Revista FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS. Vol. 39, No. 111 / **p. 203-225**
Medellín - Colombia. Julio-Diciembre de 2009, ISSN 0120-3886

Antinomia entre la protección a los autores y el derecho a la privacidad por la batalla legal contra las tecnologías P2P[1]

Antinomy Between Copyright and the Right to Privacy in the Legal Battle Against P2P Technologies

Antinomie entre la protection des auteurs et le droit a la vie privée dans la bataille juridique contre les technologies P2P

Edgar Iván León Robayo[2]
Eduardo Secondo Varela Pezzano[3]

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 Abogado del Colegio Mayor de Nuestra Señora del Rosario (Bogotá D.C. - Colombia), profesor de Derecho Civil y Comercial y coordinador de la Línea de Investigación en Derecho Comercial. Igualmente, 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. Fue representante por Colombia ante la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (Cnudmi) y miembro de la comisión redactora de la Ley 527 de 1999 por la cual se reglamentó en Colombia el acceso y uso de los mensajes de datos, el comercio electrónico, las firmas digitales y las entidades de certificación. Correo electrónico: edgar.leon24@urosario.edu.co

3 Abogado y especialista en Propiedad Intelectual del Colegio Mayor de Nuestra Señora del Rosario (Bogotá D.C. - Colombia). Profesor de la misma materia, en pregrado. Es autor de: Tecnologías peer-to-peer, derechos de autor y copyright. Ganador en dos ocasiones del concurso: "Germán Cavelier del Derecho", con los ensayos: Toysareus.com: mucho más que un nombre de dominio y Patentes sobre variedades vegetales: una forma alterna de protección. Miembro de número del Centro Colombiano de Derecho de Autor (Cecolda) y de la Association Littéraire et Artistique Internationale (ALAI). Actualmente es abogado asociado de Reyes & Reyes Abogados. Correo electrónico: evarela@reyes-abogados.com

Este artículo fue recibido el día 3 de agosto de 2009 y aprobado por el Consejo Editorial en el Acta de Reunión Ordinaria No. 10 del 2 de diciembre de 2009.

Resumen

La posibilidad de utilizar todo tipo de programas para descargar información de manera gratuita —música, películas, libros electrónicos, juegos o *software*— le facilita a cualquier sujeto conectado a la Internet perpetrar infracciones al material protegido por derechos de autor o *copyright,* con lo que la industria del entretenimiento deja de percibir millones de dólares en ingresos. Como consecuencia, se han iniciado procesos judiciales en contra de usuarios en diferentes partes del mundo, los cuales han dado lugar a diferentes posiciones jurídicas que defienden o atacan la utilización de estas tecnologías, así como sanciones bastante importantes que pueden resultar, en algunos casos, desmedidas. Esta investigación tiene como propósito analizar la antinomia que existe entre la protección al derecho de autor o *copyright* y el amparo al derecho a la intimidad, desde la perspectiva de la protección del *habeas data,* por la utilización de programas *peer-to-peer* (P2P).

Palabras clave: derechos de autor, infracción de los derechos de autor, soporte lógico.

Abstract

The possibility of using all kinds of software to download content for free—music, movies, e-books, videogames or software— makes it easy for any person with an online connection to infringe copyrighted material. Due to this, the entertainment industry is loosing millions of dollars every year. Hence, more than a few lawsuits have been brought against peer-to-peer (P2P) users in different parts of the world, creating different legal opinions that either defend or condemn the use of P2P technology, generating, in some cases, important judicial sanctions that have resulted, in most of them, unreasonable. The purpose of this dissertation is to analyze the antinomy between protecting copyright and the preservation of the right to privacy, from the perspective of *habeas data* rights in relation to the use of P2P software.

Key words: Peer-to-peer, habeas data, privacy right, *copyright.*

Résumé:

La possibilité d'utiliser toutes les sortes de logiciels de t*éléchargement* gratuit soit de musique, films, livres électroniques, jeux vidéo ou logiciels, rend facile pour tous ceux qui ont un accès Internet la commission de violations concernant les matériaux protégés par le droit d'auteur. À cause de cela, l'industrie du divertissement perd des millions de dollars. En conséquence, dans différentes parties du monde ont commencé diverses actions en justice contre les utilisateurs de la technologie peer-to-peer (P2P), donnant comme résultat différentes positions juridiques qui acceptent ou rejettent l'utilisation de ces technologies, ainsi que, des sanctions légales importantes, dans certains cas, excessives. Le but de cet article est d'analyser l'antinomie entre la protection du droit d'auteur ou *copyright* et la préservation du droit à la vie privée, dans la perspective des droits de *l'habeas data* par rapport à l'utilisation des logiciels P2P.

Mots-clés: Droits d'auteur, violation des droits d'auteur, logiciels.

Sumario

Introducción. 1. El lenguaje P2P. 2. La privacidad y el problema de las descargas P2P. 3. La solución del derecho comunitario europeo. 4. Tratamiento del problema según el ordenamiento jurídico colombiano. 5. Conclusiones. Referencias.

Introducción

La primera persona que fuera enviada a prisión en el mundo por subir películas sin licencia a un servidor de internet, a través de la utilización de tecnologías *peer-to-peer* (P2P), fue el hongkonés Chan Nai-Ming, quien para tales efectos utilizó el seudónimo "Master of Cunning". El 8 de noviembre del 2005, un tribunal de justicia lo encontró culpable de distribuir copias no autorizadas de obras protegidas por derechos de *copyright* —Daredevil, Miss Congeniality y Red Planet— y lo condenó a una pena de prisión de tres meses[4].

Probablemente, Jammie Thomas hubiera preferido pasar la misma temporada en la cárcel. Sin embargo, su suerte fue otra. En octubre del 2008 fue condenada a pagar doscientos veinte mil dólares (USD 220.000) por una Corte de Minnesota (Estados Unidos), quien la encontró culpable de haber compartido ilegalmente más de mil setecientas (1700) canciones a través de la red[5]. En un segundo proceso iniciado ante otro juez del mismo Estado, y a pesar de la fuerte influencia de un masivo movimiento de seguidores que buscaban su declaratoria de inocencia[6],

4 HKSAR *v.* Chan Nai Ming (2005) 1469 HKCU1. Dado que se trataba de su primera condena, y de la primera vez que se reportaba un fallo similar en el mundo, el juez decidió reducir su pena de prisión a este corto término, el cual pudo ser de cuatro años, según las leyes de Hong Kong.

