ISSN:0041-9060

UNA COLISIÓN *PEER TO PEER*: *HABEAS DATA VERSUS* DERECHOS DE AUTOR

A *PEER TO PEER* COLISION. *HABEAS DATA VERSUS* COPYRIGHTS

Édgar Iván León Robayo*
Eduardo Secondo Varela Pezzano**

Fecha de recepción: 13 de octubre de 2009
Fecha de aceptación: 1 de marzo de 2010

* Abogado del Colegio Mayor de Nuestra Señora del Rosario (Colombia), donde es profesor de Derecho Civil y Comercial en pregrado y posgrado y coordinador de la Línea de Investigación en Derecho Comercial de la Facultad de Jurisprudencia. Ha sido profesor de las universidades de los Andes y la Sabana. Tiene un posgrado en Derecho Civil de la Universidad de Salamanca (España) y es especialista en Derecho Comercial de la Pontificia Universidad Javeriana. Es candidato al título de Magíster en Derecho Comercial de la Universidad Externado de Colombia. Fue representante por Colombia ante la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (Cnudmi).
Correo electrónico: edgar.leon23@urosario.edu.co

** Abogado y especialista en Propiedad Intelectual del Colegio Mayor de Nuestra Señora del Rosario (Bogotá D.C. - Colombia), donde es profesor de la misma materia. Es autor del libro *Tecnologías peer-to-peer, derechos de autor y copyright* (2009) y coautor de los libros *Derecho de autor para creativos* (2010) y *Derecho del entretenimiento para adultos* (2010). Actualmente es abogado asociado de Reyes & Reyes Abogados.
Correo electrónico: evarela@reyes-abogados.com.

RESUMEN

Las redes P2P les permiten a millones de usuarios en Internet descargar archivos que, al menos en teoría, deberían protegerse por las normas sobre derecho de autor. La reacción de la industria del entretenimiento ha sido iniciar múltiples procesos judiciales en contra de los usuarios de esta tecnología, en diferentes partes del mundo. Uno de los medios que con mayor frecuencia se ha empleado para este propósito ha sido el descubrimiento de la identidad de los usuarios a través de sus direcciones IP, mediante órdenes impartidas por jueces a los proveedores de servicio de Internet. Sin embargo, esta práctica constituye una manifiesta y comprobada violación de derechos constitucionales como el *habeas data* y la privacidad.

Palabras clave: peer-to-peer, habeas data, derecho a la privacidad, derecho de autor, proveedores de servicios de Internet.

Palabras clave descriptor: Protección de datos, proveedores de servicios de internet, derechos de autor.

ABSTRACT

P2P networks allow millions of Internet users to download files that, at least in theory, ought to be protected by the laws of copyright. The entertainment industry's reaction has been to file multiple lawsuits against users of this technology in different parts of the world. One of the measures by which the latter has been achieved has been the discovery of users' identities through their IP addresses by means of judicial orders given to internet service providers. Nevertheless, this practice constitutes a manifest and proven violation of constitutional rights such as habeas data and privacy.

Key words: *peer-to-peer, habeas data, right to privacy, copyright, internet service providers.*

Key words plus: *Data Protection, Internet Service Providers Copyright.*

1. CONSIDERACIONES PREVIAS[1]

Probablemente, uno de los días más importantes en la vida de Guillermo Luis Vélez Murillo fue el 30 de abril del 2008. A pesar de ser abogado de profesión y con el propósito de conseguir un dinero extra, varios años antes decidió gastar su tiempo frente a un computador para transportar la música que se encontraba impresa en viejos y obsoletos acetatos e insertarla, en forma de archivos digitales, en discos compactos. Por cada copia cobraba la módica suma de 5.000 pesos.

Sin embargo, el 8 de octubre de 1999 el inmueble donde realizaba esta actividad fue objeto de una medida de allanamiento, practicada por la Fiscalía General de la Nación. La diligencia, que tuvo como su fuente la denuncia de una reconocida asociación de productores de fonogramas, en la que dieron cuenta de un aviso de periódico donde se promocionaba esta labor, dio como resultado la incautación de cuatro computadores, que tenían instalados programas de *software* que permitían realizar las reproducciones.

Nueve años después, tras haber sido condenado en primera instancia por el Juzgado 21 Penal del Circuito de Bogotá y confirmada esta decisión por el Tribunal Superior de Bogotá, la Sala de Casación Penal de la Corte Suprema de Justicia absolvió de todo cargo al señor Vélez Murillo. En su fallo, la corporación indicó que la descarga de música, películas y otros contenidos protegidos por derechos de autor y derechos conexos, a través de Internet, no es un hecho punible cuando la actuación del usuario no comporta un ánimo de lucro ni la intención de lesionar el patrimonio de una persona[2].

Este pronunciamiento se constituye como el primer precedente jurisprudencial latinoamericano en la materia, y resulta coincidente con tesis similares asumidas por algunos tribunales en Holanda, España, Francia e Italia[3]. Lastimosamente, esa misma suerte no fue corrida por otras personas que han sido demandadas por los mismos hechos en el mundo. Es el caso de Chan Nai-Ming, quien a través del seudónimo *Master of Cunning* fue enviado a prisión por subir películas sin licencia a un servidor de Internet[4]. Igual

---

1 Este artículo es producto del "Proyecto de investigación en propiedad intelectual", que actualmente adelanta la línea de investigación en derecho comercial, del Grupo de Investigación en Derecho Privado, de la Facultad de Jurisprudencia de la Universidad del Rosario (Colombia).

