por el proveedor de acceso para ese *router* o *modem*.

Habitualmente, estas redes públicas son operadas por un particular que ha contratado con el prestador de servicios de acceso y ofrece conexión al resto de internautas, esto puede realizarse de dos formas: a cambio de retribución o de manera gratuita. Si se realiza previo pago de una contraprestación –lo que implica que desarrolla una actividad económica vinculada al servicio que ofrece-, el particular debe recibir la condición de prestador de servicios de la sociedad de la información. En cambio, no parece posible atribuirle tal característica cuando esto es realizado de forma gratuita; no obstante, cabe la posibilidad de que, aun facilitando el acceso gratuitamente, lo haga en el marco de su actividad económica –p. ej., con fines publicitarios para atraer a los clientes-, en estos supuestos, el TJUE ha interpretado que el particular también debe ser considerado como un prestador de servicios de la sociedad de la información [STJUE *Mc Fadden*, 3.ª, 15.09.2016 (C-484/14), puntos 41 a 43]. Este sería el caso de las redes públicas de acceso a Internet mediante conexión Wi-Fi ofrecidas desde hoteles, cafeterías, aeropuertos…

Tras conocer que la IP corresponde a la red pública ofrecida por un particular que reúna las características de la LSSI para ser prestador de servicios de acceso o las indicadas por la jurisprudencia de Luxemburgo, nada impide ejercer una nueva diligencia preliminar –sobre la base del ordinal 11.º-, para identificar al usuario de su servicio que cometió la infracción. A este propósito, conviene recordar que en el asunto *Mc Fadden*, el TJUE entiende apropiado imponer, a quien ofrece una red pública en el marco de su actividad económica, la obligación de proteger la conexión a Internet mediante una contraseña, de modo que, para obtener la clave de acceso, los usuarios hayan de revelar su identidad y no puedan actuar a través de esa red pública de forma anónima [STJUE *Mc Fadden*, 3.ª, 15.09.2016 (C-484/14), puntos 93 a 96]. De esta forma, el titular de la conexión que ha actuado como proveedor de acceso podrá facilitar los datos del usuario que, haciendo uso de su red, ha infringido los derechos de propiedad intelectual.

Ahora bien, si no es posible la identificación del usuario que ha hecho uso de su servicio para infringir los derechos de propiedad intelectual, contra el particular que actúa como proveedor de acceso únicamente podrá ejercerse la acción de cese –solicitando que adopte las medidas necesarias para impedir que se siga cometiendo la infracción-, y no, en cambio, la acción de indemnización [STJUE *Mc Fadden*, 3.ª, 15.09.2016 (C-484/14), pp. 73 a 79, especialmente, puntos 74 y 76]. En nuestro ordenamiento jurídico, la base para ejercer estas acciones contra el prestador de servicios de intermediación la proporciona el art. 138.IV de la LPI.

b. Redes privadas: la posible falta de correspondencia entre quien contrató la conexión a Internet y el autor material de las infracciones

La dirección IP puede proporcionar la identidad del particular que ha contratado una red de acceso a Internet y la destina a un uso privado, esto es, restringido a un número reducido de usuarios a quienes, generalmente, se les exige disponer de la contraseña que permite conectarse –p. ej., una casa con personas que se conectan desde distintos dispositivos-; en estos casos, también todos acceden a Internet mediante una única IP pública. Si bien es menor el número de personas que utiliza una *red privada*, no cabe descartar la posibilidad de que, identificado el titular de la línea –es decir, quien contrató con el prestador-, este no haya sido el autor de las infracciones; se trata de una situación que puede darse tanto si la conexión se realiza desde diferentes dispositivos como si son distintas las personas que acceden a Internet haciendo uso de un mismo terminal –pues, en ambos supuestos, la salida al exterior se realizará a través de la misma dirección IP-.