5 Esta fue la primera condena de tal cuantía por este concepto, de 26 000 demandas interpuestas por la industria del entretenimiento estadounidense. La mayor parte de ellas terminó en acuerdos privados por sumas cercanas a los 1.000 dólares, a título de indemnización. Al respecto, véase: Bangeman, E. (2007, 4 de octubre). RIAA trial verdict is in: jury finds Thomas liable for infringement. Extraído el 21 de mayo del 2009 desde: http://arstechnica.com/news.ars/post/20071004-verdict-is-in

6 Véase: www.freejamie.com

el jurado la condenó a pagar un millón novecientos veinte mil dólares (USD 1.920.000) por concepto de daños punitivos[7].

Como ellos, diariamente, millones de usuarios comparten, copian y distribuyen archivos de audio, imagen y video que, por lo menos en teoría, deberían estar protegidos por el derecho de autor o el *copyright*[8]. La facilidad en el uso de las tecnologías informáticas y la posibilidad de utilizar todo tipo de programas para descargar datos, de manera gratuita, permite que cualquier sujeto conectado a la red perpetre tales conductas, con lo que la industria del entretenimiento deja de percibir millones de dólares en ingresos.

Esas pérdidas hicieron que entidades como la Recording Industry Association of America (RIAA), la Motion Picture Association of America (MPAA) y la Canadian Recording Industry Association (CRIA) buscaran una solución a este problema. Para ello interpusieron acciones judiciales en contra de los usuarios de estos programas que, en ocasiones, resultaron excesivas. A pesar de sus buenas intenciones, tales procedimientos solo han dado lugar, hasta ahora, a sentimientos de rechazo por parte del público y a una mala prensa (Cohen, 2006).

Adicionalmente, en desarrollo de su actividad inquisidora, la industria del entretenimiento se ha encontrado con un importante obstáculo: los sistemas impiden que el usuario sea identificado directamente, pues cuando este accede al sistema únicamente se registra la dirección de *internet protocol* (IP)[9] de su sistema operativo.

---

7 En este caso, Thomas deberá pagar 80.000 dólares por concepto de daños ocasionados por cada una de las 24 canciones que compartió ilegalmente por internet, razón por la que fue encontrada culpable de *"willful copyright infringement"* —Recuperado de 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, consulta realizada el 9 de junio del 2009—. Sin embargo, para evitar el pago de esta suma, que corresponde a unos 4.000 millones de pesos colombianos, probablemente se declarará en "bancarrota". Al respecto, véase: http://news.cnet.com/8301-1023_3-10269251-93.html?tag=mncol;txt

8 Mientras el derecho de autor es la protección legal propia de estos asuntos según el derecho romano germánico, el *copyright* corresponde al derecho anglosajón.

9 "... cuando esos dígitos son asignados por el proveedor de red a un nombre de dominio, inmediatamente son transmutados a una herramienta de comercialización intelectual para quien ostente su titularidad. Esos nombres resultan ser, en últimas, los que dan lugar al empleo de denominaciones públicas o privadas de nombres comerciales o marcas (…) una dirección IP es un valor único de cuatro octetos que se expresa en notación decimal en forma de W.X.Y.Z (por ejemplo, 192.74.58.306). (...) cuando un usuario

Así, la dificultad de registrar quiénes comparten estas copias trae consigo la imposibilidad de sancionar infracciones al derecho de autor. Igualmente, los creadores de los programas P2P utilizan mecanismos como sobrenombres —*nicknames*— y contraseñas que impiden conocer, con estricta certeza, la identidad del usuario[10].

De esta manera, la revelación de los infractores sólo ocurre cuando los proveedores del servicio de internet descubren la identidad de la persona tras la dirección IP. No obstante, este tipo de situaciones implica una violación directa a los derechos de

---

de la red solicita conectarse desde un computador a un servidor específico, el proveedor de internet procede a consultar las bases de datos para resolver la solicitud del dominio en una dirección IP. Todo este sistema, en términos generales, se conoce como *domain name system* o DNS" —(Varela,2006). Véase, además:(Halabi & McPherson, 2001, pp. 52-55).

10 Esta fue, precisamente, la defensa planteada en el famoso caso The Pirate Bay. Proclamada a sí misma como *"the world's largest tracker"* —"el *tracker* más grande del mundo"—, esta página web gratuita fue fundada en el 2003 por la organización sueca *Piratbyrån* —oficina pirata—. El sitio les permite a los usuarios buscar y descargar archivos *torrent* organizados en las siguientes categorías: audio, video, aplicaciones —*software*—, juegos —videojuegos—, pornografía y otros. Para registrarse, el navegante 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 de la página, por "promocionar la infracción de terceros a las leyes del derecho de autor" —Corte de Distrito de Estocolmo. Caso n.º B 13301-06, abr. 17/2009—. Entre las distintas acusaciones se decía que The Pirate Bay era un negocio inmensamente rentable que hacía dinero ayudando a otros a violar los derechos de autor. Así mismo, se imputaba "el asistir a una 'puesta a disposición", violatoria de tales derechos. Por su parte, 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, 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, es decir, la Asociación Sueca del Derecho de Autor. Todavía se espera la decisión del *ad quem* respecto de este recurso.

habeas data y privacidad, debido al monitoreo y descubrimiento no sólo de la actividad *on line* sino también de la información personal y secreta de los usuarios.

Esta controversia se mantiene en la actualidad, constituyéndose en uno de los principales desafíos a la protección de los autores y titulares de derechos conexos. Este artículo tiene como propósito analizar la antinomia que existe entre este derecho y el amparo a la intimidad, debido a la utilización de las tecnologías P2P y las complejidades jurídicas que estas conllevan.

Para ello se realizará, en primer lugar, un estudio del origen y de las dificultades que han presentado las tres generaciones de P2P, desde el punto de vista tecnológico y legal. Posteriormente, el análisis se dirigirá a la órbita de la protección que ciertos países plantean desde el punto de vista constitucional y legal al denominado *habeas data*.

