Sistemas de Transferencia de Música por Redes P2P*

Guillermo Carey Claro y Matías Rodríguez Burr
Carey y Cía.

Sumario: 1.- Introducción.- 2.- Los sistemas P2P.- 3.- El caso Napster.- 4.- Muerte de los sistemas de transferencia de música centralizados.- 5.- Legalidad de las redes de transferencia de música P2P semi-descentralizadas y puras.- 6.- La batalla de los titulares de derechos de autor en USA.- 7.- Posibilidad de que estas demandas lleguen a América Latina y Chile.- 8.- Responsabilidad de los ISP por sus usuarios en redes P2P.- 9.- Conclusiones.

1.- Introducción

La transferencia de música en *Internet* surgió mucho antes del fenómeno Napster; los jóvenes ya intercambiaban archivos musicales a través de e-mails, generalmente comprimidos, entre personas que conocían los e-mails de sus destinatarios.

Los Newsgroups y Bulletin Boards comenzaron a poner archivos musicales a disposición de sus usuarios; en 1996 ICQ, el más popular sistema de chat en *Internet* en ese momento, agregó a sus servicios un sistema de mensajes instantáneos que permitía transferir todo tipo de archivos entre sus usuarios.

La revolución de las redes P2P, fue permitir que terceros que no se conocían pudieran intercambiar archivos entre sí. Esto generó un fenómeno masivo de intercambio de música y, consecuencialmente, de infracciones a los derechos de autor, específicamente de reproducción y distribución.

---

* Texto preparado sobre la base de la ponencia presentada en las XI Jornadas de Trabajo y Consejo de Administración de la Asociación Interamericana de la Propiedad Intelectual (ASIPI), desarrollado en República Dominicana, entre los días 14 y 17 de noviembre de 2004.

2.- LOS SISTEMAS P2P

El sistema P2P es un sistema que existe desde los orígenes de *internet*. Antes, la conexión a *internet* sólo se hacía entre computadores que conocían su respectivo número de Internet Protocol (IP). Con el aumento del número de computadores que empezaron a conectarse a *internet* y la existencia de muy pocos computadores que pusieran a disposición contenidos (Web Servers), surgieron proveedores de servicios centralizados (ISP) que administraban las conexiones entre usuarios y Web-Servers.

Los ISPs asignan un número IP temporal a cada computador que se conecta a *internet*, el cual varía en cada conexión, por lo que no es posible para un usuario buscar por su cuenta a otro usuario. Esto permite que los ISP monopolicen las conexiones. De esta manera surge un *internet* con relaciones de cliente-servidor, estando los primeros en una segunda categoría en relación a los segundos.

La gran innovación de los sistemas P2P de transferencia de música (precisamente Napster) fue la de constituir un servidor central que mantuviere direcciones IP permanentes. De esta manera un usuario pide al servidor central la dirección de otro usuario, y una vez entregada, se establece la comunicación directa entre ambos mediante una conexión P2P, sin necesidad de la conexión del ISP.

De esta manera podemos definir los sistemas P2P como una *tecnología que permite que dos o más usuarios de internet colaboren simultáneamente en una red de iguales, sin necesidad de coordinación central.*

Las características del sistema son:

1. Red que funciona sin la necesidad de un servidor central.
2. Es una red de relaciones entre iguales. Termina con el concepto de *internet* de relaciones entre clientes y servidores. Ahora cada computador puede ser un cliente y un servidor a la vez.
3. Sirve eminentemente para la búsqueda y transferencia de archivos.
4. No requieren de un browser, ya que ocupa su propia interfase.

Existen tres tipos de redes P2P: las que han sido usadas por los tres principales *softwares* de intercambio de música: Morpheus, Kazaa y Napster. Más abajo veremos cómo el funcionamiento de cada una de estas redes conlleva distintas responsabilidades en la infracción de derechos de autor:

2.1.- Redes P2P puras o descentralizadas: Protocolo Gnutella, Morpheus

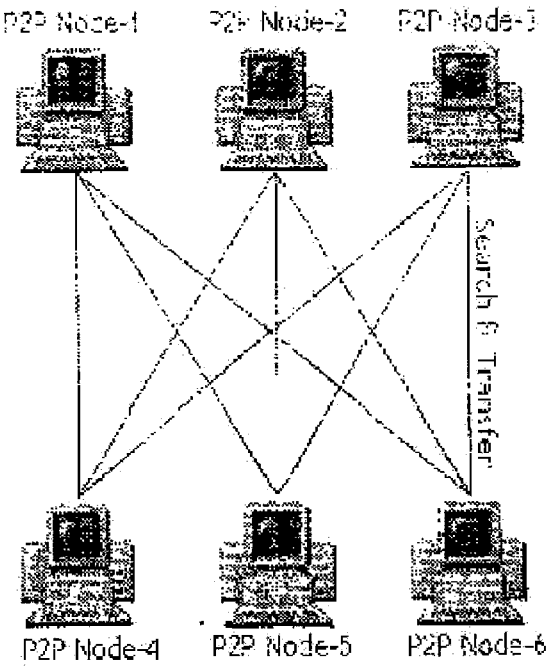
Se trata de una red absolutamente descentralizada, de tal manera que todos y cada uno de los computadores conectados o nodos, son servidores y clientes a la vez. Funciona de la siguiente manera:

Paso 1: Un nodo (X) solicita un archivo a otro nodo (Y) que se encuentra conectado a la red. De tener la información, establecen una conexión P2P para que X copie el archivo directamente del disco duro de Y.

Paso 2: En el caso de no tener el archivo, Y redirige la solicitud a otros nodos conectados que, de no tener la información, reenvían la solicitud a otros nodos.