Si quien contrató el servicio no coincide con el usuario que puso a disposición o difundió los contenidos ilícitos, no existe la posibilidad de solicitar una segunda diligencia preliminar de acuerdo con los subapartados 10.º y 11.º de la LEC –ya que el particular cuya identidad se ha obtenido no tiene la condición de prestador de servicios-, sin embargo, como se expone *infra*, no debe descartarse su solicitud con base en el art. 256.1.7.º. Ahora bien, aun cuando no sea posible identificar al usuario presunto infractor, esto no puede impedir la solicitud de la tutela judicial efectiva por parte del titular del derecho de propiedad intelectual, por este motivo, en defecto de información más precisa que permita concretar el usuario que cometió la infracción mediante la red privada, cabe entender posible exigir responsabilidad a aquel que contrató el servicio de conexión a Internet[38] –aplicando, para ello, la responsabilidad extracontractual de los arts. 1902 y ss. del CC[39]-. A pesar de lo indicado, habrá que estar a la respuesta del TJUE en el asunto Bastei Lübbe a propósito de la posibilidad de excluir la responsabilidad del titular de la línea utilizada para infringir si señala a miembros de su familia que, junto a él, han tenido acceso a esa conexión a Internet[40] [Recurso (DO) *Bastei Lübbe*, fecha de presentación: 16.06.2017 (C-149/17)].

c. Redes locales: el papel del administrador de la red a efectos de conocer la identidad del usuario y la posibilidad de recurrir al interrogatorio

Por último, nada excluye que las infracciones se hayan cometido a través de una *red local*;

[38] En caso de que el titular de la línea no identifique al infractor, GARROTE (2011, p. 61) entiende que "el abonado que contrató la cuenta de acceso a Internet debe ser considerado al menos como responsable solidario de la infracción, sin perjuicio de que pueda repetir luego lo pagado del verdadero infractor".

[39] Por su parte, LEDESMA (2011, p. 156) y MONTESINOS (2015, p. 66), barajan, como posible solución, que el abonado al servicio de acceso a Internet facilite los datos del infractor como requisito para que quepa dejarlo exento de toda responsabilidad, de lo contrario, se le considerará responsable de la infracción.

[40] En el momento en que se cerró el presente trabajo las cuestiones prejudiciales planteadas por el *Landgericht München I* en el marco el asunto Bastei Lübbe estaban pendientes de resolución.

este sistema, también denominado *intranet*, es habitualmente utilizado para la conexión a Internet por parte del personal de empresas, universidades, organismos públicos… permitiendo el acceso a recursos que forman parte de las bases de datos de la organización –o de las que tienen contratadas- que no están libremente disponibles para el resto de usuarios de Internet. Lo relevante cuando las infracciones de derechos de propiedad intelectual se cometen desde redes locales, es que la comunicación con el exterior se realiza a través de una misma dirección IP –la IP pública que es visible para los otros internautas-. Por tanto, también para la *intranet*, conocer la IP desde la que el usuario pone a disposición o difunde contenidos protegidos no conduce al infractor, sino a quien contrató con el prestador de acceso: la empresa, la universidad, el organismo público…

En estos casos, deberá solicitarse al titular o administrador de la red de área local que indique el dispositivo desde el que se cometieron las infracciones; a este respecto deben señalarse dos ideas. De una parte, la posibilidad de dirigir contra este las diligencias preliminares de los ordinales 10.º y 11.º, así como el régimen de responsabilidad que se le aplique, dependerán de si cabe considerarlo como un prestador de servicios de acceso; en defecto de pronunciamiento del TJUE sobre esta cuestión, la clave está en si el titular de la red local reúne los requisitos exigidos por la LSSI, esto es, si desarrolla una actividad económica y ofrece conexión a Internet como parte de la misma.

De ser afirmativa la respuesta –p. ej., en el caso de las empresas privadas-, su situación se corresponde con la del particular que ofrece conexión a Internet mediante una red pública: podrá ser sujeto pasivo de las diligencias de los subapartados 10.º y 11.º y solo podrá ejercerse contra él la acción de cese conforme al art. 138.IV de la LPI. En cambio, la respuesta negativa –p. ej., si se trata de universidades públicas- concede al administrador de la red local el mismo estatus que a quien contrató la red privada desde la que se cometieron los ilícitos: no puede ser sujeto pasivo de las diligencias de los ordinales 10.º y 11.º, pero podrá exigírsele responsabilidad, al menos, de acuerdo con los arts. 1902 y ss. del CC.