2 "… si en la Internet circulan millones de canciones, no puede concentrarse en el derecho penal la función de perseguir a los usuarios que, aprovechando tal circunstancia, descargan la música que se coloca a su alcance, pues en estos casos como en todos aquellos en los que la persona obra sin ánimo de lucro y sin el propósito de ocasionar perjuicio a la obra o a los intereses económicos del titular de los derechos, resulta imposible afirmar la existencia de una conducta punible, toda vez que no se lesiona o pone efectivamente en peligro el bien jurídico tutelado por la ley". Corte Suprema de Justicia. Sala Penal. Radicación 29188 (M.P. José Leonidas Bustos Martínez. Abril 30 del 2008).

3 Para un relato de estos y otros casos jurisprudenciales, véase: Édgar Iván León Robayo & Eduardo Varela Pezzano. *Panorama jurisprudencial de las tecnologías peer-to-peer.* 18 *Foro de Derecho Mercantil*. Revista Internacional. Legis. Págs. 151-180. (2008).

4 HKSAR *vs.* Chan Nai Ming [2005] 1469 HKCU1. Se trataba de las películas Daredevil, Miss Con-

ocurrió con Jammie Thomas, quien fue condenada a pagar 220.000 dólares por una Corte de Minnesota (Estados Unidos) al declararla culpable de haber compartido más de 1.700 canciones a través de la red[5]. En un segundo proceso, iniciado por razones similares, el jurado la condenó a pagar 1.920.000 dólares por concepto de daños punitivos[6].

Diariamente, las redes *peer to peer* (P2P)[7] les permiten a millones de personas compartir cualquier clase de archivo que contenga música, películas, videojuegos, *software*, libros, entre otros, los cuales, en principio, se encontrarían protegidos por derechos intelectuales. Sin embargo, desde un punto de vista práctico esto resulta difícil, por cuanto la tecnología protege a los usuarios al no permitir su identificación directa, pues al acceder al sistema solamente se registra la dirección de *Internet Protocol* (IP)[8] de su sistema operativo[9].

---

genility y Red Planet. Sin embargo, por no tener antecedentes, el juez le otorgó una pena de tres meses de prisión, a pesar de que por este delito su condena debió ser de cuatro años, de conformidad con las leyes de Hong Kong.

5 Al respecto, véase: Eric Bangeman. *RIAA trial verdict is in: jury finds Thomas liable for infringement*, http://arstechnica.com/news.ars/post/20071004-verdict-is-in (marzo 2 del 2010).

6 Por cada una de las 24 canciones que compartió ilegalmente por Internet, Thomas deberá pagar 80.000 dólares por concepto de daños. Información disponible en http://news.cnet.com/8301-1023_3-10268199-93.html?tag=mncol;txt y http://arstechnica.com/tech-policy/news/2009/06/jammie-thomas-retrial-verdict.ars (mar. 2 del 2010).

7 Para una explicación de la estructura y el funcionamiento de las redes P2P, véanse: Eduardo Varela Pezzano, *Tecnologías peer-to-peer, derechos de autor y copyright*, Págs. 32-46. Centro Editorial Universidad del Rosario. Bogotá. (2009) y Rafael Sánchez Aristi. *El intercambio de obras protegidas a través de plataformas peer to peer*. Pág. 43. Instituto de Derecho de Autor. Madrid. (2007).

8 La IP es la "… dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y, por lo tanto, es única. La dirección IP está compuesta de cuatro octetos, como 132.248.53.10". Erick Rincón Cárdenas. *Manual de comercio electrónico y de Internet*. Pág. 388. Centro Editorial Universidad del Rosario. Bogotá. (2006).

9 Igualmente, los creadores de los programas P2P utilizan mecanismos como sobrenombres –*nicknames*– y contraseñas que impiden conocer, con estricta certeza, la identidad del usuario. Precisamente, esta fue la defensa planteada en el caso *The Pirate Bay*. Esta página web fue fundada en el 2003 por la organización sueca *Piratbyrån* –oficina pirata–. En ella es posible buscar y descargar archivos *torrents* organizados en diferentes categorías: audio, video, *software*, juegos, pornografía, etc. Para registrarse, el usuario sólo requiere una dirección de correo electrónico. El 16 de febrero del 2009 se inició un juicio penal en la Corte de Distrito de Estocolmo contra los administradores del portal, por "promocionar la infracción de terceros a las leyes del derecho de autor" –Corte de Distrito de Estocolmo. Caso nº B 13301-06. Abril 17 del 2009–. Entre las distintas acusaciones se decía que *The Pirate Bay* era un negocio inmensamente rentable que hacía dinero ayudando a otros a violar el derecho de autor. Así mismo, "… el asistir a una 'puesta a disposición', violatoria de tales derechos. El abogado de la parte acusada, Per Samuelson, argumentó la famosa "defensa King Kong" –*King Kong defense*–: "… [la] Directiva de la UE 2000/31/CE dice que aquel que proporciona un servicio de información no es responsable por la información que se transfiere. Para ser responsable, el prestador de servicios debe iniciar la transferencia. Pero los administradores en *The Pirate Bay* no inician las transferencias. Son los usuarios los que lo hacen y ellos son físicamente identificables. Se llaman a sí mismos con nombres como King Kong (...). De acuerdo con las normas de procedimiento, las acusaciones deben hacerse contra un individuo al tiempo que debe haber una estrecha relación entre los autores de un delito y los que están ayudando. Este vínculo no se ha demostrado. El fiscal debe demostrar que Carl Lundström –uno de los acusados– colaboró personalmente con el usuario King Kong, quien puede perfectamente encontrarse en las selvas de Camboya...". El 3 de marzo del 2009,

Aunque no es posible precisar exactamente quién es la persona que realiza una descarga ilegal, sería posible identificar el titular del computador correspondiente, a través de las bases de datos de las que dispone el proveedor del servicio de Internet (ISP)[10] respectivo. No obstante, esta circunstancia puede dar lugar a una violación directa de los derechos de *habeas data* y privacidad, no sólo por el monitoreo de la actividad sino también por la utilización no autorizada de la información personal y secreta del usuario.