El sistema de reenvío de solicitudes tiene un límite, el "Time to Live" (TTL), que consiste en la disminución progresiva del número de nodos a los cuales se reenvía la solicitud. De esta manera, Y reenvía la solicitud a un determinado número de nodos que, a su vez, la reenvían a un número menor de nodos y así sucesivamente hasta que la solicitud deja de reenviarse.

Paso 3: Una vez que la solicitud llega a un nodo que tiene el archivo solicitado (Z), éste responde al nodo que le haya enviado el mensaje para que éste, a su vez, se contacte con Y. Y se contacta con X y éste establece una conexión directa P2P con Z para copiar el archivo.



Fuente: "Regional Characteristics of P2P"
File sharing as a multi-aplicattion, multi-national phenomenon, Sandvine Incorporated, 2003.

Así funcionaba la red P2P que generaba el *software* Morpheus. Sus principales características son:

1) Permite la transferencia de todo tipo de información.
2) Funciona como un sistema de solicitud de archivos entre nodos (computadores) y no a un servidor centralizado.
3) Es un sistema absolutamente descentralizado. No existe ningún tipo de servidor central que monopolice la interconexión e intercambio de archivos entre los nodos conectados.
4) Es anónimo. No se requiere de un registro formal previo para participar en la red.[1]

El inconveniente de Morpheus es la gran cantidad de tiempo que se demora en buscar el archivo solicitado debido a que cada usuario es también un servidor, lo cual implica que se hacen muchas búsquedas de manera ineficiente.

2.2.- Redes P2P semi-descentralizados: Protocolo Fasttrack, Kazaa

Estas redes funcionan a través de un sistema de super-nodos y nodos. Los super-nodos son computadores conectados a la red, que tienen una mayor capacidad de conexión que los otros nodos conectados. La función de super-nodo es esporádica, pudiendo un computador funcionar en ocasiones como super-nodo y en otras ocasiones no, dependiendo de su capacidad de conexión en ese momento.

Existen dos tipos de super-nodos, los "root super-nodes" y los super-nodos activos. Los primeros permiten la conexión de los nodos a la red y los segundos son los que agrupan a un grupo de nodos, se encargan de la búsqueda de las solicitudes y de la interconexión entre el nodo solicitante y el nodo que tiene el archivo solicitado.

Fasttrack funciona de la siguiente manera:

Paso 1: Un nodo (X) se conecta a la red P2P mediante un "root super-node" que lo conecta, a su vez, con un super-nodo activo (Y), quien recibe las solicitudes de X.

Paso 2: Y tiene una lista de todos los archivos que sus nodos dependientes ponen a disposición de la red (uploads). De no encontrar el archivo solicitado por X en esta lista, reenvía su solicitud a otros super-nodos activos para que busquen en su lista de uploads, hasta que encuentre un nodo con el archivo solicitado por X (Z).

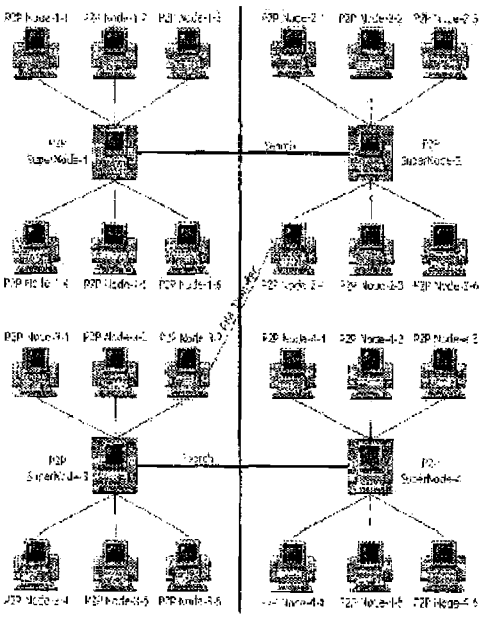
Paso 3: Se realiza una conexión directa P2P entre X y Z, para la copia del archivo.

Así funciona la red P2P generada por el *software* Kazaa. Sus características principales son:

[1] Morpheus pide una especie de registro, pero no es con clave.

1. Permite eminentemente la transferencia de archivos MP3 y MP4.[2]
2. Es un sistema descentralizado, en el sentido que no existe un único servidor central que controle las búsquedas e interconexiones.
3. Los usuarios son anónimos ya que Kazaa no requiere registros formales.[3]
4. Maximiza los recursos de todos y cada uno de los usuarios, aprovechando la mejor conectividad de los super-nodos. Esto permite búsquedas más rápidas que Morpheus.

Tiene sistemas de audio propio y búsquedas categorizadas por música, videos, intérprete, etc.



Fuente: "Regional Characteristics of P2P"
File sharing as a multi-aplicattion, multi-national phenomenon, Sandvine Incorporated, 2003.

2.3.- Sistemas P2P centralizados: Napster

Napster fue el primer *software* en revolucionar la transferencia de música gratuita por *internet*. El programa permite a los usuarios compartir sus archivos MP3 a través de un servidor centralizado, funcionando de la siguiente manera:

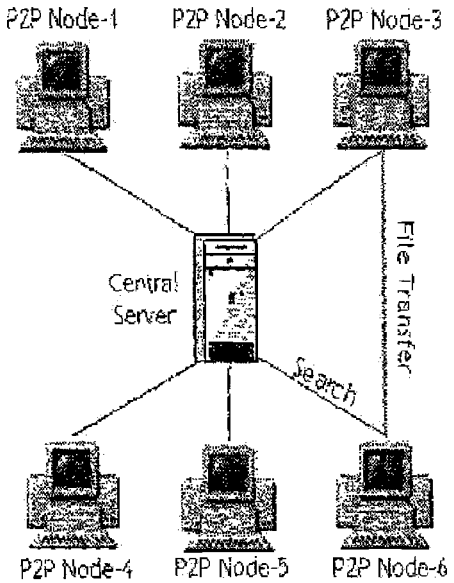
[2] MP3 es un formato digitalizado que permite guardar música de manera comprimida, de un CD a un disco duro. MP4 es también un formato digital, pero de vídeo.