1. La arquitectura P2P

La tecnología P2P se puede definir como una red compuesta de nodos que hacen las veces de clientes y servidores de otros nodos. Cuando un cliente entra al sistema hace una conexión directa a uno de ellos, convirtiéndose en otro nodo de la red, lo cual le proporciona la capacidad de recolectar y almacenar la información y el contenido disponible para compartir.

Se trata, entonces, de un programa que tiene como función conectar a los usuarios a través de una red sin servidores, que facilita la descarga de música, películas, libros, fotos y *software* entre otros usuarios, de manera gratuita[11]. Estos archivos son compartidos "de computador a computador", por el sólo hecho de tener acceso al sistema. De suerte que, en las redes P2P, los autores no encuentran remuneración por su trabajo ni se les reconoce el derecho a explotar su obra.

11 La palabra "descargar" —*download*— se entiende como: "... recibir información, típicamente un archivo, desde otra computadora a través de un módem (...). El término opuesto es subir —*upload*—, que significa enviar un archivo a otra computadora" —United States *v.* Mohrbacher. 182 F.3d 1041, 1048 (9.th Cir. 1999)—.

Esta tecnología tuvo su aparición en 1999, cuando el estadounidense Shawn Fanning creó un *software* que permitía compartir música. El programa, que denominó Napster, conectaba a los usuarios a través de una arquitectura centralizada, permitiendo la descarga de archivos gratis desde un servidor único, en formato ".mp3"[12]. Un año y medio después, la abismal cifra de 80 millones de usuarios registrados y la descarga de 10 000 canciones por segundo aterrorizaron a la industria del entretenimiento (Leander, 2000).

Fanning figuraba en todo tipo de revistas, entrevistas y publicidad, promocionando su *software*. Sin embargo, en febrero del 2001, fue llevado a juicio. En A&M Records Inc. *v*. Napster Inc., los demandantes alegaron no solo que era responsable de contribuir directamente a la infracción del *copyright —contributory infringement*—, sino, además, indirectamente, por el hecho de sus usuarios —*vicarious liability*—[13]. Así, en Estados Unidos se condenó a Napster por mantener disponible el *software* y su dominio para que la violación tuviera lugar y porque se demostró que utilizaba los títulos de las canciones más descargadas para promocionar su página de internet. Así, Fanning prefirió declarar a su compañía en bancarrota antes de ver cómo era derrotado en juicio.

Pocos meses antes, el 14 de marzo del 2000, la empresa Nullsoft había divulgado el código fuente de Napster en el dominio slashdot.org, aunque el documento estuvo expuesto al público por unas cuantas horas, este tiempo fue suficiente para que toda la información necesaria para desarrollar programas similares fuese revelada. En sí mismo, este programa era un *software* deficiente (Stoica, Morris, Karger, Kaashoek & Balakrishnan, 2001). Su principal problema consistía en que los archivos que se encontraban a disposición de los usuarios solo podían descargarse de un servidor central y heterogéneo (Dabek et al., 2001). Así, por medio de uno o más servidores centrales a los que accedían los usuarios para descargar los archivos que hacían parte del índice interno del servidor, se construyó la primera generación de arquitectura P2P.

12 Abreviatura con la que se identifica MPEG-1/2 Layer-3, formato digital de compresión de archivos de audio optimizado para alta calidad en bajos porcentajes de bits —por ejemplo, 128 kbits/s—. Al respecto, véase: (Brandenburg, 1999).

13 A&M Records Inc. *v.* Napster Inc., 239 F.3d 1004 (9.th Cir. 2001).

Ante las dificultades que planteó esta tecnología, su desarrollo posterior permitió que los usuarios se conectaran a la red de manera distribuida. Fue en esta segunda etapa donde surgió el nombre *peer-to-peer* —usuario-a-usuario—, que fue aplicado también a la anterior. Sus creadores se dieron cuenta de que sin la figura de un servidor o administrador único resultaba imposible demandar la trasgresión de los derechos de autor. No obstante, esta arquitectura tenía un gran problema, consistente en el alto tráfico generado entre los usuarios, que hacía tedioso el manejo del sistema.

Apareció entonces una tercera variación, que se encuentra presente en programas como uTorrent, LimeWire y Azureus. En esta generación se despliega una red compuesta de supernodos —*supernodes* o *ultrapeers*— que hacen las veces de servidores centrales del índice al que se conectan los usuarios. Cuando un cliente entra a la red, hace una conexión directa a uno de los supernodos, donde recolecta y almacena tanto la información como el contenido disponible para compartir. Se trata de la reunión de todas las computadoras y del ancho de banda de quienes están conectados a una red determinada, con lo cual se elimina la distinción entre servidores y clientes.

En la actualidad, la tecnología de redes P2P resulta ser la herramienta más utilizada para compartir copias de obras protegidas por derecho de autor y *copyright*, especialmente música y video. Así, se configura una constante infracción masiva de estos derechos, por cuanto los programas que permiten realizar estas operaciones se encuentran disponibles, fácil y gratuitamente, para todos aquellos que tengan acceso a internet.

Para precisar las razones por las que estos sistemas han sido objeto de persecución por parte de las autoridades judiciales, un estudio realizado en el 2002 en Estados Unidos reveló que el 10,1% de adolescentes entre los 12 y 17 años prefería descargar música de internet a comprarla en las discotiendas[14]. Igualmente, se encontró que el 53% de jóvenes en ese mismo rango de edad había copiado la música de sus amigos en vez de comprar sus copias personales.

14 Sobre estas estadísticas, véase: Edisonresearch.com. *The national record buyers study II.* Recuperado de http://www.edisonresearch.com/home/archives/Recordbuyers2.pdf

En el 2003, se conoció que más de 60 millones de personas mayores de 12 años utilizaban programas P2P (Ipsos-Reid.com, 2002) para descargar música de manera gratuita en Estados Unidos. Un año después, en el mundo entero se registraron más de un billón de descargas semanales (Oberholzer & Strumpf, 2005). En España, por ejemplo, se compartieron 270 millones de archivos ilegales de música y de películas en internet. En el 2006 la cifra aumentó a 550 millones (ABC.es, 2006).