De otra parte, debe tenerse en cuenta que el titular del derecho no dispone de la IP privada que la red local asigna al dispositivo desde el que se ha cometido la infracción, sino únicamente la IP pública y la fecha –día y hora- en que sus obras o prestaciones fueron puestas a disposición del público o difundidas. En consecuencia, será necesario que el administrador de la red local cuente con un registro que le permita conocer las conexiones realizadas por los distintos terminales y/o usuarios que acceden a partir de su *intranet*; aun así, solo podrá informar sobre el terminal y/o usuario a quien corresponde la IP privada desde la que se realizaron esas comunicaciones, pero no podrá garantizar la identidad exacta de la persona que cometió la infracción utilizando ese terminal y/o esa cuenta de usuario de la red local[41].

[41] En estos casos, GARROTE (2011, p. 61) defiende la presunción de que el usuario del terminal indicado por el administrador de la red es quien ha cometido las infracciones, no obstante, sostiene su carácter *iuris tantum*, pudiendo ser desvirtuada "identificando en su caso a otras personas que tienen acceso al ordenador o al infractor concreto, si es que lo conoce".

Salvo en el caso de que el titular de la IP pública desde la que se cometieron los ilícitos sea, a su vez, un proveedor de acceso, en el resto de supuestos, en cuanto quien contrató el acceso a Internet no tiene la condición de prestador de servicios de la sociedad de la información, no será posible que se soliciten frente a este las diligencias preliminares de los subapartados 10.º y 11.º. Ahora bien, en estos casos, no ha de descartarse la posibilidad de practicar una segunda diligencia que tenga como sujeto pasivo a quien no puede incluirse en la categoría de prestador, utilizando, para ello, el art. 256.1.7.º de la LEC[42].

Lo indicado en el párrafo precedente, *a priori*, será posible siempre que los requisitos que exige la misma se cumplan en nuestro supuesto de hecho –puesto que no limita el sujeto pasivo de la diligencia a los prestadores de servicios-. Contribuye a afirmar esta posibilidad las modificaciones introducidas por la Ley 21/2014, ya que parecen haber derogado la regulación del interrogatorio en que consistían estas diligencias preliminares y, con ello, la limitación existente respecto de quienes podían ser interrogados, eliminando toda restricción respecto de los posibles sujetos pasivos.

En defecto de consenso en la doctrina, debemos defender que, tal y como se desprende de la versión consolidada de la LEC, la referida derogación se ha producido. Así, el art. 2.1 de la Ley 21/2014 establece, respecto del art. 256.1, que se modifica el subapartado 7.º "con la siguiente redacción", e introduce un texto que prescinde de la referencia a los sujetos pasivos del interrogatorio en que consiste la práctica de esta diligencia preliminar –como sí hacía, en cambio, la versión anterior de esta disposición-. Asimismo, la versión consolidada de la LEC publicada en el *B.O.E.*, tampoco incluye referencia alguna a los posibles sujetos pasivos del interrogatorio, por lo que cabe entender que la reforma de noviembre de 2014 deroga esta parte del art. 256.1.7.º[43].

[42] GONZÁLEZ GOZALO (2005, p. 133) mantenía la posibilidad de practicar una segunda diligencia preliminar solicitando información al titular de la cuenta de acceso a Internet sobre la base del ordinal 7.º. En el mismo sentido, también antes de la reforma introducida por la Ley 21/2014, GARROTE (2011, p. 61).

[43] Entienden que la Ley 21/2014 deroga la referencia a los sujetos que pueden ser interrogados, DÍAZ PITA (2015, pp. 193 a 195); MONTESINOS (2015, p. 44). En cambio, hay autores que mantienen esta restricción de los sujetos pasivos frente a quienes puede dirigirse la diligencia del subapartado 7.º: CASTÁN (2016, p. 141), quien considera que "el subapartado 7º ha sido modificado, no derogado, por lo que subsiste en vigor aquellos párrafos del texto anterior que no se hayan visto afectados"; MINERO (2015, p. 378), quien señala, como sujetos pasivos de la diligencia del ordinal 7.º tras la reforma, a aquellos a los que se limitaba esta disposición antes de la Ley 21/2014.