Este trabajo tiene como propósito analizar las consecuencias legales de revelar la identidad de los usuarios P2P, en desarrollo de la observancia y litigiosidad del derecho de autor en Internet. Para ello, se precisará en qué consisten estos programas informáticos y se estudiarán los principales casos en los que se ha otorgado primacía al derecho a la privacidad de los usuarios P2P sobre el de los titulares de derechos de autor. Posteriormente, el análisis se encaminará a analizar el tratamiento del problema según el ordenamiento jurídico colombiano y la manera como opera la responsabilidad del ISP que revela la identidad de los usuarios que a diario descargan y comparten contenidos protegidos por el derecho de autor.

2. EL SIGNIFICADO DE LAS TECNOLOGÍAS P2P

Los programas informáticos P2P les permiten a los usuarios conectarse a través de una red interactiva de computadores, especialmente Internet, mediante la cual descargan[11] archivos digitales de música, películas, libros, fotos y *software* que se encuentran disponibles en los sistemas de otros usuarios. Los documentos son susceptibles de ser compartidos "de computador a computador", de manera gratuita, previa digitación de sobrenombres[12] y claves de ingreso[13], que garantizan la reserva de información. Esto ha dado lugar a que el uso de tales programas sea objeto de múltiples críticas, por cuanto la descarga sin costo de los archivos hace que los autores de las obras protegidas no obtengan la remuneración debida por su trabajo y que el derecho que tienen a explotar sus obras no les sea reconocido.

Fredrik Neij, Gottfrid Svartholm y Peter Sunde, administradores del sitio web, y Carl Lundström, un hombre de negocios que vendía servicios a través del nombre *The Pirate Bay*, fueron condenados a un año de cárcel y a pagar 30 millones en coronas suecas –aproximadamente unos 2,7 millones de euros o 3,5 millones de dólares, es decir, unos 8.050 millones de pesos colombianos– por "ayudar a infringir derechos de autor". No obstante, el caso fue apelado el 23 de abril sobre la base de una supuesta falta de imparcialidad del juez que dictó la sentencia –Tomas Norström–, quien era miembro de la *Svenska Föreningen för Upphovsrätt*, o sea, la Asociación Sueca del Derecho de Autor.

10 En inglés: *Internet service providers*.

11 El vocablo **descargar** –*download*– es entendido como: "... recibir información, típicamente un archivo, desde otra computadora a través de un módem (...). Por su parte, el término contrario sería **subir** –*upload*–, que significa enviar un archivo a otra computadora" –United States *vs*. Mohrbacher. 182 F.3d 1041, 1048 (9.th Cir. 1999)–.

12 En inglés: *nicknames*.

13 En inglés: *passwords*.

En efecto, si la industria del entretenimiento conociera la verdadera identidad de usuarios registrados con sobrenombres como geekboy@KaZaa, chickiepoo25@KaZaa y mr_socks@KaZaa,[14] no se producirían descargas ilegales de música, películas, videojuegos, libros y *software*. Ese rastro les permitiría a los titulares de derechos de autor y conexos, y a sus entidades de gestión,[15] identificar con certidumbre a los supuestos usuarios infractores[16].

3. DIFICULTADES QUE PLANTEA EL DERECHO A LA PRIVACIDAD FRENTE A LA VIOLACIÓN DE DERECHOS DE AUTOR POR EL USO DE TECNOLOGÍAS P2P

La falta de precisión en la identificación de los usuarios P2P ha dado lugar a que las acciones interpuestas por los autores o por sus entidades de gestión colectiva por descargas ilegales en el mundo hayan sido dirigidas, en ciertas ocasiones, contra personas equivocadas. En efecto, algunas de esas demandas se han interpuesto contra menores de edad[17], amas de casa[18], personas fallecidas[19] o, incluso, contra sujetos que no tienen computador o que ni siquiera conocen su funcionamiento[20].

De esta manera, para identificar a un usuario P2P y determinar si ha descargado copias ilegales de obras protegidas por el derecho de autor primero se debe localizar su *nickname* o su número IP y, posteriormente, desenmascarar a la persona que se oculta detrás de este último, de tal manera que se pueda iniciar la acción judicial correspondiente[21]. Sin embargo, el problema

---

14 Algunos de los *nicknames* involucrados en el litigio BMG Canada Inc. *vs.* John Doe. 2004 FC 488 aff'd 2005 FCA 193.

15 "Por gestión colectiva se entiende el sistema de administración de derechos de autor y de derechos conexos por el cual sus titulares delegan en organizaciones creadas al efecto la negociación de las condiciones en que sus obras, sus prestaciones artísticas o sus aportaciones industriales –según el caso– serán utilizadas por los difusores y otros usuarios primarios, el otorgamiento de las respectivas autorizaciones, el control de las utilizaciones, la recaudación de las remuneraciones devengadas y su distribución o reparto entre los beneficiarios". Delia Lypszyc. *Derecho de autor y derechos conexos*. Pág. 407. Unesco. Buenos Aires. (1993).

16 Así mismo, algunos programas que permiten la descarga de contenidos sin autorización de los titulares de derechos de autor y conexos encubren a sus usuarios al mostrar únicamente su número de IP, que podría ser, por ejemplo, uno similar a 175.45.98.303.

17 Nate Mook, *RIAA sues 261, including 12-year-old girl*, *BetaNews*, sep. 9/2003. www.betanews.com/article/1063159635 (mar. 2 del 2010).

18 Lewan *vs.* Sharman, U.S. Dist. Ct., N.D. Ill 06-cv-6736.

19 Eric Bangeman. *I sue dead people...*, *Ars Technica*. feb. 4/2005, http://arstechnica.com/old/content/2005/02/4587.ars, (mayo 21 del 2009).