[3] Kazaa pide una especie de registro, pero no es con clave.

Paso 1. Poner música a disposición de los usuarios. El usuario (X) descarga el *software* de "Music Share" debiendo registrarse en el sistema Napster creando un nombre de usuario ("user name") y una clave ("password").

Si X quiere poner a disposición de Napster sus archivos MP3 debe crear un directorio en su disco duro llamado "users library" y luego conectarse a Napster, usando su "user name". Napster revisa si efectivamente el archivo MP3 se encuentra almacenado en el disco duro de X y de estarlo, sube ("upload") el título del archivo y el nombre de X al directorio colectivo que Napster pone a disposición de todos los usuarios mientras X esté conectado.[4]

Paso 2. Descarga de archivos. Para que un usuario (Y) pueda descargar ("download") el archivo MP3 a través de Napster, debe haber descargado el *software* de "Music share" y registrarse de la misma manera que X. Una vez conectado al sistema puede buscar archivos MP3 a través del "search index" o del "hotlist".



Fuente: "Regional Characteristics of P2P"
File sharing as a multi-aplicattion, multi-national phenomenon, Sandvine Incorporated, 2003.

El search index permite a Y buscar en *todos* los archivos MP3 que se encuentren en el directorio colectivo de Napster y en el disco duro de usuarios conectados, mediante la búsqueda del

[4] El archivo MP3 se mantiene en el disco duro de X.

nombre de la canción o de su autor. Una vez colocada esta información, el servidor de Napster busca las coincidencias en su directorio colectivo y arroja una lista de resultados de los MP3 que se encuentren en los discos duros de los usuarios conectados (por ejemplo X). Estos resultados incluyen el título de la canción o su autor[5], el nombre de X, el tipo de conexión que tiene, el tamaño del MP3, la duración de la descarga y el método de comprensión.

Una vez encontrada la solicitud, si el usuario solicitante decide descargar el archivo, Napster establece la conexión temporal P2P entre éste y el usuario que tiene el archivo en su disco duro.

El sistema de descarga "hotlist", consiste en una lista que crea un usuario (Z) de Napster en la que incluye a otros usuarios de los que ha descargado archivos en el pasado. Cada vez que Z se conecte, Napster le avisará si algún usuario de su "hotlist" se encuentra también conectado, permitiendo a X solicitar a este usuario cualquier archivo que se encuentre en su "users library". A diferencia del sistema de "search index", los contenidos de los archivos de un usuario de "hotlist" no se almacenan en el servidor de Napster.

Todos los sistemas de transferencia de música a través de redes P2P señalados, son *gratuitos*. Esta es la principal razón de las demandas por infracción de derechos de autor de las que han sido objeto.

Las principales características del sistema de Napster se verán a continuación en el análisis de las demandas entabladas en su contra. Estas características son claves para determinar por qué Napster fue declarado potencialmente culpable de infracción secundaria de derechos de autor y Kazaa y Morpheus no.

3.- El caso Napster

Napster comienza a funcionar en junio de 1999, permitiendo la distribución en masa y gratuita de música que se encontraba amparada por derechos de autor. A poco andar Napster logró un enorme éxito. De acuerdo a cálculos señalados en la demanda de A&M Records v. Napster, aproximadamente 10.000 archivos MP3 eran compartidos por segundo y 100 usuarios trataban de conectarse a Napster con la misma frecuencia.

Napster no cobraba por los MP3 que se compartían a través de su sistema, pero generaba enormes rentas por publicidad, comisiones por links a otras páginas web, etc. A comienzos del 2001, Napster valía entre US$ 60 y 80 millones.[6]

En Diciembre de 1999 A&M Records junto a otras 17 disqueras más agrupadas en la RIAA presentaron una demanda civil contra Napster por infracción contributoria y vicaría de derechos de reproducción y distribución y por competencia desleal, ante la Corte de Distrito Norte

[5] El directorio colectivo de Napster sólo tiene el nombre de los archivos de acuerdo a cómo lo individualizaron los usuarios que hicieron el upload, y no el archivo mismo que se encuentra en el disco duro de estos usuarios. Esto no da garantías de efectivamente poder bajar el archivo que indica la nominación.

[6] Cálculos de la jueza Palet, a julio del 2000.

de California.[7] A través de esta acción se solicitaba un *"preliminary injunction"* para que Napster dejara de funcionar.[8]

En julio de 2000, la jueza Palet dictó el *"preliminary injunction"* en contra de Napster, ordenando que terminara con la facilitación y participación en la transferencia de archivos respecto de los cuales los demandantes tenían derechos de autor, salvo autorización de estos.

Esta decisión virtualmente termina con Napster, pero en febrero de 2001 la Corte de Apelaciones del Noveno Circuito, ordena a la jueza Palet modificar parcialmente la medida, de tal manera que la carga de terminar con Napster, recayera en ambas partes y no sólo en Napster. La medida revisada de marzo de 2001 establece que Napster debe sacar de su sistema todos los archivos que los demandantes le notifiquen.

Finalmente, en julio de 2001 la jueza Palet ordena terminar con Napster por no haber podido cumplir a cabalidad con la medida cautelar revisada.

Napster intentó transformarse en un sistema legítimo de transferencia de música por suscripción. Pero a esta altura la RIAA ya había lanzado varios *softwares* de transferencia legítima de música, por lo que ninguna disquera estaba interesada en invertir en Napster. La disquera Bertelsmann A.G., (BGM), que ya había aportado US$85 millones a Napster[9], estuvo a punto de comprarlo, pero la crisis interna de Napster terminó definitivamente con la empresa. Actualmente, Napster sigue funcionando legalmente bajo la propiedad de la empresa de *sofiware* Roxi.