4. La utilización de la información obtenida y el carácter reservado de las actuaciones

4.1. El uso limitado al proceso civil de los datos del usuario presunto infractor obtenidos mediante la práctica de la diligencia preliminar

En virtud de los cambios introducidos por la Ley 21/2014, el art. 259.4 de la LEC restringe el uso de la diligencia preliminar al litigio que el propio solicitante inicie, a partir de la misma, a fin de proteger los derechos que está legitimado para defender. Asimismo, esta norma impone al solicitante la prohibición de divulgar o comunicar a terceros la información que se le ha facilitado a través de la práctica de la diligencia –p. ej., a otros afectados por la infracción de derechos de propiedad intelectual, o por actos de competencia desleal, que estuvieran legitimados para iniciar un proceso civil contra el usuario presunto infractor (LÓPEZ, 2016, p. 392)-. Como señala MINERO (2015, p. 386), lo establecido en la citada disposición no impide la acumulación de acciones ante el Juzgado de lo Mercantil por quien tiene la legitimación activa[44], siempre que, al menos una de ellas, sea relativa a los derechos de propiedad intelectual cuya infracción ha motivado la práctica de la diligencia y vaya dirigida contra el usuario cuyos datos han sido facilitados [en el mismo sentido, MONTESINOS (2015, p. 70)].

El art. 259.4 de la LEC delimita el campo de aplicación de los datos obtenidos mediante la diligencia al establecer que estos serán utilizados "exclusivamente para la tutela jurisdiccional de los derechos de propiedad intelectual"; mediante esta redacción excluye toda posibilidad de utilizar la información ante órganos diferentes a los jurisdiccionales (CASTÁN, 2016, p. 149); (LÓPEZ, 2016, p. 392); (MORILLO, 2015, p. 346). En consecuencia, no será posible el uso de estos datos a efectos de iniciar un procedimiento para el restablecimiento de la legalidad ante la Sección Segunda de la Comisión de Propiedad Intelectual, si bien es cierto que esto carece de repercusión sobre los usuarios que son identificados mediante la diligencia preliminar del ordinal 11.º, ya que, conforme al art. 195.2 de la LPI[45], los sujetos pasivos del procedimiento seguido ante este órgano administrativo pueden ser, únicamente, los prestadores de servicios de la sociedad de la información (LLOPIS, 2018a, pp. 89 y ss.).

Asimismo, el hecho de que se prevea en la LEC como diligencia preliminar destinada a preparar un proceso civil impide su extensión a procesos de distinta naturaleza, en particular, a los de tipo penal, puesto que la averiguación de los datos relativos al presunto autor del delito se realizará por el tribunal competente durante la fase de instrucción –no

[44] La autora utiliza, como ejemplo de posible acumulación, la acción en defensa de la propiedad intelectual y la acción frente a un acto de competencia desleal (MINERO, 2015, p. 386).

[45] Numeración atribuida por la reciente reforma de la LPI operada en virtud del Real Decreto Ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

siendo necesario que, quien ha cometido las infracciones penales, esté identificado cuando comience el proceso-. Ahora bien, lo anterior ha de entenderse sin perjuicio de que, con posterioridad a la petición de los datos del presunto infractor, se descubra que las conductas que este ha llevado a cabo presentan características suficientes para ser calificadas como delictivas –es decir, que se trate de una infracción cometida con ánimo de obtener un beneficio económico directo o indirecto y que la actuación se haya realizado en perjuicio de tercero-, de modo que el solicitante de la diligencia inicie un proceso ante los tribunales penales contra el usuario que ya ha sido identificado –algo que podrá hacer a partir de la información obtenida sobre la base del ordinal 11.º del art. 256.1 de la LEC-[46].

4.2. La posibilidad de conceder carácter reservado a la práctica de la diligencia preliminar previa petición de su solicitante o del sujeto pasivo

Por último, cabe destacar que el art. 259.4 *in fine* prevé la posibilidad de que, si así lo solicita cualquiera de los interesados, el Juzgado de lo Mercantil competente otorgue carácter reservado a la práctica de la diligencia preliminar; el propósito de esta previsión es, conforme a lo que establece la LEC, garantizar la protección de los datos e información de carácter confidencial[47]. Si bien *a priori* esta confidencialidad parece únicamente relevante cuando la diligencia consista en la exhibición de documentos, también en el caso de que se solicite con la finalidad de identificar al presunto infractor, la no publicidad de su práctica puede tener importancia.