20 Chris Gaither. *Recording Industry Withdraws Suit*. *The Boston Globe*. septiembre 24 del 2003.

21 Así ocurrió, por ejemplo, con la orden proferida por un juez del distrito de Nueva York (Estados Unidos), quien ordenó a la compañía Google, Inc. revelar a la empresa Viacom Inc. cada registro de cada video visto por sus usuarios en el sitio web YouTube.com, incluyendo los nombres de los usuarios y sus direcciones IP. Esta decisión, de julio del 2008, la cual no tenía precedente alguno en Estados Unidos, obedeció a una acción civil que interpusiera Viacom contra el famoso sitio de videos digitales

resulta altamente complejo en aquellos Estados donde se consagra el derecho constitucional al *habeas data*[22] y a la privacidad personal, por cuanto estos sistemas legales no permiten sancionar a los presuntos infractores.

Para efectos de entender con claridad la manera como se ha debatido este problema por los diferentes tribunales de justicia, a continuación se hará referencia a las principales decisiones que sobre la materia han sido decididas en diversas partes del mundo.

3.1. Canadá

En el caso Socan *vs.* CAIP, la Corte Suprema de Canadá señaló que la navegación de una persona en Internet y sus actividades de descarga tendían a revelar información personal sobre ella misma. De esta manera, afirmó: "Los intereses íntimos de los individuos estarán directamente implicados donde los propietarios de obras protegidas o sus sociedades colectivas intenten recupe-

---

en internet y su central Google, acusándolas de infringir masivamente sus derechos de *copyright*. La demanda constituye la disputa legal más significativa hasta la fecha para Google y YouTube, pues la indemnización reclamada asciende a más de 1.000 millones de dólares en perjuicios –al respecto, véase: Viacom International, Inc. *et al vs.* YouTube, Inc. *et al*, 07 Civ. 2103 (LLS)–. Lo cierto es que, cuando Google compró YouTube, reconoció la posibilidad de que el sitio web algún día sería objeto de disputas y controversias legales relacionadas con los derechos de autor. Incluso, destinó una cuantiosa suma de dinero para el financiamiento de litigios futuros. A pesar de lo anterior, los expertos advirtieron que YouTube correría la misma suerte que Napster, el popular *software* P2P declarado en bancarrota luego de ser condenado al pago de perjuicios por infracción al *copyright* –véase: Eduardo Varela Pezzano. *Videos que se están viendo ahora: Viacom vs. YouTube revisado*, 1 Opinión Independiente, 3. Colegio Mayor de Nuestra Señora del Rosario. Bogotá. (2007)–. Google, que contestó la demanda en abril del 2007, se limitó a negar todos los cargos imputados por Viacom. Su principal defensa fue remitirse a la *Digital Millennium Copyright Act* (DMCA) [17 U.S.C. § 512] y a los *safe harbors*, disposiciones que salvaguardan a los proveedores de servicios en internet para que no puedan ser demandados por infracción al *copyright*, mientras no se les requiera primero que detengan la actuación infractora –Universal City Studios, Inc. *vs.* Reimerdes, 111 F.Supp.2d 294 (S.D.N.Y. 2000); Chamberlain *vs.* Skylink, 381 F.3d 1178 (Fed. Cir. 2004); y Lexmark Int'l, Inc. *vs.* Static Control Components, Inc. 387 F.3d 522 (6th Cir. 2005)–. Siguiendo las pautas de la DMCA y de los *safe harbors*, en febrero del 2007 Viacom notificó a YouTube acerca de más de 100.000 videos ilegales que se encontraban en su servidor y que violaban su *copyright*. El problema surgió cuando YouTube omitió impedir que sus usuarios publicaran otros videos ilegales. En efecto, tan pronto como Viacom solicitaba que estos fueran retirados, los usuarios inmediatamente publicaban nuevas versiones de los mismos.

22 Esto ocurre, por ejemplo, en Argentina, Canadá, España, Francia, Paraguay y Perú. Igualmente, en Colombia, donde esta figura fue regulada mediante la Ley 1266 del 31 de diciembre del 2008 "Por la cual se dictan las disposiciones generales del *habeas data* y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones". En ella se consagra el principio de confidencialidad, de conformidad con la cual: "Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos...". De lo anterior se desprende una reserva de confidencialidad respecto de la actividad de los usuarios del servicio de Internet, pues debe entenderse que la norma se extiende y obliga a los proveedores a no revelar las direcciones IP de sus clientes. Debe indicarse, además, que esta normativa fue declarada exequible por la Corte Constitucional –Sentencia C-1011 (m.p. Jaime Córdoba Triviño. octubre 16 del 2008)–.

rar datos de los proveedores del servicio de Internet sobre la descarga de un usuario final. Nosotros, por lo tanto, deberíamos ser prudentes en adoptar una prueba que puede animar tal supervisión"[23].

3.2. Francia

En el año 2006, el Tribunal Correctionnel de la Comuna de Bobigny profirió una sentencia[24] en la que absolvió a un usuario P2P que compartía más de 12.000 archivos ilegales en la red. La decisión tuvo como fundamento la violación de la intimidad personal del acusado, lo cual ocurrió al momento de identificar y registrar su dirección IP. Según su criterio, el proceso para descubrir al sindicado y obtener las pruebas de las descargas se hizo sin autorización de la Commission Nationale de l'Informatique et des Libertés (CNIL)[25], entidad administrativa encargada de proteger la libertad y privacidad informática[26]. Para el alto tribunal, esto no era otra cosa diferente que una evidente violación al derecho de información y privacidad del acusado.

En consecuencia, para el sistema legal francés también resulta inadmisible monitorear el uso del P2P y, por lo tanto, es prácticamente improbable que se sancione a quienes cometan ese tipo de conductas cuando se persiga su desenmascaramiento a través de las direcciones IP.