En Latinoamérica, Argentina es el país con mayor número de descargas ilegales. Durante el 2006 se transfirió una cifra cercana a los 608 millones y medio de canciones desde internet. Si se compara este número con el del 2005 —412 millones— el incremento es relativamente significativo. Adicionalmente, una encuesta realizada ese mismo año reveló que el 44% de los encuestados reconoció que bajar canciones gratis de internet infringe la legislación vigente (Infobae.com, 2006).

El panorama no es alentador, pues se calcula que para el 2010 la mitad de internautas en el planeta utilizará redes P2P. No obstante, aunque se considere que esto ha generado un manifiesto detrimento económico en los autores de las obras infringidas, se ha demostrado que, desde el surgimiento de estos programas, los ingresos recaudados por la industria del entretenimiento no han variado de manera significativa (O'Brien, 2005).

2. La privacidad y el problema de las descargas P2P

Si la industria del entretenimiento conociera la verdadera identidad de usuarios de programas P2P, registrados en internet como geekboy@KaZaa, chickiepoo25@KaZaa y mr_socks@KaZaa[15], no se producirían descargas ilegales de música, películas, videojuegos, libros y *software*. En efecto, ese rastro les permitiría a entidades como RIAA, MPAA y CRIA obtener los recursos necesarios para perseguir y demandar a los infractores.

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

En muchas ocasiones las acciones por descargas ilegales han sido dirigidas contra personas equivocadas, pues, a pesar del monitoreo que se realiza de las direcciones IP, aún es complejo determinar quiénes son los usuarios reales. En efecto, en varias de esas oportunidades las querellas han sido ejercidas en contra de menores de edad (Mook, 2003), amas de casa[16], personas fallecidas (Bangeman, 2005) o incluso contra sujetos que no tienen computadoras o que ni siquiera conocen su funcionamiento (Gaither, 2003).

Descubrir la identidad de los usuarios P2P resulta ser una ardua tarea para las organizaciones que pretenden salir a la defensa de los derechos de autor y del *copyright*. La estructura actual de esta tecnología es la que, finalmente, obstaculiza que se indemnice integralmente a los afectados con las descargas. En efecto, los navegantes utilizan direcciones electrónicas como "mr_socks@KaZaa", las cuales son *nicknames* que ocultan la identidad del usuario infractor. A esta dirección, por ejemplo, le correspondería un número IP otorgado por el proveedor del servicio de internet, que podría ser, hipotéticamente, uno similar a 175.45.98.303.

Entonces, para identificar a ese usuario y determinar si descarga copias ilegales en las redes P2P primero se debería localizar el número IP y, posteriormente, desenmascarar a la persona que se oculta detrás del sobrenombre, de manera que se pueda iniciar finalmente la actuación judicial, con los costos y los esfuerzos tecnológicos que esto conlleva. Sin embargo, el problema resulta mayor en aquellos Estados donde se consagra el derecho constitucional al *habeas data*[17] y a la privacidad personal, por cuanto sus sistemas legales no permiten sancionar a los usuarios P2P. En efecto, para identificar quiénes comparten obras ilegales es necesario que

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

17 Colombia reguló esta figura 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".* Esta normativa consagra el principio de confidencialidad, según el 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...". Esto conlleva 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. Esta normativa fue declarada exequible por la Corte Constitucional de Colombia —Sentencia C-1011, oct. 16/2008. M.P. Jaime Córdoba Triviño—.

los proveedores de internet desenmascaren[18] las direcciones IP para monitorear las actividades personales e íntimas de estas personas. Esto resulta inadmisible en países como Argentina, Canadá, Colombia, España, Francia, Paraguay y Perú.

Para ejemplificar esta situación, puede tenerse en cuenta lo ocurrido en Canadá. En un primer momento, el ordenamiento jurídico de ese país estimuló el uso de redes P2P. Todo empezó, curiosamente, cuando la Copyright Board of Canada interpretó en el 2003 la *Copyright Act* de 1921[19] para establecer que la copia de obras protegidas para usos personales no constituía una infracción[20]. Con base en esta decisión, la descarga de música se volvió legal en ese país, pero subirla a las redes P2P no (Borland, 2003).

18 En julio del 2008, un Juez del Distrito de Nueva York, Estados Unidos, ordenó a la compañía Google, Inc. revelar a la empresa Viacom Inc. cada registro de cada vídeo visto por sus usuarios en el sitio web YouTube.com, incluyendo los nombres de los usuarios y sus direcciones IP. Esta decisión, sin precedente alguno en Estados Unidos, obedeció a una acción civil que interpusiera Viacom contra el famoso sitio de videos digitales 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 v.* 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: Varela E. (2007). Videos que se están viendo ahora: Viacom v. YouTube revisado. *Opinión Independiente, 1,* 3—. 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. *v.* Reimerdes, 111 F.Supp.2d 294 (S.D.N.Y. 2000); Chamberlain *v.* Skylink, 381 F.3d 1178 (Fed. Cir. 2004); y Lexmark Int'l, Inc. *v.* 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.

19 R.S., 1985, c. C-42.

20 En consecuencia, de esta interpretación se deduce que las personas que copien canciones, películas y demás archivos, para uso personal, a través de redes P2P, no serán encontradas responsables de infringir la propiedad de las ideas. Véase: (Office de la Propriété Intellectuelle du Canada, 2005).

A pesar de esta contradicción, CRIA promovió una demanda ante una corte federal canadiense para que varios proveedores de internet revelaran la identidad de 29 personas que utilizaban este tipo de programas. No obstante, en BMG Canadá Inc. *v*. John Doe[21] se decidió que la demandante no podía obtener del juez la revelación de los usuarios, al carecer de evidencia para sustentar su petición. Así, el caso se convirtió en una victoria definitiva para la intimidad de los usuarios de redes P2P y en un salvavidas para conservar el anonimato *on line*.

En Socan *v.* CAIP[22], la Corte Suprema de Canadá señaló que la navegación de una persona en internet y sus actividades de descarga tienden a revelar información personal sobre ella misma. Así, indicó: "Los intereses íntimos de los individuos estarán directamente implicados donde los propietarios de obras protegidas o sus sociedades colectivas intenten recuperar 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].

