REVISTA CHILENA DE DERECHO Y TECNOLOGÍA
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO • UNIVERSIDAD DE CHILE
ISSN 0719-2576 • VOL. 1 NRO. 1 (2012) • PÁGS. 15-101 • DOI 10.5354/0719-2584.2012.24025

Lo imperfecto es enemigo de lo bueno: leyes antielusión versus innovación abierta

The Imperfect is the Enemy of the Good: Anticircumvention Versus open User Innovation

WENDY SELTZER
Berkman Center for Internet & Society, Harvard University

RESUMEN La gestión de derechos digitales (DRM, por sus siglas en inglés), el control tecnológico, respaldado legalmente, del uso de obras protegidas por derechos de autor, es claramente imperfecta: a menudo no logra detener la piratería y frecuentemente bloquea usos no infractores. Sin embargo, el impulso para corregir estas imperfecciones oculta un conflicto más profundo entre el sistema DRM antielusión y el desarrollo abierto en todo el entorno de los medios digitales. Este conflicto, que está en el corazón de los DRM, se profundizará incluso si otros aspectos de los DRM puedan ser mejorados. El presente artículo da una mirada sistémica al entorno legal, técnico y comercial de los DRM para destacar este conflicto y sus efectos.

PALABRAS CLAVE Derecho de autor, gestión de derechos digitales, antielusión, medidas tecnológicas de protección, innovación abierta, innovación de usuario.

ABSTRACT Digital Rights Management, law-backed technological control of usage of copyrighted works, is clearly imperfect: It often fails to stop piracy and frequently blocks non-infringing uses. Yet the drive to

correct these imperfections masks a deeper conflict, between the DRM system of anticircumvention and open development in the entire surrounding media environment. This conflict, at the heart of the DRM schema, will only deepen, even if other aspects of DRM can be improved. This paper takes a systemic look at the legal, technical, and business environment of DRM to highlight this openness conflict and its effects.

KEYWORDS Copyright, digital rights management, DRM, anticircumvention, technical protection measures, open innovation, user innovation.

1. INTRODUCCIÓN

Imagina que eres un magnate de la industria cinematográfica que desea utilizar la mejor tecnología para proteger tu nuevo estreno, *Piratas del Caribe. La precuela*. Puedes, por supuesto, limitar los cines en los cuales la película será exhibida, dejándola sólo disponible para salas de alta tecnología, con guardias de seguridad registrando a los asistentes para impedir el ingreso de personas con cámaras de video, y resguardando la película en su camino a la sala de proyección.[1] Antes de llegar a ese punto, tendrás que asegurarte de que todos quienes trabajaron en la película tengan los incentivos adecuados para impedir que ésta se filtre antes de su estreno.[2] Aun así, es probable que la película se filtre a las calles a través de alguna grieta en la armadura (sobre todo si es tan popular como tú esperas que sea). Con suerte, sin embargo, has comprado algo de tiempo y has generado suficiente expectativa como para que el público quiera ver la película en el cine, aun cuando las personas podrían adquirir copias defectuosas para verla en sus televisores. Podrías incluso aumentar la diferencia al exhibir la película en formatos IMAX y 3D, creando una experiencia difícil de replicar, aun cuando los bits sean copiados (Milian, 2009).

Una vez que termine la exhibición en cines, puedes continuar explo-

1. Véase, por ejemplo, Dawn (2008). Compare estas protecciones con la protección más limitada que Disney tuvo para *Blanca Nieves* (cf. Nimmer, 2003: 17-18).

2. Bryers y otros (2003) detectaron que los «ataques desde dentro» correspondían a más de tres cuartos de las filtraciones, muchos de éstos previos al estreno en formato DVD.

tando tu inversión a través de su alquiler y venta.[3] Podrías alquilar y vender copias digitales sin restricciones, confiando en las disposiciones de las leyes de derecho de autor que prohíben la reproducción a escala comercial, la distribución y la comunicación pública no autorizada de la película, pero tú deseas un respaldo tecnológico adicional. Entonces, para «mantener a la gente honesta», quieres incorporar sistemas de «protección anticopia», envolviendo la película en cifrado o en disposiciones contractuales, o en ambas.

El cifrado podría impedir que un usuario no deseado —aquél sin la clave correspondiente— pueda ejecutar los bits en la forma de una película, sin importar cuantas copias de ésta pueda hacer.[4] Una película encriptada se parece a una cadena aleatoria de unos y ceros cuando se lee desde el disco. Pero, salvo que le entregues al comprador la clave, lo dejas como un mero posavasos (que se puede comprar más barato en otras partes). Por lo que también deberás proveer al comprador de los medios de descifrado. Pero, si le entregas directamente la clave, el usuario poseerá toda la información necesaria para realizar copias.

Entonces, en lugar de entregar directamente la clave al usuario, deberás confiarla a un emisario de «caja negra»,[5] un programa computacional o unidad de *hardware* a la que tú restringes la ejecución de la película, en la forma que has determinado aceptable: ejecutar pero no copiar, por ejemplo. Sin embargo, ahora que has compartido el secreto con un programa computacional o *hardware*, deberás protegerlo con tanto celo como lo hiciste originalmente con la película, evitando que la clave o la película descifrada se filtren o sea «hackeada».[6] Primero, has aumentado el número de activos a proteger: ni la obra ni su clave de descifrado deben darse a conocer sin tu autorización. En segundo lugar, sólo

3. Waterman y otros (2007) discuten sobre las ventanas de lanzamiento.

4. Si usted usa un algoritmo conocido y fuerte puede estar seguro que nadie sin la clave podrá descifrarlo, o por lo menos nadie con capacidad informática disponible actualmente (Schneier, 1996: 152).

5. «Caja negra» se refiere a la opacidad en el procesamiento entre el cifrado inicial y la película final. Aunque el usuario puede ver el ingreso de la información encriptada resultando en una película en formato inteligible, no puede ver qué sucede durante el tiempo en el cual la película está siendo descifrada.

6. Messmer (2010) y Patrizio (1999) describen la ingeniería reversa del *software* Xing decodificador de DVD implicado en el primer hackeo de un DVD.

has modificado el enfoque de confianza, en lugar de removerlo. Todavía necesitas permitir que el usuario vea la película, y has decidido que no confías en él (en consecuencia, necesitas utilizar medidas tecnológicas de protección), pero para confiar en los fabricantes de programas computacionales o *hardware*, deberás hacer que ellos confíen en ti y no en los dueños o usuarios de los productos que fabrican. Simultáneamente, deberás adoptar medidas para evitar que el usuario copie un ejemplar de la obra[7] o que obtenga *hardware* o *software* que reproduzca el ejemplar copiado.[8]

Deberás, sin embargo, crear este ecosistema seguro con la compatibilidad necesaria como para atraer a los usuarios, y con suficiente control como para que los proveedores de contenido estén seguros que tus directivas se están cumpliendo. Después de todo, los propios usuarios ya se encuentran en un contexto tecnológico antes del lanzamiento de la película, pudiendo tener computadores, televisores, sistemas *home theaters*, redes caseras, video iPods o iRivers. Es poco probable que ellos deseen ver la película lo suficiente como para rediseñar todos estos sistemas, o que quieran adquirir un dispositivo específicamente para estos fines.[9] Por lo tanto, tu plan funcionará mejor si puedes aprovechar plataformas existentes. Si éstas no son suficientemente seguras, puedes tratar de atraer a un segmento importante de la industria para trabajar en la migración de los usuarios a un nuevo estándar tecnológico (con la ayuda de abogados

7. El formato DVD es controlado a través de un conjunto de patentes existentes sobre el formato, derechos de autor con medidas antielusión e incluso a través de marcas comerciales (véase *RealNetworks, Inc. v. DVD Copy Control Association*, 641 F. Supp. 2d 913, Northern District of California, 2009, pág. 920, que describe el DVD-CCA y su tecnología; véase, además, Marks y Thurnbull, 1999).

8. Seltzer (2005) describe las *broadcast flag*, etiquetas transparentes incorporadas en la señal de televisión dirigidas a los equipos receptores para que permitan grabar o no un programa transmitido.

9. En casos especiales, esta condición puede ser maleable. En el año 2005, la Academia de Obras Cinematográficas envió 6.000 reproductores de DVD, especialmente diseñados, a miembros de la Academia: un número limitado de personas designadas para recibir películas antes de su lanzamiento al público general. Incluso ahí, las limitaciones molestaron a los espectadores y algunas copias de estas obras se filtraron. Gentile (2004) y Leach (2007) detallan las quejas de un miembro de la Academia y cómo estas precauciones no impidieron la filtración de copias.

antimonopolios que aseguren que esta colaboración sea vista como una expansión del mercado, y no como un intento de controlarlo).[10]

Así podrías, si fueras un estudio cinematográfico con suficiente influencia sobre el mercado, persuadir a otros estudios, compañías electrónicas y desarrolladores de *software*, para que apoyen conjuntamente un plan de protección anticopia en torno a un nuevo formato digital para la distribución de video, estableciendo condiciones de licenciamiento para el uso y la interoperabilidad con ese formato.[11] Juntos, podrías esperar alcanzar la saturación del mercado que haría de tu formato todo un éxito: sólo reproductores de SuperDisc autorizados podrían reproducir las últimas y más grandes películas de Hollywood en toda su gloria digital. La red virtual entonces creada podría hacer que tus reglas parecieran ser complementos naturales para este nuevo formato, sin restricciones hostiles a los derechos de los consumidores y usuarios. Podrías mantener a la compañías fieles a tu esquema de licenciamiento bajo la amenaza de las responsabilidades impuestas por la Digital Millennium Copyright Act (DMCA) en caso que abandonaran tu esquema; mientras tanto, tus competidores podrían incluso agradecerte (confidencialmente) por ayudarlos a establecer un set legal de barreras de entrada al mercado de la tecnología.