BGM y Hummer Winblad, los principales inversionistas de Napster, han sido objeto de varias demandas por parte de otras disqueras (Universal Music Group, Capital Records y EMI, entre otros) para responder por tercería en la infracción de derechos de autor directa de los usuarios de Napster. Recién en julio del 2004, la misma jueza Palet denegó la petición de rechazo de la demanda presentada por Universal Records en contra de BGM y Hummer Winblad por US$ 14 billones. *Un fallo a favor de Universal puede tener gravísimas consecuencias en los mercados financieros, ya que la responsabilidad por infracciones a derechos de autor se extendería de manera excesiva.*

3.1.- Responsabilidad por infracciones a derechos de autor

Tanto la Jueza Palet como la Corte, consideraron que los demandantes demostraron posibilidad de éxito en la demanda por responsabilidad contributiva y vicaria por la infracción de derechos de autor (*copyright infrigment*), específicamente los derechos de reproducción y distribución.

Para configurar estas responsabilidades secundarias, es necesario probar primero la responsabilidad directa de los usuarios de Napster. Napster argumenta en ambas instancias que sus

7 Antes de esta demanda, el grupo Metallica ya había emprendido acciones similares, en abril del 2000.

8 Una *"preliminary injunction"* corresponde a una medida cautelar adoptada antes de dictarse sentencia, durante o inclusive antes de iniciar propiamente un procedimiento *(nota del editor)*.

9 Paradojalmente, BMG era también demandante en A&M Records v. Napster.

usuarios no cometen infracción directa en virtud de la eximente legal del "fair use".[10] En ambas instancias se desecha esta tesis por las siguientes razones:

1. El propósito de la transferencia de MP3 es comercial, ya que los usuarios evitan el gasto de comprar la música en el mercado formal.
2. Napster produce un efecto negativo en el mercado formal de música. En los juicios se afirma que se afecta tanto el negocio de venta de CDs, como el ingreso de las disqueras al mercado de música por *internet*.

Una vez establecido que los usuarios violaban directamente los derechos de reproducción, mediante el "download" de MP3, y de distribución, mediante el "upload" de estos archivos, se pueden configurar las responsabilidades secundarias de Napster.

3.1.1.- Responsabilidad contributiva

La responsabilidad contributiva se configura cuando se conoce o se debería conocer la conducta del infractor directo y se contribuye materialmente a la conducta de éste.

La Corte, asumiendo el criterio de Sony v. Universal[11], consideró que el caso de Napster era distinto, ya que el conocimiento de Napster no era solo debido (potencial) sino actual.[12] De esta manera, se cumple el requisito de conocimiento solo si se notifica a Napster de la infracción en el momento que estuviera ocurriendo y éste fallara en terminar con la conducta, pudiendo hacerlo.

La participación material de Napster se configura por el hecho de generar una red P2P centralizada. Sin el servidor centralizado, el usuario no podría saber qué usuario estaba conectado, si tenía el archivo buscado y realizar la conexión P2P para copiarlo. *En definitiva, Napster participa de manera directa supervisando, facilitando y permitiendo las descargas de MP3.*

3.1.2.- Responsabilidad vicaria

Finalmente, la responsabilidad vicaria se configura cuando se recibe un beneficio económico de la infracción directa y se tiene el derecho y capacidad para controlar los actos del infractor directo.

El beneficio económico se comprueba porque la disponibilidad de los MP3 atrae una mayor cantidad de usuarios, lo que trae como consecuencia directa ingresos por concepto de publicidad, pago por links, etc.

10 Sección 107, US Copyright Act.

11 Se estableció que no se cumple el requisito de deber conocer (no conocimiento actual) de usos ilegales de una cosa, cuando existen también varios usos potenciales legítimos para esa misma cosa.

12 Esto se prueba mediante un documento escrito por Sean Parker, co-fundador de Napster, reconociendo que el sistema consiste en la transferencia de música pirateada y varias notificaciones de la RIAA sobre la existencia de 12.000 infracciones a derechos de autor.

El control de Napster sobre el directorio colectivo y su capacidad de poder terminar con la suscripción de sus usuarios, impidiéndoles el acceso, fueron prueba suficiente de la capacidad de Napster para conocer y terminar con las infracciones a derechos de autor que ocurrían en el sistema.

En suma, los elementos que gatillaron el término de Napster fueron: centralizar su base de búsqueda y el hecho que el sistema solo servía para el intercambio de música.

4.- MUERTE DE LOS SISTEMAS DE TRANSFERENCIA DE MÚSICA CENTRALIZADOS

Con la caída de Napster, la RIAA inició una exitosa carrera de acciones legales contra todos los sistemas de transferencia de música conocidos.

En julio de 2002, Audiogalaxy fue demandado por la RIAA, bajo los mismos cargos que Napster. A finales del mismo año ambas partes llegaron a un acuerdo.

Audiogalaxy surgió como un espacio para que artistas y disqueras menores pusieran gratuitamente a disposición de los usuarios de *internet* sus MP3. Con el auge de los sistemas de transferencia de música, amplió su base de usuarios surgiendo el Satélite Audiogalaxy, que permitía tener acceso a librerías musicales más sofisticadas que las de Napster (clasificación musical por géneros, artistas, etc.).

En noviembre de 2002, se ordenó a Aimster poner fin a sus actividades, como resultado de una demandada entablada por la RIAA, en base a los mismos cargos mencionados.

Aimster surgió usando el sistema de mensajes instantáneos entre los usuarios de AOL. Luego pasó a funcionar como un sistema centralizado de intercambio de música, igual que Napster.