En Francia, el 14 de diciembre del 2006, el Tribunal Correctionnel de la comuna de Bobigny profirió una sentencia que sembró aún más dudas respecto de los procedimientos empleados por las sociedades de autores y productores para constatar las infracciones de los adeptos al P2P (Dumont, 2006). La controversial decisión absolvió a un usuario que compartía más de 12 000 archivos ilegales en red, pues, en concepto de la corporación, el proceso para descubrir al sindicado y obtener pruebas de las descargas se hizo sin autorización de la Commission Nationale de l'Informatique et des Libertés (CNIL)[24], entidad administrativa encargada de proteger la libertad y privacidad informática[25].

La absolución se otorgó por cuanto, si bien la dirección IP fue identificada y registrada, violó la intimidad personal del usuario. Según el tribunal, esto no era

21 BMG Canada Inc. *v.* John Doe, cit., supra.

22 Society of Composers, Authors and Music Publishers of Canada *v.* Canadian Association of Internet Providers, 2004 SCC 45.

23 *Ibídem.*

24 "Comisión Nacional de la Información y las Libertades".

25 El Tribunal de París absolvió a un usuario de redes P2P bajo la presunción de que este no tenía la intención de transgredir estos derechos, pues el software que utilizaba compartía archivos de manera automática sin su consentimiento —véase: Tribunal de Grande Instance du Paris, 8 de diciembre del 2005—.

otra cosa que una evidente violación al derecho de información y de privacidad del acusado. En consecuencia, para el sistema legal francés también resulta inadmisible monitorear el uso del P2P y, por lo tanto, improbable que se sancione a quienes cometan esa conducta[26].

En Latinoamérica, y aunque no se ha legislado directamente este aspecto, existiría un problema similar para sancionar las descargas ilegales. Por ejemplo, el artículo 4.º de la Ley 1682 del 2000 de Paraguay[27], 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, país miembro del Mercado Común del Sur (Mercosur), con la Ley 25326 *sobre Protección de Datos Personales*[28]. Esta preceptiva 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..." (art. 1.º). En ese mismo orden, tampoco podría divulgarse ninguna información acerca de quiénes descargan archivos ilegales en ese país.

Incluso, la Corte Suprema argentina fue más allá del concepto, al sostener hace más de 15 años: "… el derecho a la intimidad protege un ámbito que está constituido por sentimientos, hábitos, costumbres, relaciones familiares, situación económica, creencias religiosas, salud mental, física, y en suma, acciones, hechos

26 Por otro lado, la jurisprudencia francesa siempre ha sostenido la tesis de que copiar obras protegidas por derechos de autor, para usos personales, es una excepción a la regla general de prohibición. Sobre este punto, véanse: Tribunal de Grande Instance, Rodez, 13 de octubre del 2004; Coupe d'Appels, Montpellier, 10 de marzo del 2005; Tribunal de Grande Instance, Meaux, 21 de abril del 2005; Tribunal de Grande Instance, Havre, 20 de septiembre del 2005; Tribunal de Grande Instance, Toulon, 13 de octubre del 2005; y Tribunal de Grande Instance, Crétil, 2 de noviembre del 2005.

27 Expedida el 28 de diciembre del 2000, en Paraguay.

28 Sancionada el 4 de octubre y promulgada parcialmente el 30 de octubre del 2000.

o datos, que teniendo en cuenta las formas de vida aceptadas por la comunidad, están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial para la intimidad"[29].

A pesar de lo anterior, en noviembre del 2005, la Cámara Argentina de Productores de Fonogramas y Videogramas (Capif) demandó a 20 usuarios de ese país por descargar música a través de tecnologías P2P (Clarín.com, 2005). Los accionados tenían algo en común: eran considerados como "grandes *uploaders*", pues cada uno compartía más de 5000 archivos ilegales. En octubre del 2006, y como parte de una ofensiva internacional contra los usuarios P2P[30], la entidad volvió a demandar a 22 *uploaders* adeptos a esta tecnología (Clarín.com, 2006). A la fecha de redacción de este escrito, tales casos todavía no se habían resuelto.

Perú, Estado miembro de la Comunidad Andina[31] (CAN), se ubica en el mismo contexto que Argentina y Paraguay. El texto constitucional de ese país establece en el numeral 6.º del artículo 2.º que toda persona tiene derecho "… a que los servicios informáticos, computarizados o no, públicos o privados, no suministren

29 Corte Suprema de Justicia de Argentina. Sentencia del 15 de abril de 1993. E. D. 152-569.

30 Violando los derechos a la intimidad y a la privacidad, la International Federation for the Phonograph Industry (IFPI) demandó en el 2006 a más de 8 000 usuarios de redes P2P que se encontraban localizados en 17 países: Argentina, Austria, Brasil, Dinamarca, Finlandia, Francia, Alemania, Hong Kong, Islandia, Irlanda, Italia, México, Holanda, Polonia, Portugal, Singapur y Suiza. Esta fue la primera vez que se reportaron demandas de esta índole en México, Brasil y Polonia. Sin embargo, el caso más alarmante fue el de Brasil, donde se registraron más de un billón de descargas ilegales en el 2006. Según la IFPI, las personas implicadas eran usuarios de programas y otras redes como BitTorrent, eDonkey, DirectConnect, Gnutella, LimeWire, SoulSeek y WinMX. Igualmente, la IFPI había trabajado previamente y en conjunto con la RIAA en Estados Unidos, ganando 13 000 demandas en Europa, para un recaudo total de 2420 euros de lo que originalmente se había perdido con las descargas ilegales.

31 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. 4.º). Si se tiene en cuenta que el P2P es uno de estos medios, puede concluirse que la Comunidad Andina goza de una protección adicional y especial para los derechos de autor en este ámbito, a la que se le aplicarán todas las disposiciones regionales en la materia.

informaciones que afectan la intimidad personal y familiar". Según esta norma, los proveedores de internet peruanos no podrían divulgar información de los usuarios que emplean las redes P2P para distribuir y compartir archivos ilegales. En tal sentido, tampoco se podría sancionar la conducta de descargar música ilegal a través de estos sistemas por atentar contra el derecho constitucional al *habeas data*.

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 se propague información que pueda ser lesiva al derecho constitucional a la intimidad"[32].

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" (Eguiguren, 1999, p. 64). Es decir, procede para evitar que se suministre información que afecte la vida privada de las personas, como sería aquella que se divulgue si se descarga cualquier contenido ilegal por medio de redes P2P. En consecuencia, los usuarios de esta tecnología no podrían ser identificados si se intentara una sanción contra ellos en Perú.