3.3. La Unión Europea

El Tribunal de Justicia de las Comunidades Europeas (TJCE) abordó este asunto[27] en una interpretación prejudicial[28] que acogió la postura de los proveedores de Internet. En su alegato, ellos abogaron por la privacidad de los usuarios de las redes P2P, dejando de lado las pretensiones de la industria del entretenimiento en relación con la reclamación de daños y perjuicios relacionados con la infracción del derecho de autor. Según el fallo, los Estados europeos no están obligados a extender el deber de informar datos privados en virtud de la *Carta de Derechos Fundamentales*[29], que protege no sólo la

23 Society of Composers, Authors and Music Publishers of Canada *vs*. Canadian Association of Internet Providers, SCC 45. (2004).

24 Estelle Dumout. *Un Adepte du Peer-to-Peer Relaxé Grâce à un Vice de Procédure*. diciembre 19 del 2006, www.zdnet.fr/actualites/internet/0,39020774,39365738,00.htm (mayo 21 del 2009).

25 Comisión Nacional de la Información y las Libertades.

26 El Tribunal de París también absolvió a un usuario de redes P2P bajo la presunción de que éste no tenía la intención de infringir estos derechos, pues el *software* que utilizaba compartía archivos de manera automática sin su consentimiento –véase Tribunal de Grande Instance du Paris, diciembre 8 del 2005–.

27 TJCE, Asunto C-275 del 2006, enero 29 del 2008.

28 El artículo 234 del Tratado de la Comunidad Europea (TCE) establece que el TJCE es competente para pronunciarse con carácter prejudicial sobre la interpretación del TCE y sobre la validez e interpretación de los actos adoptados por la Comunidad Europea.

29 Véase: www.europarl.europa.eu/charter/pdf/text_es.pdf (marzo 11 del 2010).

propiedad[30] y la tutela judicial efectiva[31] sino también los datos personales y la intimidad[32].

Los hechos que originaron la decisión tuvieron como fundamento un procedimiento judicial de diligencias preliminares, el cual fue interpuesto por Productores de Música de España (Promusicae) en noviembre del 2005 contra Telefónica –en su calidad de ISP–. En su querella, la demandante solicitó que se revelaran los nombres y direcciones de algunos usuarios de redes P2P, susceptibles de identificación por sus números IP, así como la fecha y hora de conexión. Con base en la interpretación prejudicial del TJCE, el Juzgado Mercantil nº 5 de Madrid sentenció que los datos personales de los usuarios P2P "… no pueden ser cedidos sin consentimiento del interesado" a una entidad privada, como Promusicae[33].

3.4. Latinoamérica

Aunque todavía no existe una legislación específica que regule esta materia en ninguno de los países de la región, existe un problema similar para sancionar las descargas ilegales. Por ejemplo, el artículo 4º de la Ley 1682 del 2000 de Paraguay[34], conocida como la Ley de Privacidad, prohíbe "… dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables".

Para esta normativa, datos sensibles son aquellos que afectan "… la dignidad, la privacidad, la intimidad doméstica y la imagen privada de personas o familias". Como la tecnología de redes P2P es utilizada para la descarga de copias de uso personal, se puede concluir que en ese país no es posible identificar a los usuarios infractores, por el hecho de que con ello se invadiría la esfera de lo privado.

Igual ocurre en Argentina, con la Ley 25326 sobre Protección de Datos Personales,[35] la cual tiene por objeto: "… la protección integral de los datos personales (...) sean estos públicos, o privados (...) para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre..."[36]. En ese mismo orden, tampoco podría divulgarse ninguna información acerca de quienes descargan archivos ilegales en ese país.

---

30 Art. 17.
31 Art. 47.
32 Arts. 7º y 8º.
33 Véase: www.adslnet.es/index.php/2008/06/22/el-p2p-seguira-siendo-anonimo-segun-sentencia-judicial-a-favor-de-telefonica/ (mayo 21 del 2009).
34 Expedida el 28 de diciembre del 2000, en Paraguay.
35 Sancionada el 4 de octubre y promulgada parcialmente el 30 de octubre del 2000.
36 Art. 1º.

Perú, Estado miembro de la Comunidad Andina[37] (CAN), se ubica en el mismo contexto. La Carta Política de ese país establece que toda persona tiene derecho "… a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afectan la intimidad personal y familiar"[38]. De tal forma, los ISP peruanos no podrían divulgar información de los usuarios que emplean las redes P2P para distribuir y compartir contenidos protegidos por el derecho de autor. En tal sentido, tampoco se podría sancionar la conducta de descargar música a través de estos sistemas, por atentar contra el derecho constitucional al *habeas data*.

Con respecto a esta figura, el Tribunal Constitucional peruano ha sostenido que se trata de un proceso que permite "… acceder a los registros de información almacenados en centros informáticos o computarizados, cualquiera que sea su naturaleza, y a fin de rectificar, actualizar, excluir determinado conjunto de datos personales, o de impedir que se propague información que pueda ser lesiva al derecho constitucional a la intimidad"[39].

Por su parte, la doctrina peruana también ha recalcado que, atendiendo al tenor gramatical de la norma, el *habeas data* tiene la finalidad última de "… proteger a la persona evitando que servicios informáticos suministren datos o informaciones que afecten la intimidad personal"[40]. Es decir, procede para evitar que se suministre información que afecte la vida privada de las personas, como sería la que se divulgue si se descarga cualquier contenido a través de una red P2P.