El carácter reservado de las actuaciones nunca se decidirá de oficio, sino a instancia de parte, de modo que tanto el solicitante como el sujeto pasivo podrán instar que la práctica de la diligencia se lleve a cabo en una vista celebrada a puerta cerrada. Así, el prestador de servicios que será interrogado puede tener interés en preservar la confidencialidad de uno de sus clientes –quien ha contratado el servicio de acceso a Internet o quien actúa tras una identidad ficticia en la página web 2.0-. Por su parte, el solicitante de la diligencia, siendo consciente de la rapidez con que pueden modificarse y eliminarse los contenidos en Internet, puede estar interesado en que se respete el carácter secreto de sus actuaciones, a fin de que prosperen las acciones que finalmente ejerza contra el presunto infractor –en especial, que el usuario desconozca su intención de iniciar un proceso civil contra él-[48].

---

[46] Además de lo expuesto, señala LÓPEZ (2016, p. 392) que el art. 259.4 de la LEC impide a quien solicita la diligencia "comunicarse directamente con el infractor para conminarle al cese de la infracción o advertirle de que si persiste en su conducta iniciará acciones legales contra él".

[47] "Esta restricción parte del carácter privado de los datos que pueden conocerse a través de estas diligencias previas […] pero también se justifica por la propia naturaleza de las medidas provisionales, que se admiten, de manera excepcional y con carácter tasado" (LÓPEZ, 2016, p. 392).

[48] GONZÁLEZ GOZALO (2008, p. 48), antes de la reforma introducida por la Ley 21/2014, y a propósito de la aplicación de la diligencia del ordinal 7.º para averiguar la identidad del usuario señalaba, respecto de la limitación y el carácter reservado impuesto por el art. 259.4, "el legislador español optó […] 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 […] con vistas exclusivamente a identificar a los infractores en el marco de un procedimiento

Finalmente, aun cuando no concurren motivos para privarle de la condición de interesado, el usuario cuya identidad se pretende averiguar no es citado ante el tribunal para la práctica de la diligencia, por lo que no podrá exigir al juez que respete su carácter confidencial.

5. Conclusión

Hasta la reforma operada por la Ley 21/2014, la falta de un marco legal que permitiera identificar al usuario infractor a partir de su dirección IP constituyó un obstáculo para la tutela judicial efectiva de los derechos de propiedad intelectual –en cuanto el titular de los mismos no podía obtener el nombre y apellidos de la persona contra la que dirigir su demanda-.

Para hacer frente a este problema, el legislador español introdujo en el art. 256.1.11.º de la LEC una diligencia preliminar dirigida a averiguar la identidad del usuario que, presuntamente, está infringiendo estos derechos a través de Internet. Sin embargo, su práctica no está exenta de problemas, en cuanto exige el tratamiento de datos de carácter personal, queda sujeta al cumplimiento de una serie de requisitos y el acceso a la información resulta difícil dadas las características del plano real.

Todas estas circunstancias presentan el riesgo de restar virtualidad a la diligencia preliminar del ordinal 11.º a efectos de identificar al usuario infractor –pudiendo, incluso, convertirla en completamente ineficaz-. Por estos motivos, mientras seguimos a la espera de jurisprudencia de nuestros órganos jurisdiccionales, en el presente trabajo se han intentado concretar los aspectos esenciales del régimen jurídico de esta medida pre-procesal, a efectos de facilitar su aplicación para desvirtuar el presunto anonimato que proporcionan las direcciones IP.

Así, a modo de recapitulación de las ideas que han sido defendidas, es necesario incidir en la oportunidad de limitar el ejercicio de la diligencia preliminar al titular del derecho infringido; quien habrá de realizar, con carácter previo, un tratamiento manual e individualizado de la dirección IP desde la que se cometen las infracciones. De esta forma se garantiza el equilibrio entre dos grupos de derechos fundamentales: la tutela judicial efectiva y la propiedad intelectual, de una parte, y la intimidad y la protección de datos personales, de otra.