Mientras que los acuerdos de licencia respaldados por derechos de autor podrían mantener a los agentes comerciales bajo control, tú también deseas limitar a los empresarios que pudieran ser vistos como futuros competidores, como asimismo a potenciales copiadores individuales. No es suficiente exigir que los licenciatarios limiten la funcionalidad de sus dispositivos si los usuarios pueden desactivar esas limitaciones presionando unas pocas teclas del control remoto.[12] Mientras los usuarios

10. Véase la carta de Joel I. Klein, Asistente del Fiscal General del Departamento de Justicia, a Garrard R. Beeney, de Sullivan & Cromwell (16 de diciembre de 1998), disponible en <http://www.justice.gov/atr/public/busreview/2121.htm>.

11. Cf. pie de página anterior.

12. Por ejemplo, muchos reproductores de DVD antiguos bloqueados por región podían ser programados para reproducir discos de cualquier región presionando algunas teclas del control remoto (véase Post-Hearing Comments of the Electronic Frontier Foundation, «In re Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies», Docket nro. RM 2002-4, 5 de junio de 2003, pág. 6, disponible en <http://www.copyright.gov/1201/2003/post-hearing/post10.pdf>).

se vuelven más sofisticados, tú comenzarías a preocuparte por sus habilidades con destornilladores, placas de circuitos y compiladores de *software*. Por lo tanto, exigirás que sus licenciatarios impongan limitaciones estrictas que prohíban las modificaciones realizadas por usuarios.[13] El objetivo es que nadie más que aquellos que se han obligado a los términos de licenciamiento establecidos por ti puedan acceder a su película.

Además, una vez que has sucumbido a los imperativos de la protección tecnológica, es poco probable que te detengas en un solo componente. Si incluyes en una «caja negra» el *software* o el *hardware* decodificador, pero no aseguras los dispositivos de salida provenientes de la «caja negra» alguien podrá obtener el flujo descifrado desde ahí.[14] Si usted deja dispositivos de salida análogos de alta calidad, alguien podría redigitalizar el contenido obtenido a través de este «agujero análogo».[15] Si deshabilitas estos dispositivos de salida, sin embargo, enfrentarás las protestas de los usuarios que no están dispuestos a que sus dispositivos electrónicos sean selectivamente deshabilitados.[16]

---

13. Para que la implementación de medidas tecnológicas de protección tenga sentido en un escenario de confianza limitada, las barreras impuestas en contra de modificaciones por parte de los usuarios a la administración de derechos, debe ser por lo menos tan fuerte como aquéllas en contra del acceso de usuarios al contenido protegido (véase DVD-CCA CSS Procedural Specification § 1.6.2.4-2.5, disponible en <http://cyber.law.harvard.edu/seminar/internet-client/readings/week2/02-08CSS.pdf>).

14. Por consiguiente la Protección de Contenido de Banda Ancha Digital (HDCP, por sus siglas en inglés) para Interface Multimedia de Alta Definición (HDMI, por sus siglas en inglés) y la Interface Visual Digital (DVI, por sus siglas en inglés) proveen encriptado de las emisiones de video digital, confiando en interacciones digitales seguras y encriptadas para verificar la confiabilidad de los componentes al otro extremo del cable de video (véase Digital Content Protection, «High-Bandwidth Digital Content Protection System», 8 de julio de 2009, pág. 8, disponible en <http://www.digital-cp.com/hdcp_technologies>, seleccionar «HDCP Specification Rev. 1.4»).

15. Véase Copy Protection Technical Working Group, Charter of the Analog Reconversion Discussion Group, disponible en <http://www.cptwg.org/Assets/text%20files/ardg/analogcharterfinal11403.doc>. Este documento se refiriere a «las preocupaciones de los titulares de derechos de autor sobre la seguridad presente y futura de los contenidos de obras audiovisuales comerciales que han sido convertidas desde formato digital a formato análogo y reconvertidas a formato digital».

16. Hachman (2009) discute la petición de la Motion Picture Association of America (MPAA) a la Federal Communications Commission (FCC) referente al Control de Producción Seleccionable y la oposición por parte de Public Knowledge.

Antes que lo sepas, si tomas en serio las restricciones tecnológicas anticopia, estarás pidiendo a tus espectadores que actualicen todos los dispositivos en sus casas para satisfacer interacciones digitales seguras y encriptadas entre dispositivos; o bien degradarás el video de alta definición a una resolución lo suficientemente baja como para que los usuarios se pregunten si vale la pena tanto lío (Taub, 2001). Estarás exigiendo que cada dispositivo digital fabricado incorpore tecnología anticopia.[17] Ahora, si tan sólo pudiésemos contar con un *neuralyzer* para borrarles la memoria a los espectadores, después que terminarán de ver la película,[18] podría incluso evitar que éstos creasen «obras derivadas», compartiendo sinopsis detalladas con amigos.

No hemos conseguido que el *neuralyzer* se produzca en masa todavía, pero intentos de poner en práctica o implementar otras medidas tecnológicas van más allá de la ciencia ficción. Una gran cantidad de asociaciones llenas de siglas y grupos de presión han procurado o intentado legislar respecto a diversas partes de este escenario.[19] Aquellos que cuentan con la tecnología necesaria para resolver los problemas que creen que las tecnologías han exacerbado, se han acercado inexorablemente hacia regulaciones tecnológicas cada vez más estrictas y rigurosas. A medida que esas regulaciones se vuelven más amplias, se amplía también una grave consecuencia no prevista: la limitación del desarrollo independiente y de la innovación de usuario.

~

¿Qué importa si las medidas tecnológicas de protección impiden la innovación de usuario? La mayoría de las personas nunca va a modificar sus

17. Este proyecto de ley fue presentado por el senador Fritz Hollings. El profesor de ciencias computacionales de la Universidad de Princeton Ed Felten generó una «Fritz Hit List» con tecnologías que podrían haber sido reguladas si la ley hubiese sido aprobada, cualquier dispositivo que incluya audio o video digitalizado, incluyendo monitores de bebé y Big-Mouth Bill Bass, el pez parlante (véase «Fritz's Hit List, Freedom to Tinker», disponible en <http://www.freedom-to-tinker.com/tags/fritzs-hit-list>).

18. En la película *Men in Black* (Columbia Pictures, 1997), agentes equipados con *neuralyzers* borraban selectivamente las memorias de los testigos que hubiesen visto demasiado.

19. Las notas al pie de página se refieren a escenarios de la vida real en los cuales este relato de ficción se basa.

reproductores digitales. En un mundo en el que los videocasetes (VCR, por sus siglas en inglés) y sus sucesores, los DVD, siguen parpadeando «12:00», ¿por qué debiéramos preocuparnos por facilitar la compleja innovación de usuario? La innovación de usuario beneficia indirectamente incluso al usuario final no técnico. Cuando los usuarios curiosos tienen acceso para modificar y desarrollar tecnología, tienden a compartir sus mejoras, haciendo más fácil su obtención para quienes no realizan este tipo de actividades. Así, incluso si usted no se encuentra inmerso en la cultura «hágalo usted mismo» de modificar sus propios dispositivos, es posible que pueda comprar un producto que se adapte mejor a sus necesidades, ya que ha sido desarrollado gracias a los aportes de usuarios innovadores con gustos similares a los suyos; o usted puede contratar a alguien para agregar las características que desea añadir a un producto, encontrando que tiene más y mejores opciones gracias a que ningún fabricante puede reclamar el monopolio sobre las actualizaciones y mejoras.

Compare los ecosistemas alrededor de la música grabada y de las películas. Desde la década de 1980, la música grabada ha estado disponible en formato digital sin encriptar, en discos compactos, mientras que las películas básicamente saltaron del VHS analógico (y protegidas por Macrovision) a formatos protegidos por DRM con la introducción del DVD en 1997 y la aprobación de la DMCA en 1998.[20] Esta diferencia (que los sellos discográficos lamentan eternamente) ha significado que la música grabada puede ser legalmente manipulada mucho más fácilmente que el video. Los CD proveen de música digital de alta calidad, sin codificar, directamente a los usuarios finales. Los usuarios finales podían acceder a música digital libre de DRM mucho antes que la mayoría de las editoriales o tiendas de música ofrecieran canciones sin DRM en línea. Un entorno completo de música puede ser libremente utilizado en dispositivos de lectura abierta.

Los innovadores han tomado esa libertad y la han utilizado profusamente. Cuando el reproductor de CD fue introducido al mercado en 1982, a un precio minorista de 900 dólares (Marcom, 1985), éste podía reproducir un disco, saltar a una pista determinada, buscar o repetir. En los años venideros, la experiencia de la música digital ha sido mejorada

20. Los discos Láser nunca alcanzaron una penetración significativa en el mercado (Landro, 2008).

gracias a actores de todas las formas y tamaños: grandes fabricantes, empresas pequeñas y usuarios finales. A los reproductores de discos se le han incorporado características tales como modos de reproducción aleatoria, dispositivos de salida digitales, controles basados en menús, cambiadores de discos múltiples y versiones portátiles. Quizás lo más importante, es que la música no se ha limitado a los discos. El Diamond Rio, introducido en el año 1998, llevó la música digital a bolsillos demasiado pequeños para el Discman.[21] Una década más tarde, aunque el Diamond Rio ya no existe, dio paso a cientos de reproductores de música portátil (Musgrove, 2001). Algunos de estos reproductores se fabricaron abiertos;[22] otros han sido luego abiertos.[23] Algunas características que fueron desarrolladas por los usuarios, tales como la grabación de audio para el iPod, han sido comercializadas desde entonces, trayendo al público masivo estos desarrollos de usuarios.