4. LA CUESTIÓN EN EL ORDENAMIENTO JURÍDICO COLOMBIANO

Al igual que en Perú, Argentina y Paraguay, en Colombia el *habeas data* alude al conjunto de derechos de toda persona con respecto a la información que sobre ella se encuentra en registros o bases de datos públicos o privados[41]. De

37 La Comunidad Andina, organización integrada por Bolivia, Colombia, Ecuador y Perú, cuenta con la Decisión 351 de 1993 para la protección de los derechos de autor. Esta normativa tiene como finalidad: "Reconocer una adecuada y efectiva protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino" (art. 1°). De la misma forma, la protección reconocida por la decisión recae sobre todas las obras "… literarias, artísticas y científicas que puedan reproducirse o divulgarse por cualquier forma o medio conocido o por conocer" (art. 4º). Si se tiene en cuenta que el P2P es uno de estos medios, puede concluirse que la CAN goza de una protección adicional y especial para los derechos de autor en este ámbito, a la cual se le aplicarían todas las disposiciones regionales en la materia.

38 Art. 2º, num. 6º.

39 Tribunal Constitucional del Perú, Expediente 666-96-HD, Sentencia julio 8 de 1998.

40 Francisco Eguiguren. *Poder judicial, tribunal constitucional y habeas data en el constitucionalismo peruano*. Pág. 64. Cuadernos Constitucionales México-Centroamérica. 1ª ed. México. (1999).

41 Comisión Andina de Juristas. *El proceso de habeas data en la Región Andina. Análisis comparado*, www.cajpe.org.pe/guia/3.pdf (marzo 2 del 2010).

esta manera, si se presenta la oportunidad, las cortes otorgarían protección al derecho a la privacidad de los usuarios de redes P2P frente a peticiones inconsultas de su IP a los ISP, por quienes pretenden la protección autoral.

De hecho, la Corte Constitucional colombiana ha empleado la expresión *habeas data* para desarrollar el contenido del derecho a la privacidad, reconocido por el artículo 15[42] de la Constitución Política[43]. En efecto, el alto tribunal ha establecido que este se constituye como un derecho fundamental, traducido en la facultad que tiene la persona a la cual se refieren los datos privados para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales[44].

Igualmente, la corporación ha definido el derecho a la privacidad como "… aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales (…) la (…) exclusión (…) de los datos, así como la limitación en la posibilidad de divulgación, publicación o cesión de los mismos, todo conforme a los principios que informan el proceso de administración de bases de datos personales"[45].

En cuanto a la vida privada de las personas, la Corte ha sostenido que el derecho a la intimidad es una "… forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad. Esta particular naturaleza suya determina que la intimidad sea un derecho general, absoluto, extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer *erga omnes*, vale decir, tanto frente al Estado como frente a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular *a priori* de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada"[46].

---

42 "Todas las personas tienen derecho (...) a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas...".

43 Corte Constitucional. Sentencias T-002 (m.p. Alejandro Martínez Caballero. Mayo 8 de 1992); T-414 (m.p. Ciro Angarita Barón. Junio 16 de 1992); C-479 (m.p. José Gregorio Hernández Galindo y Alejandro Martínez Caballero. Agosto 13 de 1992); T-022 (m.p. Ciro Angarita Barón. Enero 29 de 1993); C-114 (m.p. Fabio Morón Díaz. Marzo 25 de 1993); T-389 (m.p. Hernando Herrera Vergara. Septiembre 15 de 1993); T-459 (m.p. Hernando Herrera Vergara. Octubre 13 de 1993); T-460 (m.p. Hernando Herrera Vergara. Octubre 13 de 1993); SU-528 (m.p. José Gregorio Hernández Galindo. Noviembre 11 de 1993); T-017 (m.p. José Gregorio Hernández Galindo. Enero 30 de 1995); SU-082 (m.p. Jorge Arango Mejía. Marzo 1º de 1995); SU-089 (m.p. Jorge Arango Mejía. Marzo 1º de 1995); T-097 (m.p. José Gregorio Hernández Galindo. Marzo 3 de 1995); T-119 (m.p. José Gregorio Hernández Galindo. Marzo 16 de 1995); T-552 (m.p. Vladimiro Naranjo Mesa. Noviembre 1º de 1997); C-662 (m.p. Fabio Morón Díaz. Junio 8 del 2000); C-831 (m.p. Álvaro Tafur Galvis. Agosto 8 del 2001); C-1147 (m.p. Manuel José Cepeda Espinosa. Octubre 31 del 2001); T-729 (m.p. Eduardo Montealegre Lynett. Septiembre 5 del 2002) y C-356 (m.p. Jaime Araújo Rentería. Mayo 6 del 2003).

44 Corte Constitucional. Sentencia SU-082 (m.p. Jorge Arango Mejía. Marzo 1º de 1995).

45 Corte Constitucional. Sentencia T-729 (m.p. Eduardo Montealegre Lynett. Septiembre 5 del 2002).

46 Corte Constitucional. Sentencia T-414 (m.p. Ciro Angarita Barón. Junio 16 de 1992).

De esta manera, los ISP en Colombia no podrían revelar la identificación IP de los usuarios que descargan contenidos a través de las redes P2P. Ello sería contrario al derecho que tienen los colombianos a autorizar, en forma expresa y voluntaria, la divulgación de su información íntima y personal. Adicionalmente, tampoco podrían ser sancionados aquellos que realicen descargas que no tienen como fin obtener un ánimo de lucro, de conformidad con lo indicado por la Sala Penal de la Corte Suprema de Justicia en su fallo del 30 de abril del 2008, citado en la introducción de este artículo[47].

5. LA RESPONSABILIDAD DE LOS ISP POR LA REVELACIÓN DE DATOS DE USUARIOS P2P

Ha quedado demostrado que los derechos al *habeas data* y a la privacidad impiden que los ISP puedan divulgar la identidad de quienes utilizan plataformas P2P para descargar archivos que, al menos en teoría, deberían estar protegidos por el derecho de autor. Por tal razón, cabe preguntarse cuál sería la responsabilidad en que podrían incurrir tales proveedores en el evento en que revelasen los datos de usuarios P2P, en contravención de los derechos constitucionales indicados.