3. La solución del derecho comunitario europeo

El Tribunal de Justicia de las Comunidades Europeas (TJCE) abordó recientemente este asunto. En su decisión, acogió la postura de los proveedores de internet, abogando por la privacidad de los usuarios y dejando de lado las pretensiones de la industria del entretenimiento[33].

Los hechos que dieron lugar a la controversia tuvieron que ver con un procedimiento judicial de diligencias preliminares interpuesto por Productores de

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

33 TJCE, Asunto C-275/06, 29 de enero del 2008. Recuperado de http://www.iustel.com/v2/diario_del_derecho/noticia.asp?ref_iustel=1027055

Música de España (Promusicae) en noviembre del 2005 contra Telefónica —en su operación de proveedor de servicios de internet—. En su querella, la demandante solicitó conocer los nombres y direcciones de algunos usuarios masivos de redes P2P, susceptibles de identificación por sus números de IP y la fecha y hora de conexión, quienes se encontraban afiliados a la demandada.

Fue así como el Juzgado Mercantil n.º 5 de Madrid (España) ordenó entregar la información. Sin embargo, Telefónica se opuso a entregarla, alegando que el procedimiento no era penal sino civil. Cabe aclarar que en ese país la infracción de derechos de autor solo constituye un delito cuando se actúa "con ánimo de lucro", entendido éste como la "… búsqueda de un beneficio comercial" (Artículo 270 del Código Penal español).

Dado que la oposición de Telefónica se basaba en una normativa española que tenía como origen disposiciones de la Unión Europea, el juzgado decidió plantear una cuestión prejudicial ante el TJCE en la que preguntó si debían interpretarse las normas europeas en el sentido de obligar a los Estados miembros a imponer a los proveedores de servicios y, en particular, de acceso, el deber de proporcionar los datos de conexión y tráfico también en procedimientos civiles[34]. Según el ente comunitario, las directivas invocadas por el Juzgado pretenden asegurar una protección eficaz de la propiedad intelectual[35]. No obstante, lo hacen sin perjuicio de las normas sobre protección de la confidencialidad y tratamiento de datos personales. Por ello, afirma la corporación, los Estados no están obligados a extender el deber de informar a los procesos de naturaleza no penal. Tampoco lo hace la *Carta de Derechos Fundamentales*, que protege la propiedad y la tutela judicial efectiva, pero también los datos personales y la intimidad.

34 TJCE. Caso C-275/2008 (Promusicae *v.* Telefónica). Recuperado de http://www.iustel.com/v2/diario_del_derecho/noticia.asp?ref_iustel=1027055

35 *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); Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información y Directiva 2004/48/CE del Parlamento Europeo y del Consejo, relativa al Respeto a los Derechos de Propiedad Intelectual.* Recuperado de http://eur-lex.europa.eu

No obstante, el TJCE incluyó en su decisión una normativa no invocada previamente: la *Directiva 2002/58, sobre Tratamiento de Datos Personales y Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas*. Así, determinó que de acuerdo con el derecho comunitario resulta perfectamente posible que las leyes nacionales impongan a los proveedores de acceso y de otros servicios el deber de facilitar los datos de conexión y tráfico en el marco de procedimientos civiles.

La interpretación comunitaria resulta de la mayor importancia. En efecto, el mensaje se desprende de su fallo es el siguiente: "Aunque los Estados no están obligados a imponer un deber de información en los procedimientos civiles, sería aconsejable que lo hicieran; y, entre tanto, sería bueno que los jueces, aun no estando obligados por el derecho comunitario, interpretaran la ley en tal sentido" (Casas, 2008).

Con base en las consideraciones del alto tribunal europeo, y para decidir el caso sub judice, el Juzgado Mercantil n.º 5 de Madrid indicó que de conformidad con la ley española es preciso conservar la información, por si es necesario facilitarla "en el marco de una investigación criminal o para la salvaguardia de la defensa nacional o de la seguridad pública", lo cual no ocurre en este asunto. Además, agregó que los datos personales "no pueden ser cedidos sin consentimiento del interesado" a una entidad privada, como lo es Promusicae. Por estas razones aceptó la oposición de Telefónica[36].

4. Tratamiento del problema según el ordenamiento jurídico colombiano

El legislador colombiano olvidó reglamentar el uso de las copias privadas en las leyes 23 de 1982 y 44 de 1993. La creación de aparatos, artefactos y sistemas que permiten reproducir obras protegidas, tales como fotocopiadoras, grabadoras, quemadores de discos compactos o DVD no está expresamente prohibida por el ordenamiento. Mucho menos, las redes P2P.

36 Véase: http://www.adslnet.es/index.php/2008/06/22/el-p2p-seguira-siendo-anonimo-segun-sentencia-judicial-a-favor-de-telefonica/

Así, únicamente podría prohibirse el uso de esta tecnología si se interpretara en este sentido el artículo 271 del Código Penal[37]. Según esta disposición, incurrirá en prisión de cuatro a ocho años y multa de 26.66 a 1000 salarios mínimos vigentes quien, sin autorización previa y expresa del titular de los derechos: "… por cualquier medio o procedimiento, reproduzca una obra de carácter literario, científico, artístico o cinematográfico, fonograma, videograma, soporte lógico o programa de ordenador, o (...) distribuya (...) a cualquier título dichas reproducciones".

Como ya fue expuesto, el uso de la red P2P implica la distribución a título gratuito de archivos ilegales en internet. De esta manera, la conducta estaría tipificada en la ley penal colombiana. Sin embargo, acontecería lo mismo que en Perú, Argentina y Paraguay. En estos ordenamientos, el *habeas data* alude al conjunto de derechos de toda persona respecto a la información que sobre ella se encuentra en registros o bases de datos públicos o privados[38].

La Corte Constitucional colombiana ha empleado esta expresión para desarrollar el contenido de los derechos reconocidos en el artículo 15[39] de la Constitución Política[40]. De esta manera, la corporación ha establecido que se trata de un derecho fundamental, traducido en la facultad que tiene la persona a la que se refieren los datos privados para autorizar su conservación, uso y circulación, de conformidad con

37 Artículo modificado por el artículo 2.º de la Ley 1032 del 2006, publicada en el Diario Oficial n.º 46.307 del 22 de junio del 2006.