El Squeezebox, por ejemplo, comenzó como un pequeño dispositivo musical conectado a través de un cable Ethernet fabricado por una pequeña empresa, Slim Devices. El Slimp3 inicial podía llevar música desde un computador a un sistema estéreo, a través de un convertidor digital a analógico, un poco de poder computacional y una pantalla brillante. Desde entonces, ha dado lugar a una línea completa de dispositivos de música, desde productos inalámbricos para consumidores comunes hasta productos altamente especializados dirigidos a audiófilos.[24] Conectado a un equipo que ejecuta el software *Squeezebox Server*, el Squeezebox libera música desde el disco duro de un computador para ser escuchada en cualquier lugar de la casa, añadiendo una pantalla de «ahora reproduciendo», un control remoto, menús de selección basados en la web, y todas las flexibilidades propias de una librería musical digital, incluyen-

21. Dunn (1998) señala que «el último regalo de Navidad de este año fue el reproductor de MP3 Diamond Multimedia Rio de 199 dólares, un dispositivo del tamaño de una cajetilla de cigarrillos». Véase, además, «Sony Corp. Introduces New Compact-Disk Player», *Wall Street Journal*, 17 de marzo de 1988, pág. 7.

22. Véase, por ejemplo, Teuthis Open Source Kits, Daisy MP3 Project Page, disponible en <http://www.theutis.com/daisy/index.html>.

23. Véase, por ejemplo, Rockbox Software Project, disponible en <http://www.rockbox.org/twiki/bin/view/Main/WhyRockbox>.

24. Véase Logitech, Logitech Squeezebox, disponible en <http://www.logitechsqueezebox.com>. Slim Devices es ahora un área de Logitech.

do prolongadas e ininterrumpidas listas de reproducción, acceso fácil a toda la música en un sólo lugar y sin ningún disco físico que buscar o rayar. Debido al formato abierto de la música y a la habilidad de los usuarios para transportarla sin controles de copia, el Squeezebox pudo ser desarrollado sin el apoyo o permiso de la industria musical establecida. Sus desarrolladores podían tomar la disponibilidad de la música digital y construir para interoperar con la interfaz.

Por otra parte, aquellos que compran el Squeezebox no se encuentran limitados a lo que viene en la caja, ya que pueden personalizar el *software* de código abierto *Squeezebox Server*. Muchos lo han hecho, escribiendo y distribuyendo *plugins* para configurar alarmas musicales, programar estaciones de radio, mostrar el tiempo e integrarse con otras aplicaciones.[25] Incluso aquellos que no escriben códigos tienen acceso a los productos de la comunidad, ya que muchos usuarios comparten sus aportes.[26] Incluso Chumby, una plataforma de *hardware* abierto, que por su diseño se parece a un *beanbag* con una pantalla (y altavoz), puede ser programado para reproducir música desde una librería administrada por *Squeezebox Server.*[27]

El Squeezebox es sólo un ejemplo. Debido a la naturaleza abierta de la música digital y de las transmisiones televisivas, los usuarios y desarrolladores independientes pueden crear y elegir su experiencia preferida. Podemos llenar nuestros dispositivos portátiles con sets de pistas de música; podemos equipar nuestros hogares con sistemas de audio y video conectados a la red que comparten el contenido alrededor de la

25. Los usuarios pueden crear listas de reproducción a través de un motor de recomendaciones de terceros MusicIP, organizar la metadata musical sobre índices de Gracenote o MusicBrainz, o enviar hábitos musicales como estatus a un blog. Véase SqueezeCenter Plugins, disponible <http://www.wiki.slimdevices.com/index.php/SqueezeCenter-Plugins>.

26. El *Squeezebox Server* fue lanzado bajo una licencia GNU (General Public License), versión 2. Véase Softpedia, Download SqueezeBox Server, <http://mac.softpedia.com/get/Audio/SqueezeCenter.shtml>. La licencia GNU GPL bajo la cual fue lanzada no requiere las redistribución de la fuente, pero señala que aquel que distribuye binarios compilados también debe distribuir la fuente que la acompañe. Véase Free Software Foundation, GNU General Public License, Version 2 §3 (1991), disponible en <http://www.gnu.org/licenses/gpl-2.0.html>. Muchos usuarios-desarrolladores encuentran atractivo compartir su trabajo con la comunidad, invitando las mejoras de otros.

27. Véase *Chumby: Squeezebox Server* en <http://www.chumby.com/pages/cp_squeeze>.

casa o nos siguen a medida que nos movemos; podemos disponer de los horarios en los cuales accedemos a programas de televisión; podemos sincronizar nuestras colecciones de música y video entre dispositivos y a través de diferentes formatos. DJ, profesionales o en casa, pueden mezclar *beats* a la perfección.[28]

Ahora compare el vibrante ambiente en el que se desarrolla la música y el rango de dispositivos capaces de reproducirla, con los límites existentes sobre las películas. El DVD ha sido uno de los productos electrónicos de consumo de mayor éxito de todos los tiempos, con números que crecieron rápidamente después de su lanzamiento en 1997 (JOHNSON, 2004), pero la experiencia de ver películas apenas ha cambiado desde entonces. El HD-DVD y el Blu-Ray introdujeron imágenes de mayor resolución, pero no permiten mucho más que ver películas y los extras.[29] En su mayor parte, las nuevas tecnologías para ver películas ofrecen sólo las mismas características básicas que ofrecían los reproductores de DVD cuando fueron lanzados al mercado, hace más de una década. A la fecha no existen *jukebox* de discos DVD,[30] ni navegación directa simple, ni la opción de seleccionar escenas de algunas películas para mostrarlas en secuencia o en comparación. Sólo en el último año los usuarios finales han

28. Es verdad, las leyes de derecho de autor limitan a los usuarios cuando realizan copias, pero mientras hayan comprado la música, pueden ampararse bajo los «usos justos» referente al derecho de manipular su acceso a la música, incluso cuando esto signifique la realización de copias transitorias (Litman [2001: 26-8] describe las consecuencias de tratar todo lo digital como copia). El derecho de autor no debiera impedir el mero acto de escuchar; véase *The Cartoon Network, LP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008), que determinó que el almacenaje remoto de los dispositivos de grabación de video digital de Cablevision no violaba los derechos de autor de los demandantes.

29. Ni siquiera queda claro si muchos consumidores notan la diferencia. Muchos todavía tienen pantallas de baja resolución, y falsificadores comerciales han tomado ventaja de la ignorancia de los consumidores para vender discos Blu-Ray falsos, comprimidos a una resolución más baja (cf. Fowler, 2008).

30. Kaleidescape introdujo un sistema con un valor de alrededor de 8 mil dólares; sin embargo, aunque ganó la primera ronda de batallas contractuales con DVD-CCA, la Corte de Apelaciones revocó y reenvió para mayor consideración la especificación general de CSS, que Kaleidescape consideraba inaplicable (*DVD Copy Control Ass'n v. Kaleidescape*, Inc., 176 Cal. App. 4th 697, Cal. App. 6th Dist. 2009). DVD-CCA exitosamente logró impedir a RealNetworks la creación de un dispositivo más barato (*RealNetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, N.D. Cal. 2009).

obtenido la oportunidad (aprobada por los estudios cinematográficos) de copiar una película en un reproductor portátil, enviarla a un teléfono móvil, o ponerla en una red casera para que pueda moverse desde la cocina a la sala de estar o al dormitorio. Mientras tanto, los reproductores de MP3, comerciales o caseros, impulsados por el desarrollo *amateur*, han sido capaces de hacer esto con la música durante años, dejando a las películas atrás. Los DVD protegidos por candados digitales amparados por la DMCA dejan fuera a los desarrolladores independientes y a mucha de la experimentación que esto conlleva. Los usuarios han debido esperar años para que los «modelos de negocios» se pongan al día con características tales como las descargas digitales o la «copia digital» autorizada.[31]

~

Un impresionante número de estudios se han generado alrededor de la tecnología de gestión de derechos digitales, DRM.[32] La mayoría de quienes estudian el tema critican los DRM por sus efectos sobre el *fair use*:[33] en un mundo basado en ellos, un profesor de comunicación no puede utilizar el clip de una película para hacer comentarios en su clase sin una excepción especial; un crítico literario no puede extraer páginas de un libro electrónico (o incluso pueden borrarle sus libros electrónicos),[34] y un artista *mashup* se encuentra impedido de hacer *sampling*. Estas restricciones son consecuencias directas de los DRM, generando dificultades para los derechos de autor y para la cultura (Litman, 2001; Cohen, 1998b: 462; Samuelson, 1999: 519). La mayoría de los académicos han caracterizado el «problema de los DRM» como un problema de ajuste con el *fair use*. Algunos alegan que la pérdida de *fair use* marginales es

31. Por ejemplo, Disney File Digital Copy en <http://disney.go.com/disneyvideos/disneyfile/>. Los alquileres todavía son limitados en variedad y la portabilidad usualmente restringida a una pequeña e inconsistente variedad de dispositivo.

32. Véase más adelante la parte 3.

33. Nota de los traductores. Hemos decidido mantener la expresión *fair use* en su lengua original, usualmente traducida como «usos justos» o »usos legítimos», para identificar con precisión esta institución del derecho de autor norteamericano.

34. Fowler (2009) describe la eliminación del libro electrónico *1984* de los Kindles de los usuarios debido a que el distribuidor carecía de los derechos para comercializarlo.

un costo necesario para la mejor protección de los derechos de autor (Picker, 2005; Ginsburg, 2003). Otros argumentan que el problema del *fair use* puede ser resuelto a través de permisos de usuario, anulaciones o recursos a una tercera parte.[35] Otros sostienen que el *fair use* en los medios digitales es innecesario, ya que estos derechos pueden ejercerse a partir de otros formatos.[36] Sin embargo, otros argumentan que debido a que el corazón del *fair use* es, precisamente, el uso sin autorización de una manera imprevista; los controles tecnológicos y las excepciones nunca podrán igualar la gama de consideraciones que un juez podría considerar si el asunto llegara a su conocimiento a través de un litigio (Armstrong, 2006: 57-59, 85-87), ni la espontaneidad de «usar primero, pedir permiso después».