5.- LEGALIDAD DE LAS REDES DE TRANSFERENCIA DE MÚSICA P2P SEMI-DESCENTRALIZADAS Y PURAS

La oleada de demandas contra los *software* de intercambio de música terminarían con la resolución del caso Metro Goldwin Mayer Studios v. Streamcast Networks and Grokster.[13] La RIAA demanda a Streamcast Networks (antes Musicity) y Grokster por infracción contributiva y vicaria de derechos de autor, generada por la operación de los *softwares* Morpheus y Kazaa, propiedad de cada una de estas compañías respectivamente.

Morpheus opera con el protocolo Gnutella y Kazaa con el protocolo Fasttrack, explicados precedentemente, permitiendo la transferencia gratuita de archivos de música, video y otros entre sus usuarios.

Al bajar los *software* de Kazaa y Morpheus el usuario, sin necesidad de registrarse formalmente, puede poner a disposición de la red sus archivos, sin participación de un servidor centralizado que autorice estos uploads, como es el caso de Napster. Un mismo usuario puede estar haciendo downloads y uploads a la vez.

[13] Vid. Traducción del fallo en Jaramillo, Paula y Ruiz, Claudio. "Sistemas P2P. Comentario a Metro Goldwin Mayer Studios, Inc. et al. v. Grokster Ltd., et al.", en *Revista Chilena de Derecho Informático*, núm. 5, 2004, pp. 205 – 219 *(nota del editor)*.

Partiendo de la base que los usuarios de Kazaa y Morpheus son responsables de infracción directa a los derechos de autor, se analiza separadamente la responsabilidad secundaria de los dueños de estos *softwares*.

5.1.- Responsabilidad contributiva de los demandados

En relación a la posibilidad de que se verificara responsabilidad contributiva, debe observarse que: primero, el nivel de conocimiento no se cumple, porque a pesar de tener conocimiento actual de la infracciones a derechos de autor, no tienen la capacidad de terminar con la infracción; y, segundo, el principal argumento es que no se cumple el requisito de contribución *substancial*, dado que la búsqueda y conexión se realiza mediante peticiones entre usuarios, sin que estas solicitudes o archivos pasen por algún servidor central operado por los demandados.

En definitiva, si los sistemas de los demandados se cayeran, la búsqueda y transferencia de archivos sería todavía posible (a diferencia de Napster).

5.2.- Responsabilidad vicaria de los demandados

En cuanto a la configuración de responsabilidad vicaria, se observa que si bien se configura el beneficio económico, debido a que la transferencia ilegal de archivos aumenta el número de usuarios y esto, a su vez, genera grandes ingresos por concepto de publicidad,[14] ni Streamcast ni Grokster tienen capacidad de control sobre las infracciones a derechos de autor, porque su *software* permite acceder a redes P2P que están fuera de su control.[15]

En definitiva, este fallo exime de responsabilidad a los propietarios de redes descentralizadas o semi-descentralizadas P2P de transferencia de archivos, por las infracciones a derechos de autor cometidas por sus usuarios.

6.- LA BATALLA DE LOS TITULARES DE DERECHOS DE AUTOR EN USA

Luego de la decepcionante derrota contra las redes P2P descentralizadas y semi-descentralizadas, la RIAA ha iniciado en USA una serie de ofensivas contra el tráfico ilegal de música en *internet*.

Antes de iniciar proyectos de ley y ataques judiciales, la RIAA intentó disuadir del uso de los sistemas P2P mediante la inserción de virus en los archivos intercambiados, tales como: Hydra, que

[14] En la primera mitad de 2002 Streamcast percibió ingresos, por concepto de publicidad, estimados en US$ 2 millones y proyectaban US$ 5,7 millones para fines de ese mismo año.

[15] Los demandantes argumentaron que los demandados podían instalar sistemas para fiscalizar la transferencia ilegal de música. Este argumento fue desechado, debido a que la obligación de fiscalizar solo se genera cuando previamente existe la capacidad de control.

se inserta en el computador de los usuarios que compartían música, analizaba su disco duro y avisaba a la RIAA de la cantidad de archivos copiados; Freeze, el cual paraliza los computadores por varias horas, pudiendo llegar a producir la pérdida de información; y Silence, que analiza el disco duro y borra los archivos pirateados. No obstante, no se tienen registros de muchos ataques con estos virus.

6.1.- Iniciativas legales

El primer intento legislativo, fue un proyecto de ley que autorizaba a los titulares de derechos de autor, a "hackear" los computadores que estuvieran distribuyendo o copiando sus obras. "Hackear", consistía en impedir la transferencia del archivo o destruir el computador. El proyecto fue ampliamente rechazado principalmente por ser contrario a la leyes antihacking y a la libertad de comunicación anónima (*first amendment*). Fue sacado de consideración en mayo de 2003.

En junio del 2004, el Senado norteamericano inicio la discusión de dos proyectos de ley que buscan abordar la violación a los derechos de autor por *internet:* la *"Artist Rights and Theft Prevention Act"* y la *"Piracy Act"*.

La primera iniciativa contempla durísimas penas por compartir archivos de cualquier tipo que estén protegidos por derechos de autor. En caso de primera infracción la pena puede llegar hasta los *3 años de cárcel,* sin perjuicio de las indemnizaciones civiles que correspondan. En caso de reincidencia, las penas pueden llegar hasta los *10 años de cárcel,* sin perjuicio de las indemnizaciones civiles que correspondan.

La "Piracy Act" otorga mayor facilidad a los fiscales para perseguir delitos de piratería en *internet.* Ya no tienen que demostrar el conocimiento del infractor sino que basta el solo acaecimiento de la infracción, para poder entablar una demanda por violación a derechos de autor.