La complejidad de los sistemas que se utilizan en Internet para infringir la propiedad intelectual puede determinar que, según su configuración, el titular de los derechos disponga o no de la dirección IP desde la que se cometen los ilícitos; esto repercute, directamente, en el sujeto pasivo de la diligencia preliminar que se solicita. Así, de

civil por vulneración de la propiedad intelectual, y asegurando en lo demás la confidencialidad de esos datos".

conocerse la IP será suficiente con pedir al proveedor de acceso los datos de quien contrató la línea. En cambio, si carece de esta información, podrá, en todo caso, solicitar al prestador de servicios de alojamiento que proporcione la identidad de quien comparte obras desde su sitio de Internet; en este supuesto no cabe descartar la posibilidad de que sea necesaria la práctica de una segunda diligencia, algo que se producirá si el alojador 2.0 solo puede proporcionar la dirección IP desde la que actuó el usuario de su servicio.

Entre las actividades que justifican la solicitud de la diligencia preliminar del art. 256.1.11.º de la LEC, destaca la exclusión de la consistente en reproducir contenidos protegidos –siendo esta la conducta por excelencia del usuario infractor-. Por su parte, respecto de las actividades que sí han sido incluidas –poner a disposición y difundir directa o indirectamente obras-, habrá de evitarse una interpretación excesivamente estricta en fase pre-procesal. En este sentido, únicamente deben quedar fuera del ámbito de aplicación de la diligencia los usuarios cuya actividad ilícita reúna, de manera acumulativa, dos requisitos: se ha realizado de buena fe y sin ánimo de obtener beneficios económicos o comerciales. En cuanto a la necesidad de demostrar el volumen apreciable de contenidos ofrecidos sin autorización, la idea de indicios razonables de la infracción debe permitir solicitar la diligencia sin probar la falta de consentimiento de los terceros para la puesta a disposición del público de sus obras.

A pesar de los esfuerzos realizados por el solicitante de la diligencia es posible que, practicada la misma, la identidad de quien contrató la conexión a Internet no se corresponda con la del usuario que ha infringido sus derechos. Si bien esto constituye una dificultad añadida, no debe impedir el acceso a la justicia ni la demanda de responsabilidad; a tal efecto, es determinante el tipo de red utilizada para cometer las infracciones –red pública, red privada o red local-, siendo diferente el régimen jurídico que se aplica respecto de cada una de ellas, así como los distintos sujetos que pueden verse implicados y a quienes se les podrá pedir que faciliten información o que respondan por el ilícito.

Finalmente, conviene recordar que los datos obtenidos mediante la diligencia solo podrán utilizarse en el marco de un proceso civil que tenga como partes al solicitante de la misma y al infractor que ha sido identificado; no obstante, esto no puede impedir la acumulación de acciones o la persecución en sede penal de los ilícitos después de obtener la información del usuario mediante el art. 256.1.11.º. Asimismo, la propia LEC prevé la posibilidad de conceder carácter reservado a la práctica de la diligencia, una confidencialidad que puede instarse por el solicitante o por el sujeto pasivo, y que, en cuanto sus características determinan que los contenidos puedan modificarse o eliminarse con facilidad y rapidez, deviene particularmente relevante cuando Internet es el medio utilizado para cometer las infracciones.

6. Tabla de jurisprudencia citada

Tribunal de Justicia de la Unión Europea

Asunto, Sala y Fecha	Nº asunto	Magistrado Ponente	Partes
Promusicae, Gran Sala, 29.01.2008	C-275/06	J. Malenovský	Promusicae c. Telefónica de España
Auto* LSG, 8.ª, 19.02.2009	C-557/07	J. Malenovský	LSG c. Tele2 Telecommunication
Scarlet, 3.ª, 24.11.2011	C-70/10	J. Malenovský	Scarlet Extended c. SABAM
SABAM, 3.ª, 16.02.2012	C-360/10	J. Malenovský	SABAM c. Netlog
Bonnier, 3.ª, 19.04.2012	C-461/10	J. Malenovský	Bonnier Audio y otros c. ePhone
Svensson, 4.ª, 13.02.2014	C-466/12	J. Malenovský	Svensson c. Retriever Sverige
GS Media, 2.ª, 8.09.2016	C-160/15	M. Ilešič	GS Media c. Sanoma y otros
Mc Fadden, 3.ª, 15.09.2016	C-484/14	J. Malenovský	Mc Fadden c. Sony Music
Breyer, 2.ª, 19.10.2016	C-582/14	A. Rosas	Breyer c. Bundesrepublik Deutschland
Stichting Brein II, 2.ª, 14.06.2017	C-610/15	M. Ilešič	Stichting Brein c. Ziggo
Bastei Lübbe, Recurso*, Presentado: 16.06.2017	C-149/17		Bastei Lübbe c. M. Strotzer