El debate sobre *fair use* es importante, pero no es el único problema que existe con los DRM. Igualmente importante, pero hasta ahora ignorado, es el impacto en la innovación de usuario y en el desarrollo legítimo de tecnología de medios digitales. Dado que los sistemas de DRM, por su diseño y por su técnica contractual, deben ser endurecidos en contra de las modificaciones de usuario, terminan excluyendo toda una gama de tecnologías y un modo completo de desarrollo. Este problema es distinto del problema del *fair use*. Incluso si pudiéramos agitar una varita mágica y acomodar totalmente el *fair use* a los DRM, la incompatibilidad con la innovación de usuario se mantendría, ya que proviene de un aspecto diferente y más profundo de los sistemas de DRM. Incluso los sistemas «más justos» en el mercado hoy en día, son injustos para los desarrolladores de nuevas tecnologías.

---

35. Por ejemplo, Fox y LaMacchia (2003). Burk y Cohen (2001) consideran y rechazan este camino. También Erickson y Mulligan: «En este sentido, el sistema se quebraría desde una perspectiva de derechos de autor: el sistema puede proteger los derechos de autor del creador mientras que altera el balance de la ley de derechos de autor, al eliminar derechos de los usuarios y la posibilidad de nuevos «derechos» que puedan emerger orgánicamente a través del proceso legal» (2004: 995).

36. La Corte, en el caso *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001), adoptó los argumentos de la demandante en el siguientes sentido: «La DMCA no impone ni siquiera una limitación discutible respecto a la posibilidad de ejecutar una variedad de usos justos en películas en formato DVD, tal como comentar su contenido, citar extractos de sus guiones, e incluso grabar porciones de las imágenes de video y sonidos del filme, apuntando una cámara o un micrófono al monitor mientras se ejecuta la película DVD» (pág. 459).

Las leyes antielusión, respaldando las medidas tecnológicas de protección y las normas de blindaje, son fundamentalmente incompatibles con la innovación de usuario de nivel profundo. En un régimen de derechos de autor utilitarios, en el que, como Thomas Macaulay ha señalado, los derechos de autor se aceptan como «un impuesto a los lectores con el fin de dar una recompensa a los escritores» (1952: 734-5), la ley debe tener en cuenta todos los costos asociados a eliminar modos abiertos de desarrollo. El «impuesto al modo de desarrollo» es una importante carga no reconocida en las economías basadas en la cultura, la creatividad y la tecnología.[37]

La segunda parte del presente artículo examina la ley y la tecnología de gestión de derechos digitales, particularmente la interacción de la ley estatutaria, las medidas tecnológicas de protección y las condiciones de blindaje contractual generalmente añadidas a ellas. La parte tercera, en tanto, examina brevemente la historia y los debates académicos actuales en torno a los DRM, con el fin de analizar por qué se han pasado por alto los impactos a la innovación de usuario. La parte cuarta desarrolla ejemplos de los conflictos existentes entre los DRM y los modelos de desarrollo abierto, en contraste a mecanismos anticopia de «advertencia» más flexibles. En la parte quinta se expone la rica literatura económica y comercial existente respecto a las innovaciones tecnológicas y la innovación de usuario, para argumentar que las restricciones impulsadas por los DRM son sustancialmente perjudiciales para el desarrollo cultural y tecnológico, así como para la autonomía del usuario. Finalmente, la parte sexta llega a la conclusión de que el impuesto al modo de desarrollo es un precio demasiado alto a pagar por una protección imperfecta de los derechos de autor.

2. LOS MECANISMOS DEL CÓDIGO Y DE LA LEY

A) TECNOLOGÍA BÁSICA DE LA GESTIÓN DE DERECHOS DIGITALES

La tecnología de gestión de derechos digitales apunta a «dar» obras digitales a los usuarios, mientras que a su vez gestiona sus usos o copias: una canción protegida con DRM de la tienda de música iTunes puede ser

37. Para ver un ejemplo de este impuesto tecnológico, uno sólo necesita observar los reproductores musicales versus los reproductores de DVD, mencionados antes.

transferida a sólo cinco dispositivos; un DVD sólo puede ser reproducido en reproductores autorizados, codificado para la región para la cual fue vendido; una película *pay-per-view* «caduca» veinticuatro horas después de haber sido ordenada. El reto fundamental de los DRM es proporcionar los usos deseados, pero no más que eso: ofrecer a los usuarios control suficiente para disfrutar de la obra, pero no lo suficiente como para permitir que ellos (o los sistemas bajo su control) copien las obras.[38] Llevando las cosas al extremo, por supuesto, se podría desarrollar un sistema completamente seguro, negando el acceso a todo el mundo, pero esto tendría poca demanda en el mercado.[39]

Un archivo multimedia digital es una serie de bits (unos y ceros) escritos en un formato que puede ser leído por un *hardware* o reproductor de *software*, en forma de música, texto, video o una combinación multimedia. Los archivos digitales son inherentemente copiables, ya que no suele haber escasez de bits o medios de almacenamiento para mantenerlos. Como dice el criptógrafo Bruce Schneier, «tratar de hacer que los archivos digitales no sean copiables es como tratar de hacer que el agua no sea húmeda».[40] Para gestionar los bits, por lo tanto, los proveedores tratan de controlar el acceso —restringiendo el acceso a suscriptores pagos autentificados, o impidiendo la copia— encapsulando los bits en una especie de contenedor, ya sea físico o digital, que resista el acceso de un posible copista.[41]

---

38. Véase Reid y Caelli (2005). La premisa esencial de los DRM es que un titular de derechos desea licenciar contenido digital (el cual se representa a través de dígitos binarios o bits) a un licenciatario o cliente quien acepta vincularse por las condiciones de la licencia. Es necesario notar que el cliente no está comprando los bits en sí mismos. En cambio, lo que están adquiriendo es el derecho a usar los bits de una forma definida y restringida, en los términos autorizados por la licencia. Entonces, la licencia define una política de uso.

39. Cercano a este extremo, los productores de medios digitales sueñan con un mercado segmentado por precios, en donde cada uso puede ser avaluado de acuerdo a la disponibilidad de los usuarios para pagarlo. Véase Meurer (1997: 877) y también Fisher III (2007: 1).

40. Schneier (2006) describe lo rápido que Microsoft parchó su reproductor de multimedia para desactivar el software FairUse4WM, el cual quitó la protección de copia existente en los archivos DRM 10 y 11 del programa Windows Media.

41. Más precisamente, podemos distinguir controles de acceso, controles de copia y timbres de agua: los controles de acceso apuntan a impedir que usuarios no autorizados

Puesto que los bits son fácilmente copiables, los controles de copia dependen de la cooperación de los dispositivos de acceso y de reproducción para su funcionamiento. Las editoriales tratan de integrar sus obras a un ecosistema en donde las copias no puedan ser reproducidas. Las cintas de video VRC, un medio de grabación analógica, utilizan el ruido incorporado de Macrovision como una estrategia de contención.[42] Aunque esta protección podía ser superada programando la primera videocasetera para suprimir la señal de ruido o la segunda para ignorarla, fue efectiva cuando era utilizado con un par de dispositivos idóneos.[43] La efectividad de los controles de copia de los VHS dependía, por consiguiente, tanto de manipular el formato de la señal como de limitar el diseño de dispositivos de reproducción y grabación. Ya que lo que la tecnología podía establecer, la misma tecnología podía cambiar; la tecnología es necesaria pero no suficiente para proteger el contenido digital. Para controlar la copia, los sistemas anticopia controlan entornos (y sus usuarios).

La tecnología de control de contenidos es una perpetua competencia armada. Los entornos protegidos persisten por un tiempo, y entonces caen frente a ataques más fuertes, a través de análisis de códigos, manipulación de *hardware* o captura de señales desde el dispositivo.[44] De-

---

accedan a un recurso determinado; los controles de copia tratan de prevenir su reproducción; y los timbres de agua rastrean el uso o reproducción de un recurso, sin necesariamente impedir algún tipo de conducta.

42. Véase «How Stuff Works, How Does Copy Protection On a Video Tape Work?», disponible en <http://electronics.howstuffworks.com/question313.htm>. Una señal integrada en el intervalo de supresión vertical de los datos del video no se muestra en la reproducción en el televisor, sino que interfiere con el componente de control de aumento automático de otros videograbadoras, impidiendo la grabación de VCR a VCR.

43. Macrovision inicialmente tomó ventaja de las propiedades accidentales de la tecnología VCR. Sin embargo, los fabricantes de VCR, una vez que tomaron conciencia de su uso como control de copia, diseñaron sus dispositivos para que no fueran engañados por las señales espurias de Macrovision. Entonces, para robustecer este control de copia, el Congreso añadió un mandato legal a la DMCA. «Ninguna persona fabricará, ofrecerá al público, comercializará ninguna… grabadora videocasete en formato VHS, a menos que tal dispositivo se encuentre conforme a la tecnología de control de copia…» (17 USC § 1201 (k)(1)(A)(i) (2006)).

44. Si la reproducción se encuentra en un *software*, los usuarios podrían tratar de obtener el *software* para descargar los datos sin cifrar, por ejemplo, copiándolo de memoria,

bido a que hay muchas más personas tratando de romper los sistemas de protección que de fortalecerlos, los atacantes tienen una ventaja en el largo plazo.[45] Entonces, las leyes antielusión tratan de evitar lo in-

emulando una tarjeta de sonido o video, o emulando un entorno completo. Véase Schoen (2003) y también Huang (2003: 119-37); veáse Messmer (2010).

45. Los lectores pueden preguntarse cómo los DRM difieren del cifrado fuerte, que puede ser implementado en el código abierto y, sin embargo, soportar irrupciones contra significativos actores estatales y no estatales que quisieran romperlo. La encriptación para proteger el contenido contra el espionaje por parte de terceros enemigos es un problema difícil, pero bien entendido. Ahora tenemos algoritmos aplicables (y aplicados) sobre computadoras personales que se creen que son impermeables a los ataques con todo el poder computacional del mundo. Sólo un ataque de fuerza bruta, probando todas las claves posibles, podría descifrar el encriptado, incluso uno con una simple clave de 64 bits, esto deja las posibilidades en 1,8 elevado a 19.