6.2.- Demandando a los clientes

Tanto en los fallos del caso Napster como en el de Streamcast y Grokster, quedó establecida la responsabilidad directa por infracción a derechos de autor de los usuarios de estos *softwares*; basándose en ello, la RIAA ha iniciado una oleada de demandas en contra de los usuarios. Esta estrategia ha estado plagada de críticas debido a los millonarios montos pecuniarios que persiguen, al desconocimiento público sobre el tema y principalmente porque la *RIAA está demandando a sus propios clientes.*

La seguidilla de demandas se mantienen hasta hoy y han desembocado en:

1) aproximadamente 1000 demandas por infracción a los derechos de autor en USA, contra aquellos usuarios que registran más transferencias de música (las sanciones por cada infracción van de los US$ 750 a los US$ 150.000 de acuerdo al Digital Millenium Copyright Act);
2) una disminución considerable en el uso de los *software* de intercambio de música[16];
3) el inicio de un proceso internacional de demandas por los mismos cargos; y,
4) una serie de acuerdos extrajudiciales que van desde los US$ 3.000 a los US$ 12.000.

[16] En Octubre de 2003, se registró en USA una baja de 3,8 millones de usuarios de Kazaa, en relación a junio del mismo año.

En abril del 2003, la RIAA demandó a 4 universitarios, que manejaban sistemas de búsqueda y transferencia de música en los campus de sus respectivas universidades. La demanda perseguía daños y multas por alrededor de US$ 100 millones. Afortunadamente para los estudiantes, todo terminó en un avenimiento por US$ 17.000.

Después de esta exitosa demanda, la RIAA comienza acciones contra los principales usuarios de los *software* tradicionales de intercambio de música (Kazaa, Morpheus, etc.). La RIAA conocía el número IP de sus computadores y el momento preciso en que se efectuaba la infracción. Lo único que faltaba era la individualización del usuario, que era información que podía obtener de los ISP.

La RIAA ocupó la sección 512 (h) de la Digital Millenium Copyright Act (DMCA), para exigir a los ISP que identificaran a sus usuarios que cometían infracciones a derechos de autor. En enero de 2003, en *RIAA v. Verizon Internet Services,* se estableció la facultad de los titulares de derechos de autor de exigir de los ISPs la identificación de los usuarios que infringieran sus derechos en redes P2P.

A partir de este fallo la RIAA comenzó a recabar información de los ISP sobre sus usuarios infractores. De esta forma, en septiembre de 2003 la RIAA entabla demandas contra 261 usuarios. La mayoría de los demandados suscribieron avenimientos con la RIAA por aproximadamente US$ 3.000.[17]

Ejemplos de los excesos incurridos por esta oleada de demandas, fue el caso de Brianna Lahara, niña de 12 años, demandada por infracción a derechos de autor. El avenimiento con la madre de esta niña fue por US$ 2.000. También fue enormemente controvertido el caso de una señora de 60 años de Boston que fue acusada de compartir música "hardcore rap" por Kazaa. Esta acusación fue probada falsa, llamando la atención sobre la veracidad de las demandas de la RIAA.

Debido a las críticas, la RIAA inició en octubre de 2003 un proceso de notificaciones previas a la presentación de demandas, ofreciendo avenimientos. De 204 usuarios notificados, 124 respondieron en el plazo de 10 días que entregaban las notificaciones. El resto de los 80 notificados fueron demandados.

En diciembre de 2003 la exitosa apelación de *Verizon Internet Services* a las solicitudes de identificación de la RIAA, hizo pensar que la oleada de demandas llegaría a su fin. Pero en definitiva esto no fue así.

[17] Junto con estas demandas, la RIAA ofrecía la posibilidad del "Clean Slate". Esta consistía en una campaña de amnistía dirigida a aquellos usuarios que no habían sido todavía demandados. Estos debían destruir todos los archivos pirateados que tenían en su disco duro, y firmar una declaración jurada en donde se comprometían a nunca más volver a compartir archivos protegidos por derechos de autor en *internet.*

6.2.1- ISP y la sección 512 de la DMCA

La sección 512 de la DMCA establece cuatro hipótesis de *safe harbours* (puerto seguro). Estas son funciones de los ISP que les permiten eximirse de responsabilidad pecuniaria por infracciones a derechos de autor efectuadas por sus usuarios.

En la transferencia de archivos mediante redes P2P, el ISP actúa como un mero conductor de información, por lo que encaja en el Safe Harbour de "Comunicación Digital Transitoria".[18] Esta función consiste en la mera transmisión, enrutamiento o suministro de conexiones para el material infractor, sin modificar su contenido. Los otros requisitos para que se configure este Safe Harbour son:

1. La única copia que hace el ISP del material infractor debe ser temporal y automática.
2. La transmisión debe ser iniciada por un sujeto distinto del ISP.
3. El ISP no puede intervenir en el destino del material infractor.
4. Las copias temporales sólo pueden estar a disposición del destinatario del material y solamente por un período de tiempo razonable.

Lo que alega Verizon en su apelación, es que no se le puede exigir entregar información sobre la identidad de los infractores, debido a que la notificación no cumple con uno de los requisitos esenciales que exige la DMCA, que es la identificación del material infractor para que el ISP lo pueda remover o deniegue el acceso a éste.[19] Este requisito no lo cumple la notificación debido a que un ISP funciona sólo como un conducto para los archivos transmitidos por redes P2P, de tal manera que no tiene capacidad para identificar el material infractor ni menos para bloquear su acceso.

La Corte de Apelaciones de Columbia, aceptó esta tesis, concluyendo que los ISP que cumplen sólo funciones de transmisión, como lo hacen cuando sus usuarios intercambian archivos a través de redes P2P, no son objeto de las notificaciones de la sección 512(h) de la DMCA y, por lo tanto, no están obligados a identificar a sus usuarios infractores. Según la Corte estas notificaciones sólo se aplican respecto de ISP que cumplen funciones de almacenaje de archivos (sin contar el almacenaje temporal), ya que estos permiten identificar el material y obstruir su acceso. Esto se da en los otros tres Safe Harbours.[20]

La Corte también argumenta que de la historia legislativa de la DMCA se desprende claramente que el legislador no previó la aparición de las redes P2P ni menos de las infracciones a los derechos de autor que ocurrían en ellas.