38 Comisión Andina de Juristas. *El proceso de habeas data en la Región Andina. Análisis comparado.* Recuperado de http://www.cajpe.org.pe/guia/3.pdf

39 "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...".

40 Corte Constitucional de Colombia. Sentencias T-002, mayo 8/92. M.P. Alejandro Martínez Caballero; T-414, jun. 16/92. M.P. Ciro Angarita Barón; C-479, ago. 13/92. M.P. José Gregorio Hernández Galindo y Alejandro Martínez Caballero; T-022, ene. 29/93. M.P. Ciro Angarita Barón; C-114, mar. 25/93 M.P. Fabio Morón Díaz; T-389, sep. 15/93. M.P. Hernando Herrera Vergara; T-459, oct. 13/93. M.P. Hernando Herrera Vergara; T-460, oct. 13/93. M.P. Hernando Herrera Vergara; SU-528, nov. 11/93, M.P. José Gregorio Hernández Galindo; T-017, ene. 30/95. M.P. José Gregorio Hernández Galindo; SU-082, mar. 1.º/95. M.P. Jorge Arango Mejía; SU-089, mar. 1.º/95. M.P. Jorge Arango Mejía; T-097, mar. 3/95. M.P. José Gregorio Hernández Galindo; T-119, mar. 16/95. M.P. José Gregorio Hernández Galindo; T-552, nov. 1.º /97. M.P. Vladimiro Naranjo Mesa; C-662, jun. 8/2000. M.P. Fabio Morón Díaz; C-831, ago. 8/2001. M.P. Álvaro Tafur Galvis; C-1147, oct. 31/2001. M.P. Manuel José Cepeda Espinosa; T-729, sep. 5/2002. M.P. Eduardo Montealegre Lynett y C-356, mayo 6/2003. M.P. Jaime Araujo Rentería.

las regulaciones legales[41]. Igualmente, lo ha definido 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"[42].

Frente a este tema, el alto tribunal también ha considerado: "… en relación con el derecho a la información y la legitimidad de la conducta de las entidades que solicitan información de sus eventuales clientes, a las centrales de información que para el efecto se han creado, así como la facultad de reportar a quienes incumplan las obligaciones con ellos contraídas, tiene como base fundamental y punto de equilibrio, la autorización que el interesado les otorgue para disponer de esa información, pues al fin y al cabo, los datos que se van a suministrar conciernen a él, y por tanto, le asiste el derecho, no solo a autorizar su circulación, sino a rectificarlos o actualizarlos, cuando a ello hubiere lugar. Autorización esta que debe ser expresa y voluntaria por parte del interesado, para que sea realmente eficaz, pues de lo contrario no podría hablarse de que el titular de la información hizo uso efectivo de su derecho".

De esta manera, los proveedores del servicio de internet en Colombia no podrían revelar la identificación de los usuarios de redes P2P. Ello sería contrario al derecho que tienen los colombianos a autorizar, expresa y voluntariamente, la divulgación de su información íntima y personal[43].

En cuanto a la vida privada de las personas, la corporación sostuvo 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*

41 Corte Constitucional de Colombia. Sent. SU-082, mar. 1.º/95. M.P. Jorge Arango Mejía.

42 Corte Constitucional de Colombia. Sent. T-729, sep. 5/2002. M.P. Eduardo Montealegre Lynett.

43 Sobre qué informaciones, actividades, situaciones y fenómenos pertenecen a la vida privada, véase: (Novoa, 1979).

priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada"[44].

En ese orden de ideas, y aunque el uso del P2P esté prohibido en Colombia por tratarse de una conducta tipificada en los delitos contra los derechos de autor, es inadmisible e imposible monitorear y sancionar a sus usuarios, se reitera, por la concurrencia del derecho al *habeas data* en la Constitución Política. De conformidad con lo mencionado, y en cualquier caso, si se hiciera referencia a los delitos contra la propiedad intelectual, muchos colombianos serían grandes delincuentes[45].

5. Conclusiones

Todavía quedan cabos por atar en esta controversia. Mientras la industria del entretenimiento continúa enfilando sus baterías para dar la batalla en contra de lo que cree un delito atroz, la tecnología avanza día a día en la construcción de diferentes sistemas que permitan descargar archivos con mayor rapidez[46].

44 Corte Constitucional de Colombia. Sent. T-414, jun. 16/92. M.P. Ciro Angarita Barón.

45 Frente a este tema, la Sala Penal de la Corte Suprema de Justicia de Colombia profirió un fallo donde analizó la presunta violación de derechos patrimoniales de autor, por la utilización de tecnologías P2P. La decisión tomada por esa alta corporación de justicia, el 30 de abril del 2008, se convierte en un primer precedente jurisprudencial latinoamericano sobre la materia, el cual resulta coincidente con tesis asumidas por algunos tribunales de España, Francia e Italia. Esta jurisprudencia adquiere entonces una importancia absoluta en el contexto internacional. Para la Corte, no puede ser punible el intercambio de datos a través del uso de tecnologías P2P cuando la actuación del usuario no conlleva un ánimo de lucro ni la intención de lesionar un patrimonio ajeno —Corte Suprema de Justicia de Colombia, S. Penal, Rad. 29188, abr. 30/2008. M.P. José Leonidas Bustos Martínez—.

46 Actualmente, Verizon Communications trabaja en el desarrollo de una nueva infraestructura, que inició pruebas el 14 de marzo del 2009. *Proactive Network Provider Participation for P2P* (P4P) es el nombre que recibe esta nueva tecnología, que proporcionaría una mejora significativa en las descargas P2P y descongestionaría el tráfico de datos en la web. En ella, los usuarios se seleccionan de manera inteligente, a través de un protocolo que utiliza datos de topología de red para maximizar la eficacia de información enviada por los proveedores del servicio de internet a las conexiones P2P. Recientes análisis demostraron que P4P incrementa entre un 200 y un 600% la velocidad de archivos descargados entre usuarios P2P y ofrece un mecanismo para minimizar costos y reducir el ancho de banda utilizado por los usuarios. De acuerdo con Verizon, esta plataforma pretende optimizar la descarga de archivos y solamente sería aplicable en servicios comerciales legales —véase: http://arstechnica.com/old/content/2008/03/verizon-embraces-p4p-a-more-efficient-peer-to-peer-tech.ars

Es evidente que todos los días se realizan millones de descargas ilegales de información protegida por derecho de autor y *copyright* en todo el mundo, debido al fácil acceso que tienen los internautas a las tecnologías P2P. Al traducirse esta situación en pérdidas inconmensurables para los titulares de las obras y de derechos conexos, la industria del entretenimiento ha iniciado acciones en contra de los usuarios que, en ocasiones, fueron rechazadas por cuanto la manera como se realizó tal actividad condujo a excesos que llegaron a vulnerar derechos fundamentales.