El problema de los DRM es, sin embargo, diferente. Como Cory Doctorow ha señalado, «en los DRM el atacante es también el destinatario» (Cory Doctorow, «Address to the Microsoft Research Group», 17 de junio de 2004, disponible en <http://craphound.com/msftDRM.txt>). El usuario del material protegido por DRM es también aquél contra cuyo espionaje el sistema está tratando de proteger. El «lomo de toro» debe impedir que el usuario haga cosas no deseadas con el archivo, permitiendo al mismo tiempo que pueda hacer las cosas para las cuales ha pagado. Mientras que la criptografía moderna ha resuelto muchos problemas difíciles, es impotente ante el desafío de mostrar algo y al mismo tiempo impedir verlo.

El código abierto funciona de maravilla con el cifrado porque los criptosistemas modernos se construyen, siguiendo el principio de Kerkhoffs, en la máxima de menor secreto posible: revelar algoritmos y asegurar claves. Cualquiera puede implementar cifrado compatible con Pretty Good Privacy (PGP), y descifrar un mensaje firmado por PGP en el código abierto GNU Privacy Guard (GPG) siempre y cuando él tenga la clave privada con la que se ha cifrado. Los usuarios pueden verificar de forma independiente (o terceros comprobar por ellos) la seguridad de sus aplicaciones, y a la vez mantener, a través de algoritmos, la seguridad de comunicaciones determinadas, respecto de cualquiera que conozca las claves particulares asociadas a ese intercambio en particular. El modelo de amenazas, como los investigadores de seguridad lo describen, es la tercera parte que espía. Alice y Bob pueden comunicarse de forma segura sin que Eva escuche. Incluso si Eva capturara el flujo de comunicaciones, sin la clave, sólo ve un flujo de comunicaciones ininteligibles.

La encriptación asimétrica, o clave pública, permite a los emisores y receptores intercambiar mensajes cifrados sin tener que intercambiar secretos antes. El destinatario publica una clave pública, la mitad de un par de claves público/privadas, resguardando la mitad privada. El emisor encripta con la clave pública, utilizando algoritmos públicos, y sólo el destinatario en posesión de la clave privada puede descifrar el mensaje. Incluso

evitable, trayendo la artillería pesada de las sanciones civiles y penales a la batalla entre fabricantes de DRM y quebrantadores de DRM. Esto posibilita la manipulación, a través de los DRM, del entorno en el cual los medios digitales son reproducidos limitando los dispositivos, puesto que ellos pueden «contener» medios protegidos. La protección de copia nunca puede regular sólo el objeto en sí mismo, sino que debe regular todo el ecosistema para proteger una obra con eficacia. Por lo tanto, la tecnología DRM implica todo un conjunto de normas subsidiarias para imponer su cumplimiento.[46]

B) LOS MECANISMOS DE LAS LEYES ANTIELUSIÓN

Las leyes antielusión extienden el control de los derechos de autor, proporcionando un gancho legal del cual los titulares pueden colgar restricciones contractuales adicionales. La industria del entretenimiento de Estados Unidos presionó a la Organización Mundial de Propiedad Intelectual (OMPI) para reconocer protección jurídica a las medidas tecnológicas de protección en el artículo 11 de Tratado OMPI sobre Derecho de Autor.[47] Para implementar esta obligación internacional, el Congreso

---

el espía, con toda la otra información sobre el mensaje (algoritmo y clave pública), no puede hacer nada más que tratar los ataques de fuerza bruta, que no funcionarán si las partes han utilizado una clave lo suficientemente larga.

Este método funciona bien como un control de acceso inicial: sólo quien tiene la clave privada puede leer los mensajes enviados a ella, pero no para hacer valer ningún tipo de control después de que el mensaje ha sido descifrado, como intentan hacerlo los DRM. Sin embargo, cuando los sistemas DRM utilizan cifrado para el control de uso, están tratando de asegurar las comunicaciones en contra de los mismos usuarios a quienes está tratando de vender dicha comunicación, todo mientras tratan de entregar el uso para el cual el usuario ha pagado. Es como si la misma persona es a la vez Bob, el destinatario, y Eva, la espía. La solución de los DRM es entregar las claves de Bob para ver, sin dárselas a Eva, su alter ego. Podríamos prohibir a Bob hacer cosas malas con las claves, pero eso es lo que ya hace la ley de derechos de autor, al prohibir el uso no autorizado. Entonces, existen dos cosas que el sistema debe ocultar, al tiempo que lo hacen usable, la clave y el texto.

46. Crawford (2003: 629) entrega un ejemplo extremo del impacto en el entorno: una vez que el vampiro DRM muerde, cualquier otro dispositivo conectado a un sistema de DTV Broadcast Flag estaría sujeto a control regulatorio.

47. «Las partes contratantes proporcionarán protección jurídica adecuada y recursos jurídicos efectivos contra la acción de eludir las medidas tecnológicas efectivas que sean

aprobó el capítulo 12 de la Ley de Propiedad Intelectual a través de la DMCA.[48]

La sección 1201, la disposición central de las leyes antielusión, establece que los titulares de derechos de autor que añadan candados tecnológicos a sus obras pueden servirse de sanciones civiles y penales[49] para impedir que otros «eludan» esas protecciones.[50] La ley protege a la tecnología DRM a través de tres restricciones, prohibiendo a cualquiera que «eluda una medida tecnológica que efectivamente controle el acceso» a una obra protegida por derechos de autor,[51] o que fabrique, importe, ofrezca al público, proporcione o que de cualquier manera comercie tecnología, producto, servicio, dispositivo, componente, o parte de los mismos, que:

a) esté diseñado o producido principalmente con el propósito de eludir una medida tecnológica que controla efectivamente el acceso a una obra protegida bajo este título;

b) tenga sólo un propósito o uso comercial limitado, distinto al de evadir una medida tecnológica que controla efectivamente el acceso a una obra protegida bajo este título; o

c) sea comercializado por una persona, o por un tercero actuando en concierto con dicha persona, con conocimiento de su uso para eludir medidas tecnológicas que controlan efectivamente el acceso a una obra protegida en virtud de este título.[52]

Una norma paralela de antitráfico prohíbe las herramientas utilizadas para la elusión de los controles de copia, mientras que el acto de eludir

---

utilizadas por los autores en relación con el ejercicio de sus derechos en virtud del presente Tratado o del Convenio de Berna y que, respecto de sus obras, restrinjan actos que no estén autorizados por los autores concernidos o permitidos por la Ley» (artículo 11 del Tratado de la Organización Mundial de la Propiedad Intelectual sobre Derecho de Autor de 1996). Sobre lo mismo, véase también Litman (2001: 134-45).

48. Digital Millennium Copyright Act. Para más discusión referente a la génesis del DMCA, véase más adelante la sección 3A.

49. 17 USC §§ 1203-1204 establecen las sanciones civiles y penales aplicables.

50. 17 USC § 1201 (a)(3)(A) («eludir una medida tecnológica de protección significa decodificar una obra codificada, descifrar una obra cifrada, o, a través de cualquier método, evitar, burlar, remover, desactivar, o debilitar una medida tecnológica de protección, sin la autorización del titular de derechos de autor…»).

51. 17 USC § 1201 (a)(1)(A).

52. 17 USC § 1201 (a)(2).

dichos controles se enmarca dentro de las prohibiciones de incumplimiento ordinario establecidas en la ley de derechos de autor.[53]

Los prerrequisitos tecnológicos para la protección legal son mínimos «una medida tecnológica controla efectivamente el acceso a una obra, si la medida, en el curso normal de su funcionamiento, requiere la aplicación de información, o un proceso o tratamiento, con la autorización del titular de derechos de autor, para tener acceso a la obra».[54]

Fundamental para el funcionamiento del gancho antielusión, es que «la autorización del titular de los derechos de autor» pueda concederse condicionalmente (Marks y Thurnbull, 1999: 10). Mientras que tempranas críticas argumentaron que el control de acceso debía ser binario —es decir, que una vez que el «acceso» se había autorizado, los usos futuros ya no cabían dentro del ámbito de la DMCA, sino que se sujetarían únicamente a las matrices ordinarias del uso no autorizado—[55] las Cortes no han llegado a un acuerdo. En lugar de determinar que la autorización de acceso había sido entregada directamente a través de la compra de un DVD, la Corte del Segundo Circuito determinó que había sido adquirido sólo un dispositivo de DVD licenciado, y sólo para usos aprobados por el licenciante.[56] Con tal opción, el titular de derechos de autor puede entonces condicionar el acceso a términos que están bastante más allá de los derechos de autor, tal como los requerimientos de codificación por territorio establecidos en las licencias DVD-CCA, limitaciones a aplicaciones o interconexiones y reglas de blindaje.[57] Las leyes antielusión transforman medidas tecnológicas débiles en fuertes controles de uso, limitando las posibilidades tecnológicas.

---

53. 17 USC §§ 501, 1201 (b)(1).

54. 17 USC § 1201 (a)(3)(B).

55. Véase, por ejemplo, la carta de Copyright's Commons a David O. Carson, Consejero General del Copyright Office de Estados Unidos (31 de marzo, 2000), disponible en <http://www.copyright.gov/1201/comments/reply/109selzer_bcis.pdf>, documento que entrega comentarios de respuesta a la reglamentación en materia de leyes antielusión.

56. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 317 n.137 (SDNY 2000), aff'd sub nom. *Universal City Studios, Inc. v. Corley*, 73 F.3d 429, 443 n.13 (2d Cir. 2001).

57. Véase Prepared Testimony of Gwen Hinze, Staff Attorney, Elec. Frontier Found., 15 de mayo de 2003, disponible en <http://w2.eff.org/IP/DMCA/copyrightoffice/20030515_region_DVD.php>.