En definitiva, este fallo permite concluir tres cosas:

[18] Transitory Digital Network Communication

[19] Sección 512 (h)(2)(A) de la DMCA.

[20] Es requisito para que se configuren estos otros tres Safe Harbours que, ante la notificación de infracción de derechos de autor, el ISP remueva el material infractor o deniegue el acceso a éste.

1. Un ISP se encuentra eximido de responsabilidad por infracciones a derechos de autor cometidas por sus usuarios, en la transferencia de archivos a través de redes P2P. Se aplica el Safe Harbour de Comunicación Digital Transitoria.
2. Un ISP no tiene la obligación de remover el material infractor para que se le aplique el Safe Harbour de Comunicación Digital Transitoria. Y,
3. Un ISP no tiene la obligación de revelar la identidad de sus usuarios que infringen derechos de autor a través de las mencionadas redes, a la luz de la DMCA.

6.2.2- Demandas contra "John Does"

La decisión analizada arriba no impidió que la RIAA encontrara un nuevo camino legal para identificar a los usuarios infractores en redes P2P. Mediante la interposición de demandas contra sujetos indeterminados ("John Does") con la información que la RIAA disponía (vista arriba), ahora es el tribunal quien pasa a hacerse cargo de identificar a los infractores. Con esta estrategia la RIAA demandó a 532 John Does, en enero del 2004, en New York y Washington.

En julio del 2004 la Corte de Distrito del Sur de New York, denegó la petición de anular la orden de entrega de información hecha a Cablevision (ISP), en enero de 2004. Cablevision había obedecido la orden de entregar las identidades de los usuarios de la demanda de John Does de la RIAA.

Estos usuarios alegaron principalmente, que la entrega de su identidad violaba la privacidad de comunicación garantizada por la *first amendement*. La Corte consideró que siendo efectivamente la transmisión de música a través de *internet* una forma de comunicación anónima garantizada por la *first amendment*, esta se protege de manera *relativa* (a diferencia de otras formas de comunicación anónima como la política, cuya protección es absoluta). Es por lo anterior, que el derecho de protección de este tipo de comunicación cede ante el derecho de la RIAA de investigar judicialmente infracciones a los derechos de autor, siendo legítima la entrega de identidad de los potenciales infractores.

7.- POSIBILIDAD DE QUE ESTAS DEMANDAS LLEGUEN A AMÉRICA LATINA Y CHILE

Casi todas las legislaciones nacionales de América Latina contemplan la prohibición de distribuir y reproducir obras mediante *cualquier medio*, sin la autorización del titular de derechos de autor de la obra. El Tratado de la OMPI de 1996, establece el derecho exclusivo de los autores de obras literarias y artísticas para "autorizar cualquier comunicación al público de sus obras puesta por *medios alámbricos o inalámbricos*". De estas disposiciones se desprende que los derechos de autor en América Latina, también se protegen cuando las infracciones ocurren en *internet*.

Ahora existe una excepción a estos derechos exclusivos parecida al "fair use" norteamericano, consistente en la copia privada y sin ánimo de lucro de una obra. No obstante, la copia de música y vídeo para ponerla a disposición de miles de usuarios anónimos, no es considerada un uso privado sin ánimo de lucro, de acuerdo al criterio jurisprudencial establecido en Napster.

Con la proliferación de los Tratados de Libre Comercio (TLC), se están exigiendo estándares de protección a los derechos de autor similares entre las partes signatarias. Esto ocurre en el caso del acuerdo suscrito entre Chile y USA, cuyas disposiciones tienen el objetivo de homogenizar la protección legal chilena de la propiedad intelectual en *internet*, con la protección legal dada en USA.

Ejemplos de esta intención se hacen evidentes en varias disposiciones del capítulo 17 de este TLC. Así el artículo 17.5 (1) establece que: "cada Parte dispondrá que los autores de obras literarias y artísticas tengan el derecho de autorizar o prohibir toda reproducción de sus obras, de cualquier manera o forma, ya sea permanente o temporal *(incluido su almacenamiento temporal en forma electrónica)*".

Por su parte el artículo 17.5 (5) también hace evidente la intención de protección a los derechos de autor en *internet*: "Cada Parte otorgará a los artistas intérpretes o ejecutantes y a los productores de fonogramas el derecho de autorizar o prohibir la radiodifusión o cualquier comunicación al público de sus interpretaciones o ejecuciones fijadas o fonogramas, *ya sea por medios alámbricos o inalámbricos,* incluida la puesta a disposición del público de esas interpretaciones o ejecuciones y fonogramas".

Ahora, las mayores similitudes entre la legislación sobre propiedad intelectual de USA y el TLC, se producen en el artículo 17.11 número 23 (limitación de la responsabilidad de los ISP) con la sección 512 del DMCA, ya que:

1. Se ocupa la misma definición de ISP.
2. Se contemplan los mismos cuatro *Safe Harbours: Transitory Digital Networks Communications, System Catching, Information Residing on Systems or Networks at the Direction of Users y Information Location Tools*. También se establecen varios de los requisitos exigidos por la DMCA para que aquéllos se configuren, tales como que el ISP retire y bloquee el acceso en caso de notificación de infracciones; no reciba un beneficio económico de las infracciones; y, designe públicamente a un representante para recibir las mencionadas notificaciones.
3. Las medidas precautorias que se contemplan en los casos de Comunicación Digital Transitoria y de los otros tres Safe Harbours son iguales. En el primer Safe Harbour se contempla el término de la cuenta del usuario infractor, y en los otros tres se contempla esta medida junto a otras, como el retiro o denegación de acceso al material infractor.
4. Se establece casi el mismo procedimiento de notificaciones y contranotificaciones entre los titulares de derechos de autor y el ISP, así como entre éste y los supuestos infractores. Estas notificaciones tienen por objeto terminar con el acceso a los usuarios o el acceso a los materiales infractores.
5. Se establece la obligación de legislar un procedimiento de notificación a los ISP, para que entreguen la identidad de algún supuesto usuario infractor de derechos de autor.
6. Se establece la exención de cualquier responsabilidad por parte de un ISP que termina de buena fe con una cuenta, siempre que haya cumplido con la notificación al usuario afectado.