En la actualidad, no existe un régimen de responsabilidad de los ISP en Colombia[48]. La única preceptiva vigente que reglamenta una situación de hecho en que estos podrían ser sancionados por ocasión de su conducta es el artículo 9º del Decreto 1524 del 2002, que reglamenta la Ley 679 del 2001 "por medio de la cual se expide un Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución[49].

De conformidad con esta normativa, los proveedores o servidores, administradores y usuarios que no cumplan o infrinjan las obligaciones y deberes establecidos en ella están sujetos a la imposición de multas que van hasta los cien (100) salarios mínimos legales mensuales vigentes o la suspensión o cancelación de la correspondiente página web[50]. Tales sanciones son impuestas por el Ministerio de Comunicaciones mediante la apertura de una investigación administrativa, sin perjuicio de las acciones penales a las que haya lugar.

Sin embargo, se puede afirmar que, por virtud del régimen de responsabilidad extracontractual civil contenido en el artículo 2341 del Código Civil,[51] los ISP están obligados a responder "… por los daños que ellos causen con dolo –conocimiento–, o con grado de negligencia de cierta magnitud –con el

47 Radicación 29188, *supra* nota 2.
48 Como punto de referencia, véase: Rincón Cárdenas, *supra* nota 8, 176-181.
49 Véase: www.colomsat.net.co/Decreto_201524_20240702.pdf (mayo 21 del 2009).
50 Art. 10.
51 "El que ha cometido un delito o culpa, que ha inferido daño a otro, es obligado a la indemnización, sin perjuicio de la pena principal que la ley imponga por la culpa o el delito cometido".

deber de tener conocimiento–"[52]. Así ocurriría, por ejemplo, cuando uno de ellos haya revelado a un tercero la identidad de un usuario P2P, a sabiendas de que está violando sus derechos constitucionales, o que por descuido u omisión haya facilitado la dirección IP de una persona sin su autorización.

Sin embargo, esto no podría entenderse como una apología de las descargas que se realizan en redes P2P sin retribución económica para los titulares de derechos de autor y conexos. Por el contrario, se trata de una reflexión que parte del principio de conformidad con el cual los derechos fundamentales –especialmente, la privacidad y el *habeas data*– priman sobre las demás normas del ordenamiento jurídico –cualquiera sea su rango legal–, como serían las referidas a la protección.

52 Carlos M. Álvarez. *Responsabilidad de los ISP en Colombia*, *Internet, comercio electrónico & telecomunicaciones*, Pág. 703. Grupo de Estudios en Internet, Comercio Electrónico & Telecomunicaciones e Informática. Legis. Bogotá. (2002).

CONCLUSIONES

El 14 de marzo del 2009, Verizon Communications inició las pruebas tendientes a desarrollar una nueva infraestructura tecnológica que permitirá conseguir una mejora significativa en las descargas P2P y descongestionará el tráfico de datos en la web. Este nuevo sistema, denominado *Proactive Network Provider Participation for P2P* (P4P)[53], les permitirá a los usuarios seleccionar de manera inteligente la información, a través de un protocolo que utiliza datos de topología de red para maximizar la eficacia de los datos enviados por los ISP a las conexiones P2P. Con ello, según mediciones de la compañía, P4P incrementaría entre un 200 y un 600% la velocidad de descarga entre usuarios P2P, gracias a un mecanismo informático que reducirá el ancho de banda utilizable.

Según Verizon, esta plataforma solamente sería aplicable en servicios comerciales legales. Sin embargo, es probable que termine siendo utilizada para realizar descargas de información protegida por derecho de autor y *copyright*. Esta situación dará lugar a que se les continúe generando pérdidas incalculables a los titulares de las obras y de derechos conexos de todo el mundo.

Es evidente que la tecnología avanza día a día a pasos agigantados. Por ello, es necesario construir mecanismos que les permitan a los millones de afectados por estas conductas iniciar acciones en contra de los usuarios P2P, con los cuales se eviten excesos que vulneren derechos fundamentales[54]. Como ha quedado indicado, revelar la identidad de los usuarios a través de sus direcciones IP, mediante órdenes impartidas por jueces a los ISP, ha sido la forma más utilizada por los afectados para obtener protección de sus derechos.

No obstante, este tipo de decisiones constituye una manifiesta violación directa al derecho a la privacidad, pues se trata de información que se encuentra reconocida y protegida, en la mayor parte de los casos, por normas constitucionales. Esto ocurre, además, con el *habeas data*, el cual ha sido reconocido en Colombia como el derecho fundamental que tiene toda persona a proteger la información que de ella se encuentra depositada en registros o bases de datos públicos o privados.

---

53 Véase: http://arstechnica.com/old/content/2008/03/verizon-embraces-p4p-a-more-efficient-peer-to-peer-tech.ars (mayo 21 del 2009).

54 Para ello se requiere mucha creatividad en la generación de estrategias seguras que permitan alcanzar este fin. Ejemplo de lo anterior, es la posibilidad que existe de descargar música directamente de páginas web, mediante un pago *on-line*. Así mismo, ocurre con frecuencia que se generan contratos de colaboración empresarial entre los titulares de derechos de autor y *copyright* con compañías de telefonía móvil celular, quienes venden los teléfonos cargados con archivos de video o música –es el caso de Shakira o Juanes, que cedieron los derechos de sus últimas producciones musicales a Sony Ericsson–. Otra forma de evitar pérdidas por descargas ilegales es la comercialización de obras protegidas a precios muy bajos, pero con una promoción y circulación realizada en masa, como ocurrió con el último disco de Carlos Vives –Clásicos de la provincia II–, el cual fue promocionado y vendido a través de todos los supermercados Éxito.

Aunque el uso de las tecnologías P2P se encontraría tipificado por la legislación nacional como un delito contra los derechos de autor, a menos que se trate de circunstancias en las cuales las descargas no tengan un ánimo de lucro, como lo ha señalado la jurisprudencia de la Sala de Casación Penal de la Corte Suprema de Justicia, en ningún evento sería posible monitorear las direcciones IP de los usuarios.