La adopción de medidas tecnológicas por parte de un titular de derechos de autor, fortifica estas obras contra el acceso realizado sin la autorización del titular; y también protege los dispositivos de reproducción legítimos frente a la competencia o modificaciones no autorizadas.[58] Incluso un esquema débil de codificación contempla la totalidad de los derechos antielusión. Interoperar con una obra codificada sin la autorización del titular de los derechos de autor constituye una violación de la ley, aunque ninguno de los objetivos de la interoperabilidad o de los usos previstos del producto constituya una violación de los derechos de autor en sí mismo.

En resumen, antes de la sección 1201 de la DMCA, alguien que quería construir un reproductor multimedia para una obra que acababa de adquirir, poseía la libertad legal de hacerlo,[59] y quizás también podía mejorar las opciones del reproductor en el camino. Bajo un régimen antielusión, sin embargo, si cualquier medida de protección ha sido aplicada a una obra, los desarrolladores deberán pedir permiso para construir legalmente un reproductor o modificar uno existente.[60] La sección 1201 (f), que permite algunos actos de elusión para ingeniería inversa[61] no ha servido como escudo para el desarrollo independiente de la tecnología de medios digitales.[62]

Como se describió anteriormente, la protección de la DMCA sobre los DVD ayuda a explicar el retraso en las opciones de reproducción de video, en comparación con sus homólogos reproductores de música. Otros casos judiciales ilustran la libertad de acción pre-DMCA que el derecho de autor dio a la ingeniería inversa y la investigación. Por ejemplo, cuando Sony trató de utilizar los derechos de autor para monopolizar su plata-

58. 17 USC §§ 1201 (a)(1), 1201 (b).

59. Esto asume que los únicos derechos IP existentes son restricciones de derechos de autor. Las patentes, tal como aquellas alegadas sobre codificaciones MP3, pueden servir como un impedimento separado.

60. 17 USC § 1201.

61. 17 USC § 1201 (f).

62. Véase *Universal v. Reimerdes*, 82 F. Supp. 2d 211, 218 (S.D.N.Y. 2000): «La historia legislativa ha hecho abundantemente claro que la sección 1201 (f) permite sólo la ingeniería reversa de programas computacionales protegidos por derechos de autor, y no permite la elusión de sistemas que controlan el acceso a otras obras protegidas, tales como las películas». Véase también *Davidson & Assocs. v. Jung*, 422 F.3d 630, 642 (8th Cir. 2005).

forma PlayStation, para los que fabricaba consolas y juegos licenciados, la Corte del Noveno Circuito rechazó las alegaciones de Sony en contra de la interoperabilidad del Virtual Game Station.

> El tribunal de distrito declaró que «en la medida en que tal sustitución [del PlayStation de Sony por el Virtual Game Station de Connectix] se produzca, Sony perderá ventas de la consola y las utilidades». Reconocemos que esto puede ser así. Sin embargo, debido a que el Virtual Game Station es transformador, y no se limita a suplantar a la consola PlayStation, es un legítimo competidor en el mercado de las plataformas en las que Sony y los juegos licenciados por Sony se pueden reproducir. Por esta razón, una pérdida económica por parte de Sony, como resultado de esta competencia, no obliga a una constatación de inexistencia de uso justo. Sony comprensiblemente busca el control sobre el mercado de dispositivos que reproducen los juegos que Sony produce o licencia. La ley de derechos de autor, sin embargo, no confiere tal monopolio.[63]

La Corte del Noveno Circuito rechazó asimismo el intento de Sega de usar los derechos de autor para bloquear el mercado, respecto de juegos ejecutados a través de sus consolas propietarias: «Un intento de monopolizar el mercado al hacer imposible para los demás competir, va en contra de los fines estatutarios de la promoción de la expresión creativa, y no puede constituir una base sólida equitativa para oponerse a la invocación de la doctrina del *fair use*.[64]

Las normas antielusión ofrecen a Sony y Sega el poder que los derechos de autor en sí no otorgaban. Como lo señalan Dean Marks y Bruce Turnbull, las leyes antielusión de medidas tecnológicas de protección sirven como el elemento aglutinador entre los controles tecnológicos y los múltiples acuerdos de licenciamiento que regulan el uso y las limitaciones de los medios digitales sujetos a dichos controles. Sólo aquellos que se comprometen a obedecer varias condiciones no asociadas a derechos de autor pueden obtener una autorización (Marks y Turnbull, 1999: 10-5).

Aunque nada en el texto de la ley se refiere específicamente a los modos de desarrollo, eso no quiere decir que la ley no tenga influencia en ellos. Según la interpretación de la mayoría, la antielusión prohíbe las

63. Ídem.

64. *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1523–24 (9th Cir. 1992).

modificaciones de usuario de reproductores (ya sea *hardware* o *software*) utilizados para reproducir obras protegidas que han tenido alguna protección técnica.[65] Manipular un dispositivo constituiría aparentemente la anulación de la «autorización» que implica la licencia del reproductor. Más generalmente, la prohibición del desarrollo abierto proviene de una característica común de los acuerdos de licencia a través del cual se crean plataformas DRM: «las reglas de blindaje» y su implementación.

C) LICENCIAMIENTO PARA EL BLINDAJE DE DERECHOS: CÓMO LOS PROVEEDORES DE CONTENIDOS INFLUYEN EN EL MERCADO DEL HARDWARE

Si uno sólo puede acceder a obras protegidas por DRM con la «autorización del titular de derechos de autor»,[66] entonces las licencias bajo las cuales se concede dicha autorización se convierten en la ley de esas obras. Dichas licencias imponen condiciones al fabricante de dispositivos de reproducción y, a través de ellas, al usuario final de las obras protegidas.

Mientras que sus términos de uso pueden variar, los sistemas de licencias DRM siguen un patrón estructural común. Estos exigen la protección de los contenidos a través de «reglas de uso» que serán traspasadas al usuario final, y la protección al sistema DRM en sí mismo, con reglas internas de «cumplimiento» y «blindaje».[67] Si tú impones medidas tecnológicas de protección es porque desconfías de los usuarios y quieres detenerlos, a través de la tecnología, de hacer cosas que de otro modo serían posibles. A medida que tu comprensión de las capacidades e intereses

65. Véase, por ejemplo, *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001); *RealNetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913 (N.D. Cal. 2009); *321 Studios v MGM Studios, Inc.*, 307 F. Supp. 2d 1085 (N.D. Cal. 2004).

66. 17 USC § 1201 (a)(3)(A) (2006).

67. Las reglas de «conformidad» regulan la adhesión a los términos de uso de los dispositivos del licenciatario, mientras que las de «blindaje» requieren esfuerzos para impedir modificaciones. Véase Advanced Access Content System Adopter Agreement F-1 (9 de junio de 2009), disponible en <http://www.aacsla.com/license/AACS_Adopter_Agrmt_090619.pdf>; DVD-CCA CSS Procedural Specification ¶6.2.6, disponible en <http://cyber.law.harvard.edu/seminar/internet-client/readings/week2/02-08CSS.pdf>; Microsoft Corp., Compliance and Robustness Rules for Windows DRM, disponible en <http://wmlicense.smdisp.net/wmDRMcompliance/>.

de los usuarios mejora, tratarás de rellenar las grietas en la protección tecnológica que has creado. En la lógica de los diseñadores de DRM, esta condición tiene sentido: si la antielusión consiste en detener la copia, el sistema anticopia debe ser tan resistente al *hackeo* como el propio cifrado. Después de todo, una cadena sólo es tan fuerte como su eslabón más débil, y un «lomo de toro» no hará que el tráfico sea más lento, si puede ser evitado circulando a toda velocidad. Y así, la sección 1201 implica el endurecimiento de la tecnología de reproducción, incluso si la ley no lo exige directamente.

En una revisión de los acuerdos de licencia de varios sistemas de protección de contenidos es posible encontrar reglas de blindaje casi idénticas en todos ellos.[68] Las implementaciones de *hardware* o *software* de reproducción multimedia o de transporte deben estar diseñados para «efectivamente frustrar»[69] o «resistir los intentos de modificar dichos productos para anular»[70] las protecciones a los contenidos: ellos no han de incluir ningún componente modificable por el usuario tales como interruptores, botones, puentes o rastros que puedan ser cortados; ellos no deben ser accesibles a un depurador; y deben ser capaces de «mantener secretos». En resumen, para ser autorizados a acceder a una obra, una implementación debe ser endurecida en contra de retoques y de la exploración por parte del usuario (Gillespie, 2007: 225-9).

---

68. Ver fuentes citadas en la nota anterior; véase además Gillespie (2006: 651-69).

69. Advanced Access Content System Interim Content Participant Agreement, Exhibit C, part 2, § 3.2, disponible en <http://www.aacsla.com/license/AACS_Interim_Content_Participant_Agrmt_090605.pdf>: «Los productos licenciados serán fabricados de una manera claramente diseñada para frustrar efectivamente los intentos de modificar dichos productos licenciados o el uso de dichos productos licenciados para derrotar los requerimientos de protección de contenido». Incluso el DREAM, de Sun, la especificación supuestamente abierta de DRM, requiere el blindaje de parte de sus clientes: «Seguridad del cliente: la implementación de un cliente blindado que será requerida para una solución viable. La implementación de un cliente blindado dependerá del *hardware* y del SOFTWARE disponible» (DREAM-CAS Client Specification Version 1.0 Rev A, Technical Specification, § 1.1, 2007, en poder del autor).

70. Microsoft, Microsoft Windows Media 10 SDK Robustness Rules, disponible en <http://wmlicense.smdisp.net/wmDRMcompliance/> (hacer clic en «Robustness Rules for WMDRM10 Devices»): «Los productos licenciados son despachados… deben ser diseñados y fabricados para resistir los intentos de modificar dichos productos como para vencer las funciones de la implementación de Microsoft».