Tribunal Constitucional

Tribunal, Sala y Fecha	Referencia – BOE	Magistrado Ponente	Partes
STC, Pleno, 30.11.2000	STC 292/2000 – B.O.E. n.º 4, 4.01.2001	Julio Diego González Campos	Recurso de Inconstitucionalidad* Promotor: Defensor del Pueblo

Tribunal Supremo

Tribunal, Sala y Fecha	CENDOJ-Roj	Magistrado Ponente	Partes
STS, 3.ª, 3.10.2014	STS 3896/2014	José María del Riego Valledor	Promusicae c. AEPD y Telefónica

Audiencias Provinciales

Tribunal, Sala y Fecha	CENDOJ-Roj	Magistrado Ponente	Partes
SAP Madrid, Civil Sec. 28.ª, 14.01.2014	SAP M 4/2014	Ángel Galgo Peco	Telecinco c. Youtube

Juzgados de lo Mercantil

Tribunal, Sala y Fecha	CENDOJ-Roj	Magistrado Ponente	Partes
SJM Madrid, Sec. 7.ª, 20.09.2010	SJM M 84/2010	Andrés Sánchez Magro	Telecinco c. Youtube

7. Bibliografía

Antonio CASTÁN PÉREZ-GÓMEZ (2016), "El nuevo régimen de diligencias preliminares en propiedad intelectual frente a las defraudaciones en el entorno digital", en Juan José MARÍN LÓPEZ, Ramón CASAS VALLÉS, Rafael SÁNCHEZ ARISTI (Coordinadores), ET AL., *Estudios sobre la ley de propiedad intelectual: últimas reformas y materiales pendientes*, Dykinson, Madrid, pp. 121 a 154.

Alberto José DE NOVA LABIÁN (2010), *Delitos contra la propiedad intelectual en el ámbito de Internet: (especial referencia a los sistemas de intercambio de archivos)*, Dykinson, Madrid.

María Paula DÍAZ PITA (2015), "Diligencias preliminares y propiedad intelectual tras la reforma operada por la Ley 21/2014, de 4 de noviembre en la Ley de Enjuiciamiento Civil 1/2000, de 7 de enero", en Inmaculada VIVAS TESÓN (Directora), ET AL., *Cuestiones de actualidad en el ámbito de la propiedad intelectual*, Dykinson, Madrid, pp. 175 a 214.

Ramón DURÁN RIVACOBA (2011), "Defensa civil de la propiedad intelectual e identificación del usuario de Internet", *Actualidad Civil,* n.º 10, 16 pp. (consultado en versión electrónica).

F. Javier GARCÍA SANZ y Carles VENDRELL CERVANTES (2013), "Doctrina judicial en torno a las diligencias preliminares en materia de propiedad intelectual", *Diario La Ley,* n.º 8128, 17 de Julio, 10 pp. (consultado en versión electrónica).

Ignacio GARROTE FERNÁNDEZ-DIEZ (2011), "Protección de datos vs. Tutela judicial efectiva en casos de infracción de derechos de propiedad intelectual", *Pe. i.: Revista de propiedad intelectual*, n.º 38, pp. 13 a 75.

Ignacio GARROTE FERNÁNDEZ-DIEZ (2014), *La responsabilidad de los intermediarios en Internet en materia de propiedad intelectual. Un estudio de derecho comparado*, Tecnos D. L., Madrid.

José Javier GONZÁLEZ DE ALAIZA CARDONA, J. J. (2004), "La lucha de los titulares de derechos de autor contra las redes «peer to peer» (P2P)", *Pe. i.: Revista de propiedad intelectual*, n.º 18, pp. 25 a 68.

Alfonso GONZÁLEZ GOZALO (2008), "El conflicto entre la propiedad intelectual y el derecho a la protección de datos de carácter personal en las redes *peer to peer*", *Pe. i.: Revista de propiedad intelectual*, n.º 28, pp. 13 a 68.