En principio, el ordenamiento jurídico colombiano no contiene ninguna preceptiva que establezca responsabilidad alguna en cabeza de los ISP, salvo lo previsto en la Ley 679 del 2001, así como su decreto reglamentario, en materia de protección a los menores por abuso sexual. Sin embargo, debe precisarse que el Congreso de la República aprobó la Ley 1143 del 2007, por medio de la cual se aprueba el "Acuerdo de promoción comercial entre la República de Colombia y los Estados Unidos de América", sus "Cartas adjuntas" y sus "Entendimientos", suscritos en Washington el 22 de noviembre del 2006[55].

Este instrumento, del que se espera una próxima aprobación por parte del legislador del país norteamericano, consagra una obligación especial para el Gobierno colombiano, consistente en el deber de establecer "… limitaciones relativas al alcance de los recursos disponibles contra los ISP por infracciones a los derechos de autor que ellos no controlen, inicien o dirijan, y que ocurran a través de sistemas o redes controladas u operadas por ellos, o en su representación…"[56]. Aunque es claro que tales limitaciones serían por el momento inoperables, pues el ordenamiento jurídico nacional no contempla sanciones contra los ISP por infracciones contra el derecho de autor que no hayan sido perpetradas ni ordenadas por ellos, el TLC consagra que la elegibilidad de las mismas no puede estar condicionada a que el proveedor monitoree su servicio o que "… decididamente busque hechos que indiquen una actividad infractora"[57]. De ello se colige que no sólo están exentos de revelar la identidad de los usuarios P2P, sino que, en un futuro, cuando el Congreso regule las limitaciones relativas a su responsabilidad sobre la materia, estas ni siquiera puedan estar supeditadas al deber de monitorear personas que infrinjan derechos de autor en sistemas o redes controladas u operadas por ellos.

En otras palabras, los ISP colombianos tampoco estarán obligados a inspeccionar la conducta lícita o ilícita en que incurran los adeptos a redes P2P. Además, si lo estuvieran, encontrarían una adecuada barrera de protección constitucional para desconocer tales órdenes: el *habeas data* y el derecho a la intimidad.

---

55 Véase www.temascomunicaciones.com.co/leyes/leyes/ley%201143.htm (marzo 9 del 2010).
56 Art. 16.11(29)(b).
57 Art. 16.11(29)(b)(vii).

BIBLIOGRAFÍA

Carlos M. Álvarez, *Responsabilidad de los ISP en Colombia*, *Internet, comercio electrónico & telecomunicaciones*. Pág. 703. Grupo de Estudios en Internet, Comercio Electrónico & Telecomunicaciones e Informática. Legis. Bogotá. (2002).

Eric Bangeman. *I sue dead people...*, *Ars Technica*. febrero 4 del 2005. http://arstechnica.com/old/content/2005/02/4587.ars, (mayo 21 del 2009).

Eric Bangeman. *RIAA trial verdict is in: jury finds Thomas liable for infringement*. http://arstechnica.com/news.ars/post/20071004-verdict-is-in. (mayo 21 del 2009).

John Borland. *Canada deems P2P Downloading Legal*. (2003). http://news.com.com/2100-1025_3-5121479.html (mayo 21 del 2009).

Comisión Andina de Juristas. *El proceso de* habeas data *en la Región Andina. Análisis comparado*, www.cajpe.org.pe/guia/3.pdf (marzo 2 del 2010).

Estelle Dumout. *Un Adepte du Peer-to-Peer Relaxé Grâce à un Vice de Procédure*. diciembre 19 del 2006. www.zdnet.fr/actualites/internet/0,39020774,39365738,00.htm (última visita. mayo 21 del 2009).

Francisco Eguiguren. *Poder judicial, tribunal constitucional y habeas data en el constitucionalismo peruano*. 64. Cuadernos Constitucionales México-Centroamérica. 1ª ed. México. (1999).

Chris Gaither. *Recording Industry Withdraws Suit*, *The Boston Globe*. (2003).

Édgar Iván León Robayo & Eduardo Varela Pezzano. *Antinomia entre la protección a los autores y el derecho a la privacidad por la batalla legal contra las tecnologías P2P.* 111. Revista Facultad de Derecho y Ciencias Políticas. Universidad Pontificia Bolivariana (próxima publicación) (2010).

_____. *Panorama jurisprudencial de las tecnologías peer-to-peer.* 18. Foro de Derecho Mercantil, Revista Internacional. Legis. (2008). Pág. 151.

Delia Lypszyc. *Derecho de autor y derechos conexos*. Pág. 407. Unesco. Buenos Aires. (1993).

Nate Mook. *RIAA sues 261, including 12-year-old girl*, *BetaNews*. septiembre 9 del 2003. www.betanews.com/article/1063159635 (marzo 2 del 2010).

Office de la Propriété Intellectuelle du Canada, *A Guide to Copyrights*. (2005). www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/wr00037.html (mayo 21 del 2009).

Erick Rincón Cárdenas. *Manual de comercio electrónico y de Internet*. 388. Centro Editorial Universidad del Rosario. Bogotá. (2006).

Rafael Sánchez Aristi. *El intercambio de obras protegidas a través de plataformas* peer to peer. 43. Instituto de Derecho de Autor. Madrid. (2007).

Eduardo Varela Pezzano. *Tecnologías peer-to-peer, derechos de autor y copyright*. Págs. 32-46. Centro Editorial Universidad del Rosario. Bogotá. (2009).

_____. *Videos que se están viendo ahora: Viacom vs. YouTube revisado*. 1 Opinión Independiente, 3. Colegio Mayor de Nuestra Señora del Rosario. Bogotá. (2007).