Las reglas de blindaje son reglas de diseño.[71] Dan forma a la arquitectura de los sistemas que los licenciatarios tienen permitido poner a disposición de los usuarios finales. Como Tarleton Gillespie (2007: 225-9) lo describe, estas reglas reestructuran la relación entre el usuario no sólo con los medios digitales, sino que también con la propia tecnología. Ellos establecen al usuario como un consumidor pasivo, en lugar de ser un participante activo en la creación tanto de cultura como de tecnología. Como señala Lawrence Lessig (2008: 28), estas reglas nos llevarán de una cultura de «leer-escribir», a una cultura de «sólo leer».

El requisito de autorización establecido en la sección 1201 importa los términos impuestos por licencias. Cuando todas las licencias para sistemas DRM de importancia requieren el blindaje como una condición, éste se convierte en el equivalente de un requerimiento legal. El derecho privado se transforma en público. Sin embargo, académicos como Lessig (2000: 95-8, 223-5) han señalado que este derecho privado puede ser igualmente restrictivo y más opaco por su falta de dirección.[72]

De hecho, el mecanismo de blindaje podría haber sido escrito en la ley. En el reglamento de Broadcast Flag las regulaciones adoptadas por la Federal Communication Commission (FCC) para la protección de las transmisiones de televisión digital, establecieron el blindaje como un mandato.[73] Así podría ser impugnada en los tribunales. La American

71. Baldwin y Clark (2000: 80) describen las reglas de diseño como un set de limitaciones a la fabricación.

72. Gillespie (2007: 219) describe «protecciones de derecho de autor impuestas a través de medidas técnicas que dependen de contenido encriptado, tecnologías que responden a un set de reglas aplicadas a dicho contenido, y leyes que vuelven ilegal la alteración o la creación de alternativas a esas tecnologías».

73. Véase Robustness Requirements for Covered Demodulator Products, 47 C.F.R. § 73.9007 (2005): «Los requisitos de protección de contenidos establecidos serán implementados a través de métodos razonables para que no puedan ser vulnerados o eludidos por un usuario normal a través de herramientas o equipos disponibles al público general»). Incluso la frase «generalmente disponibles» se encuentra definida en el Reglamento: «Herramientas o equipos generalmente disponibles significará cualquier herramienta o equipo que esté ampliamente disponible a un precio razonable, incluyendo, pero no limitado a, destornilladores, puentes, clips y soldadores. Herramientas o equipos generalmente disponibles también significará herramientas especializadas de electrónica o herramientas de *software* que están ampliamente disponibles a un precio razonable, excepto los dispositivos o tecnologías que se han diseñado y puesto a disposición para el

Library Association y otros grupos de interés público lo hicieron y argumentaron con éxito que la Broadcast Flag Rule excedía la autoridad de la FCC.[74] Las impugnaciones a DRM respaldados por la DMCA debieran obtener la misma posibilidad.

D) EL SOFTWARE DE CÓDIGO ABIERTO ES INCOMPATIBLE CON LOS REQUERIMIENTOS DE BLINDAJE

En agudo contraste con el entorno limitado de la DMCA, el *software* libre y de código abierto promueve la modificación por parte de los usuarios finales.[75] Al revelar sus detalles y conceder a los usuarios permisos para modificar (en términos de derechos de autor, para crear obras derivadas), el código libre y abierto ofrece un diagrama esquemático (más o menos bien marcado) de los componentes mecánicos. Incluso los principiantes pueden aprender ajustando algunas líneas y volviendo a compilar para ver el efecto de la misma manera en que uno puede aprender a diseñar una página web viendo la fuente de una página y aprendiendo a través de imitación y adaptación. Los expertos pueden perfeccionar y adaptar el *software* a sus necesidades, corrigiendo errores y agregando funciones. Las comunidades de usuarios reunidas en torno al *software* libre y de código abierto han desarrollado complejas aplicaciones, sistemas operativos y entornos completos (Lakhani y von Hippel, 2003: 924). El *software* libre y de código abierto alimenta mucha de la estructura existente en Internet. Más de la mitad de los servidores de Internet ejecutan

---

propósito específico de evadir o eludir las medidas tecnologías de protección utilizadas para cumplir con los requisitos establecidos en esta subparte. Tales herramientas electrónicas especializadas o herramientas de *software* incluyen, pero no se limita a, los lectores y escritores EEPROM, depuradores o decompiladores».

74. Véase *Am. Library Ass'n v. Fed. Commc'n Comm'n*, 401 F.3d 489 (D.C. Cir. 2005).

75. *Software* libre tiende a ser la etiqueta elegida por aquellos que, siguiendo la Free Software Foundation, dan una dimensión explícitamente política al intercambio de código fuente y la libertad de modificar el *software*; «código abierto» se usa a menudo para hacer hincapié en los beneficios económicos y de eficiencia asociados a la revelación del código fuente. Ya sea por temperamento filosófico o económico, su modo de desarrollo tiene el efecto de hacer las funciones del *software* mucho más accesibles para la innovación de usuario.

el código abierto para web Apache,[76] muchas veces a través del sistema operativo libre GNU/Linux, y muchos hoy utilizan navegadores de código abierto como Mozilla Firefox o Google Chrome. Incluso alguien que nunca lee una línea de código fuente se beneficia de esta apertura: de la competencia de programadores independientes a la disposición de los servicios del *software*, de la presión que pone sobre vendedores de *software* propietario y de la facilidad de desarrollo de aplicaciones complementarias.

El desarrollo de *software* de código libre y abierto depende críticamente de la apertura. Aunque los términos «*software* libre» y «código abierto» reflejan enfoques y motivaciones diferentes de sus participantes (Seltzer, 2005b: 149; Benkler, 2001: 84), en el fondo ambos se refieren a *software* cuyo código fuente (la versión legible de las instrucciones de equipo) se pone a disposición de los usuarios de programas para su uso y modificación.[77]

La Free Software Foundation expresa los principios básicos del *software* libre como «cuatro libertades esenciales»:

1. La libertad de ejecutar el programa, con cualquier propósito (libertad 0).
2. La libertad de estudiar cómo funciona el programa, y modificarlo para que haga lo que el usuario quiera (libertad 1). El acceso al código fuente es una condición previa para esto.
3. La libertad de distribuir copias, para ayudar a tu vecino (libertad 2).
4. La libertad de mejorar el programa y publicar sus mejoras (y versiones modificadas en general) al público, de manera que beneficie toda la comunidad (libertad 3). El acceso al código fuente es una precondición para esto.[78]

76. Véase Netcraft, Web Server Survey Archives, disponible en <http://news.netcraft.com/archives/web_server_survey.html>.

77. Véase Free Software Foundation, The Free Software Definition, disponible en <http://www.gnu.org/philosophy/free-sw.html>; Open Source Initiative, The Open Source Definition, disponible en <http://www.opensource.org/docs/definition.php>.

78. Véase el documento de Free Software Foundation en la nota anterior.

Estos cuatro componentes son necesarios para dar a los usuarios plena autonomía en su entorno de *software*; para utilizar y aprender del programa y modificarlo para adaptarlo a sus necesidades. Protegen del *lock-in* de un vendedor que no coopera o de un sistema descontinuado, y aseguran que los usuarios podrán volver a utilizar sus aportes individuales al programa. Por otra parte, la Free Software Foundation afirma que «La libertad 1 [la libertad de modificar] debe ser práctica, y no sólo teórica; es decir, no debe existir una "tivoización"».[79] La versión 3 de la licencia GPL, publicada en el año 2007,[80] requiere que los licenciatarios provean de un programa de instalación suficiente como para permitir el uso del código modificado de la misma manera que la del programa instalado originalmente.[81] «Mirar pero no tocar» no es libertad.

La Licencia Pública General GNU (GPL) mantiene esas libertades a tra-

79. El mismo documento de la Free Software Foundation se refiriere al grabador digital de video TiVo, el cual ejecuta un sistema operativo GNU/Linux y pone a disposición el código fuente, pero sin permitir al usuario instalar modificaciones al dispositivo TiVo.

80. Los desarrolladores de código pueden elegir qué licencia aplicar, sujeta a los requisitos que se heredan del código licenciado que desean utilizar. El kernel de Linux sigue estando bajo la licencia GPLv2, mientras que las nuevas versiones de las utilidades GNU de la FSF son liberadas bajo la licencia GPLv3. Aquellos que deseen distribuir las nuevas utilidades GNU, por lo tanto, deben poner a disposición del públicos tanto el código fuente como la información de instalación.

81. Free Software Foundation, GNU General Public License, Version 3 § 6 (2007), disponible en <http://www.gnu.org/licenses/gpl.txt>. El GPL establece: «En el caso de que usted transmita el código objeto de una obra conforme a esta sección en un producto de usuario, junto con un producto de usuario o específicamente para su uso en un producto de usuario, y la transmisión se produzca como parte de una transacción mediante la cual los derechos de posesión y uso del producto de usuario se transfieran al destinatario por un plazo limitado o ilimitado (independientemente de las particularidades de la transacción), la Fuente Correspondiente transmitida conforme a esta sección deberá ir acompañada de la información de instalación. Por "información de instalación" de un producto de usuario se entiende cualquier método, procedimiento, clave de autorización u otro tipo de información requerida para instalar y ejecutar versiones modificadas de una obra amparada en dicho producto de usuario a partir de una versión modificada de su Fuente Correspondiente. La información debe ser suficiente para garantizar que el funcionamiento continuo del código objeto modificado no se vea afectado o imposibilitado por el solo hecho de haberse realizado la modificación».

vés de una disposición de *copyleft*: cualquiera es libre de volver a utilizar código con licencia GPL, siempre y cuando quienes publiquen sus obras derivadas lo hagan en los mismos términos, esto es, bajo la GPL.[82]

La Open Source Initiative (OSI) está más explícitamente orientada hacia las «ventajas económicas y estratégicas» que derivarían de la apertura.[83] Se necesita apertura como fundamento de la diversidad y la innovación productiva. «Requerimos acceso a un código fuente "no-ofuscado" porque no se pueden desarrollar programas sin modificarlos. Dado que nuestro propósito es hacer que el desarrollo sea fácil, requerimos que la modificación también lo sea».[84] La OSI tiene como objetivo aprovechar a la comunidad de desarrolladores de código abierto: «con el fin de obtener el máximo beneficio del proceso, la máxima diversidad de personas y grupos debieran tener el mismo derecho a contribuir a las fuentes abiertas. Por lo tanto, prohibimos que cualquier licencia de código abierto deje a alguien fuera del proceso».[85] La OSI identifica un número de licencias que cumplen la regla de código abierto.[86] Al igual que la GPL, que se encuentra dentro de ellas, todas las distribuciones licenciadas de código abierto incluyen el código fuente y la posibilidad de modificar el *software*.[87]

---

82. [5] Usted puede transmitir una obra basada en el Programa, o las modificaciones para producirlo a partir del Programa, en forma de código fuente… siempre y cuando también cumpla con todas las condiciones que se incluyen a continuación:

a) La obra debe conservar avisos llamativos que establezcan que usted la ha modificado e incluyan la fecha correspondiente.

b) La obra debe conservar avisos llamativos que establezcan que la misma se realiza conforme a esta licencia…

c) Usted debe otorgar una licencia por la obra completa, en forma íntegra, conforme a esta Licencia, a cualquier tercero que adquiera una copia.