Uno de los medios que con mayor frecuencia se ha empleado para cumplir con este propósito ha sido el descubrimiento de la identidad de los usuarios a través de sus direcciones IP, mediante órdenes impartidas por los jueces a los proveedores del servicio de internet. Sin embargo, esa conducta constituye una manifiesta violación directa a los derechos de *habeas data* y privacidad, pues se trata de información personal y secreta que se encuentra reconocida y protegida por normas de índole constitucional y por decisiones judiciales proferidas por tribunales comunitarios de justicia. No obstante, la imposibilidad tecnológica de determinar claramente contra quién se deben dirigir las acciones judiciales le atribuyen mayor interés a esta contienda, dadas las múltiples estrategias que podrá asumir la industria del entretenimiento para lograr su cometido.

En Colombia el *habeas data* ha sido reconocido 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. Aunque el uso de las tecnologías P2P está tipificado por la legislación nacional como un delito contra los derechos de autor, en ningún evento sería posible monitorear las direcciones IP en aquellos casos que se presenten ante las cortes de justicia.

Referencias

ABC (2006): *Las descargas ilegales de música aumentan un 10% este año en España.* Recuperado de http://www.alfa-redi.org/noticia.shtml?x=8026

Bangeman, E. (2005). *I sue dead people...* Recuperado de http://arstechnica.com/old/content/2005/02/4587.ars

Bangeman, E. (2007). *RIAA trial verdict is in: jury finds Thomas liable for infringement.* Recuperado de http://arstechnica.com/news.ars/post/20071004-verdict-is-in

Brandenburg, K.H. (1999). MP3 and ACC explained. *AES 17.th International Conference on High Quality Audio Coding.*

Borland, J. (2003). *Canada deems P2P downloading legal.* Recuperado de http://news.com.com/2100-1025_3-5121479.html

Casas Vallés, R. (2008). *En los tribunales: a la caza del pirata P2P – el necesario equilibrio entre el derecho de autor y el derecho a la protección de la intimidad.* Recuperado de http://www.wipo.int/wipo_magazine/es/2008/02/article_0004.html

Clarín.com (2005). *Demandan a 20 usuarios de Argentina por bajar música de internet.* Recuperado de http://clarin.com/diario/2005/11/15/um/m-01090270.htm

Clarín.com. (2006). *Inician 22 demandas a usuarios argentinos por intercambiar música en internet.* Recuperado de http://www.clarin.com/diario/2006/10/18/um/m-01292587.htm

Cohen, Julie E. (2006). Copyright, Commodification, and Culture: Locating the Public Domain. En L. Guibault & P.B. Hugenholtz, (eds.), *The future of the public domain* (121-166) Recuperado de http://ssrn.com/abstract=663652

Comisión Andina de Juristas. *El proceso de habeas data en la Región Andina. Análisis comparado.* Recuperado de http://www.cajpe.org.pe/guia/3.pdf

Dabek, F., Brunskill, E., Kaashoek, M. F., Karger, D., Morris, R., Stoica, I, & Balakrishnan, H. (2001) Building peer-to-peer systems with chord, a distributed lookup service. En *Proceedings of the Eighth IEEE Workshop on Hot Topics in Operating Systems (HotOS-VIII).*

Dumont, E. (2006). *Un adepte du peer-to-peer relaxé grâce à un vice de procedure. Recuperado de http://www.zdnet.fr/actualites/internet/0,39020774,39365738,00.htm*

Eguiguren, F. (1999). *Poder judicial, Tribunal Constitucional y habeas data en el constitucionalismo peruano* (1.ª ed.). México: Cuadernos Constitucionales México-Centroamérica.

Edisonresearch.com. (s.f). *The national record buyers study II.* Recuperado de http://www.edisonresearch.com/home/archives/Recordbuyers2.pdf

Gaither, C. (2003). Recording industry withdraws suit. *The Boston Globe,* 24 de septiembre.

Halabi, S. & McPherson, D. (2001). *Arquitecturas de enrutamiento en internet* (2.ª ed). Madrid: Cisco Press.

Infobae.com. (2006). Grave: avanza la piratería musical por internet. Recoperado de http:// www.alfa-redi.com/noticia.shtml?x=8062

Ipsos-Reid.com (2002). Americans Continue to Embrace Potential of Digital Music. *Tempo: Researching the Digital Landscape.* Recuperado de http://www.ipsosna.com/dsp_tempo.cfm

Leander, K. (2000). Intel says: think like Napster. *Wired News.* Recuperado de http//: www.wired.com/news/technology/0,1282,38413,00.html

Novoa Monreal, E. (1979). *Derecho a la vida privada y libertad de información* (1.ª ed.). Bogotá: Editorial Siglo XXI.

Oberholzer, F. & Strumpf, K. (2005). *The effect of file sharing on record sales. An empirical analysis.* Recuperado de www.unc.edu/~cigar/papers/FileSharing_June2005_final.pdf

O'Brien, T. (2005). King Kong *v.* The pirates of the multiplex*. The New York Times.* 28 de agosto.

Office de la Propriété Intellectuelle du Canada. (2005). A guide to copyrights. Recuperado de: http://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/eng/wr00037.html

Stoica, I., Morris, R., Karger, D., Kaashoek, M. F. & Balakrishnan, H. (2001). Chord: a scalable peer-to-peer lookup service for internet applications. *Proceedings of the ACM SIGCOMM 2001 Conference SIGCOMM-01.*

Varela, E. (2006). Toysareus.com: mucho más que un nombre de dominio. *Temas Jurídicos,* (18).

Varela, E. (2007). Videos que se están viendo ahora: Viacom *v.* YouTube. *Opinión Independiente,* (1), septiembre-octubre.