Alfonso GONZÁLEZ GOZALO (2005), "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", en *Pe. i.: Revista de propiedad intelectual*, n.º 20, pp. 77 a 134.

Jorge LEDESMA IBÁÑEZ (2011), *Piratería digital en la propiedad intelectual: análisis jurídico de la piratería digital en el ámbito español e internacional*, Bosch, Barcelona.

Pedro LETAI (2012), *La infracción de derechos de propiedad intelectual sobre la obra musical en Internet*, Comares, Madrid.

Patricia LLOPIS NADAL (2018), *La protección de la Propiedad Intelectual vulnerada en Internet: determinación del órgano competente según el sistema español*, Instituto de Derecho de Autor - Colección Premio Antonio Delgado, Madrid.

Patricia LLOPIS NADAL (2018), *Tutela judicial civil de la Propiedad Intelectual en Internet*, Aranzadi-Thomson Reuters, Cizur Menor, consultado en versión electrónica.

Paz LLORIA GARCIA (2016), "La protección penal de la propiedad intelectual tras la reforma del CP de 2015", *La Ley Penal: Revista de derecho penal, procesal y penitenciario*, n.º 121, julio-agosto, 1 de julio, 24 pp.

Julián LÓPEZ RICHART (2016), "El ejercicio de acciones civiles frente a los usuarios de redes P2P antes y después de la Ley 21/2014, de 4 de noviembre", en Juan José MARÍN LÓPEZ, Ramón CASAS VALLÉS, Rafael SÁNCHEZ ARISTI (Coordinadores), ET AL., *Estudios sobre la ley de propiedad intelectual: últimas reformas y materiales pendientes*, Dykinson, Madrid, pp. 343 a 398.

Miguel Ángel MARTÍNEZ AYUSO (2006), "Las redes P2P y la descarga ilegal de contenidos", *Revista Aranzadi de derecho de deporte y entretenimiento*, n.º 18, consultado en versión electrónica.

Gemma MINERO ALEJANDRE (2015), "Medios de tutela de la propiedad intelectual", en Rodrigo BERCOVITZ RODRÍGUEZ-CANO (Director), ET AL, *La Reforma de la Ley de Propiedad Intelectual*, Tirant lo Blanch, Valencia, pp. [363] a 386.
Ana MONTESINOS GARCÍA (2015), "Las diligencias preliminares en materia de propiedad intelectual tras la reforma operada por la Ley 21/2014, de 4 de noviembre", *Pe. i.: Revista de propiedad intelectual*, n.º 50, pp. 35 a 70.

Fernando MORILLO GONZÁLEZ (2015), "Protección de los derechos de propiedad intelectual", en Rodrigo BERCOVITZ RODRÍGUEZ-CANO (Coordinador), *Manual de propiedad intelectual*, Tirant lo Blanch, Valencia, 6ª ed., pp. [307] a 329.

Manuel ORTELLS RAMOS (2015), *Derecho Procesal Civil,* Aranzadi-Thomson Reuters, Cizur Menor, 14ª ed.

Miquel PEGUERA POCH y Marc TARRÉS VIVES (2010), "Marco jurídico de los servicios de la Sociedad de la Información y del Comercio Electrónico", en Miquel PEGUERA POCH (Coordinador), ET AL., *Principios de derecho de la sociedad de la información*, Aranzadi, Cizur Menor, pp. 317 a 389.

Alejandro PUERTO MENDOZA (2015), *Introducción al derecho de Internet; régimen jurídico básico de los contenidos digitales*, CEF, Madrid.

Rafael SÁNCHEZ ARISTI (2007), *El intercambio de obras protegidas a través de las plataformas peer-to-peer*, Instituto de Derecho de Autor, Madrid.

Carmen TOMÁS Y VALIENTE LANUZA (2015), "Delitos contra la Propiedad Intelectual", en José Luís GONZÁLEZ CUSSAC (Director), Elena GÓRRIZ ROYO y Ángela MATALLÍN EVANGELIO (Coordinadoras), *Comentarios a la Reforma del Código Penal de 2015*, Tirant lo Blanch, Valencia, 2ª ed., pp. [843] a 890.