Todas estas normas no han entrado aún en vigencia, debido a que actualmente solo constituyen una obligación de legislar para el Estado de Chile. Sin embargo ya se están organizando los grupos de trabajo correspondientes para iniciar el trabajo legislativo.

De todo lo señalado se puede concluir que respecto a la persecución de los usuarios por infracción directa de derechos de autor en América Latina es perfectamente posible dirigirse en contra de los usuarios de redes P2P. Respecto a la responsabilidad de los ISP por estas infracciones se podría decir que una vez que se legisle en Chile sobre las disposiciones del capítulo 17 del TLC, no serán responsables en virtud del Safe Harbour de Comunicación Digital Transitoria,

Si los ISP chilenos se encuentran obligados a identificar a los usuarios infractores de acuerdo a las disposiciones del capítulo 17, es algo que se debe resolver a nivel legislativo y de jurisprudencia local.

8.- RESPONSABILIDAD DE LOS ISP POR SUS USUARIOS EN REDES P2P

Como ya se vio anteriormente, en USA un ISP no es responsable por infracciones a derechos de autor cometidas por sus usuarios en redes P2P, de acuerdo al Safe Harbour de Comunicación Digital Transitoria (sección 512, DMCA). Según la sección 512 (h), tampoco se le exige a un ISP vigilar la información que transmite o almacena por posibles delitos y le está prohibido retirar material cuando esto implique infringir otras leyes.

La situación de los ISP en la Unión Europea es casi la misma. El artículo 12 de la Directiva 2000/31/CE, de 8 de junio de 2000, establece una eximente de responsabilidad que consiste en la "mera transmisión de información". Esta eximente es casi idéntica al Safe Harbour de Comunicación Digital Transitoria, y contempla los mismos requisitos mencionados en el precedente punto 6.3. De esto se puede concluir que en Europa, al igual que en USA, un ISP no es responsable por las infracciones a derechos de autor cometidas por sus usuarios en la transferencia de archivos en redes P2P.

La Directiva de la Unión Europea, al igual que la DMCA, también establece la inexistencia de una obligación al ISP de vigilar la información que transmite o almacena en búsqueda de posibles delitos.

Se debe tener presente que en los países latinoamericanos donde no existe regulación especial sobre este tema, se podrían aplicar supletoriamente las reglas civiles de responsabilidad extracontractual. Así, por ejemplo, en Chile, la Corte de Apelaciones de Concepción, en *Orlando Fuentes con ENTEL S.A.*, se manifestó en este sentido; siendo este un caso de perturbación a la honra y no de infracción a los derechos de autor, la Corte afirma que un ISP no es responsable de la infracción, debido a que sólo es *conductor*, a menos que no elimine el contenido nocivo una vez solicitado por la autoridad o el ofendido.

Esta solución se asemeja al criterio de USA y de la Unión Europea, en cuanto los ISP no son responsables por *información que no tienen posibilidad de controlar.*

Ahora, los ISP se ven afectados por la transferencia de archivos en redes P2P debido a la cantidad de ancho de banda que ocupan. Esto, sumado a las infracciones de derechos de autor, han llevado a los ISP a generar costosos mecanismos para evitar la excesiva transferencia de archivos en *internet*. Por ejemplo Bell Canada le impone multas a sus usuarios por excesos en descargas. Otro mecanismo es disminuir la velocidad de procesamiento en caso de descargas excesivas. Los grandes inconvenientes de estos mecanismos son: primero, el excesivo costo tecnológico para los ISP; segundo, inhiben la transferencia legítima de archivos; y, tercero, generan cobros o sanciones injustas para los usuarios, como en el caso que las mayores descargas se produzcan por "spam".

9.- CONCLUSIONES

Actualmente, las disqueras y los autores no tienen forma jurídica de terminar con los *softwares* de transferencia de música que manejan redes P2P descentralizadas o semi-descentralizadas. Tampoco pueden responsabilizar por los daños ni exigir el término de esta actividad a los ISP.

Lo único que queda es dirigirse en contra de los usuarios de estos *softwares*. Pero ha quedado demostrado que la oleada de demandas de la RIAA, si bien han logrado disminuir la transferencia ilegal de música en USA, han dañado seriamente la imagen de las disqueras.

¿Qué alternativa les queda a los titulares de derechos de autor para proteger sus obras?

Una vez que Napster terminó sus funciones de transferencia gratuita de música, las disqueras comenzaron a desarrollar redes P2P de transferencia legítima de música, en las cuales se pagan royalties a los titulares de derechos de autor. Ejemplos de estas redes son los *softwares* MusicNet y MusicNow. Pero de estos *softwares*, el más exitoso es iTunes Music Store (iTunes), de Apple Computer.

iTunes fue lanzado en mayo de 2003 y su éxito sigue sorprendiendo. Tan solo en su primer mes de lanzamiento, las acciones de Apple Computer subieron en 27% y más de tres millones de canciones habían sido bajadas.

Estos *softwares* demuestran que los usuarios están dispuestos a pagar dinero, por mejor calidad de archivos musicales. Los autores y disqueras deberían explotar este nicho, que podría cambiar de manera definitiva la forma en que se compra música y video. Lección *si no puedes contra ellos únetele y, mejor aún, gánales.*