[6] Usted puede transmitir una obra amparada en código objeto conforme a los términos de las secciones 4 y 5, siempre y cuando también transmita la Fuente Correspondiente legible por máquina conforme a los términos de esta Licencia (§§ 5, 6).

83. Open Source Initiative, About the Open Source Initiative, disponible en <http://www.opensource.org/about>.

84. Véase el mismo documento de Open Source Initiative referido en la nota 77.

85. Ídem

86. Véase Open Source Initiative, Open Source Licenses by Category, disponible en <http://www.opensource.org/licenses/category>.

87. La definición de *código abierto* no requiere una provisión estilo *copyleft* que orde-

Sería imposible construir un reproductor basado en DRM que estuviese en regla con las definiciones tanto del *software* libre, como con la definición de código abierto. Los DRM son incompatibles con la letra y el espíritu del código abierto y de las licencias de *software* libre.[88] Las medidas antielusión prohíben a los usuarios explorar las posibilidades de sus medios digitales, e impiden a los desarrolladores ofrecer reproductores que puedan ser modificados por los usuarios.

Internet multiplica las oportunidades de desarrollo de código abierto, conectando las abundantes fuerzas de programas computacionales de código abierto, una masa crítica de posibles contribuyentes interconectados y comunicaciones más baratas entre ellos, en una plataforma neutral. Como presidente de la Federal Communication Commission, Julius Genachowski, preguntó en septiembre de 2009, en un discurso que presentaba la discusión de la Comisión sobre código abierto: «¿Por qué Internet ha demostrado ser un poderoso motor de creatividad, innovación y crecimiento económico? Una gran parte de la respuesta se remonta a una decisión fundamental de los arquitectos originales de Internet: hacer de Internet un sistema abierto».[89]

---

ne la apertura de redistribuidores, aunque es compatible con el requerimiento de *copyleft* de la GPL. Véase fuentes citada en nota 77.

88. Véase más adelante la sección 5 de este artículo. En la revisión de 2007 de la GPL, la FSF añadió una cláusula explícita que prohíbe el uso de la GPL en medidas tecnológicas de protección (véase Licencia Pública General GNU, en nota 97, § 3: «Ninguna obra amparada se considerará parte de una medida tecnológica efectiva conforme a cualquier ley aplicable que cumpla las obligaciones del artículo 11 del Tratado de la Organización Mundial de la Propiedad Intelectual sobre Derecho de Autor de 1996 o a leyes similares que prohíban o restrinjan la evasión de dichas medidas»). Esta prohibición específica es distinta de la incompatibilidad general de los DRM con el modo de desarrollo de código libre y abierto.

89. «Julius Genachowski, Chairman, FCC, Remarks at The Brookings Institution: Preserving a Free and Open Internet: A Platform for Innovation, Opportunity, and Prosperity» (21 septiembre de 2009), disponible en <http://openinternet.gov/readspeech.html>. Genachowski dijo: «Los creadores de la Internet no querían que la arquitectura de la red —o cualquier otra entidad— eligiera a ganadores y perdedores. Porque podría elegir a los equivocados. En cambio, la arquitectura abierta de Internet impulsa la toma de decisiones y la inteligencia al borde de la red, a los usuarios finales, a la nube, a las empresas de todos los tamaños y en todos los sectores de la economía, a los creadores y oradores en todo el país y en todo el mundo. En palabras de Tim

EL DEBATE ACADÉMICO

A) LOS DEFENSORES DE LA ANTIELUSIÓN

Los intentos de «protección de copia» de soportes han existido por mucho tiempo, pero la llegada del almacenamiento digital aceleró que se movieran desde la tecnología a la ley. Los medios digitales, señalaron los titulares de derechos de autor, permiten a los usuarios hacer copias perfectas, mientras que la alta velocidad de las redes de comunicaciones permite compartir fácilmente esas copias.[90] Las industrias de propiedad intelectual proclamaron un «dilema digital»: no habrán autos que transiten la autopista de la información a menos que la ley de derechos de autor garantice protección para sus contenidos protegidos.[91] Las industrias buscaron esta protección tanto en la tecnología como en la ley.

Las industrias editoriales establecieron un silogismo: el «contenido» fue clave para el crecimiento de la naciente Internet —entonces conocida como la Infraestructura de la Información Nacional (NII, por su sigla en inglés)—; la producción de contenidos podría suspenderse si su protección no se aseguraba; por lo tanto, la producción de contenido debe ser una parte fundamental de Internet.[92] El grupo de trabajo NII

Berners-Lee, Internet es un "lienzo en blanco" que permite a cualquier persona aportar e innovar sin permiso».

90. Véase «NII Copyright Protection Act of 1995: Hearing on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary» (1996) (declaración de Barbara A. Munder, Asociación de la Industria de la Información). Véase también «NII Copyright Protection Act of 1995: Joint Hearing on H.R. 2441 and S. 1284 Before the Subcomm. on Courts and Intellectual Property of the House Judiciary Comm. and the Senate Judiciary Comm.» (1995).

91. Information Infrastructure Taskforce, Intellectual Property and the National Information Infrastructure: the Report of the Working Group on Intellectual Property Rights, págs. 10-17 (1995), disponible en <http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.txt>, de aquí en adelante Reporte NII.

92. «El potencial de la NII no se hará realidad si los productos de la educación, información y entretenimiento protegidos por las leyes de propiedad intelectual no están protegidos eficazmente cuando se difundan a través de la NII. Creadores y otros titulares de derechos de propiedad intelectual no estarán dispuestos a poner sus intereses en riesgo si los sistemas adecuados, tanto en los Estados Unidos como a nivel internacional, no se implementan para permitirles establecer y hacer valer los términos y las condiciones bajo

no sobreestimó a la tecnología: «es evidente que la tecnología se puede utilizar para derrotar cualquier tipo de protección que la tecnología pueda ofrecer»,[93] concluyendo que la ley debía ser añadida a la mezcla, en apoyo de restricciones basadas en medidas tecnológicas. El White Paper del NII propuso un híbrido: prohibición legal de elusión de medidas tecnológicas de protección.

> El Grupo de Trabajo considera que la protección jurídica por sí sola no será suficiente para proveer incentivos a los autores para crear y difundir obras al público. Del mismo modo, la protección tecnológica probablemente no será eficaz a menos que la ley también proporcione cierta protección para los procesos tecnológicos y los sistemas utilizados para prevenir o restringir el uso no autorizado de obras protegidas.
>
> El Grupo de Trabajo considera que la prohibición de dispositivos, productos, componentes y servicios que vulneren los métodos tecnológicos para prevenir el uso no autorizado es de interés público y promueve la finalidad constitucional de las leyes de derechos de autor. Los consumidores de obras protegidas pagan por los actos de los infractores; los propietarios de derechos de autor han sugerido que el precio de las copias legítimas de obras protegidas pueden ser mayores debido a las pérdidas por infracción sufridas por los titulares de derechos de autor. El público también tendrá acceso a más obras protegidas por derecho de autor a través de la NII, si no son vulnerables al quebrantamiento de los sistemas de protección.
>
> Por lo tanto, el Grupo de Trabajo recomienda la modificación de la

---

las cuales su obras se ponen a disposición en el entorno NII. Asimismo, el público no va a usar los servicios disponibles en la NII ni generará el mercado necesario para su éxito, a menos que una amplia variedad de obras estén disponibles bajo condiciones equitativas y razonables, y la integridad de las obras esté asegurada. Todas las computadoras, teléfonos, máquinas de fax, escáneres, cámaras, teclados, televisores, monitores, impresoras, interruptores, *routers*, cables, redes y satélites en el mundo no van a crear un NII exitoso, si no hay contenido. Lo que impulsará la NII es el movimiento de los contenidos a través de ella [...] Que el grupo de trabajo NII no haya podido prever o explicar Wikipedia, cuyos autores y editores contribuyen sabiendo que sus obras son libremente compartidas, incluso cuando otros puedan obtener ganancias a través de ellas, o las licencias Creative Commons que muchos utilizan para compartir sus obras, es tal vez el primer indicio de que el suyo no era el único camino para el progreso de la ciencia (Reporte NII, págs. 10-11).

93. Reporte NII, pág. 136.

> Ley de Propiedad Intelectual a fin de incluir un nuevo capítulo 12, que incluya una disposición que prohíba la importación, fabricación o distribución de cualquier dispositivo, producto o componente incorporado en un dispositivo o producto, o la prestación de cualquier servicio, cuyo propósito principal o efecto es evitar, eliminar, desactivar o eludir de cualquier manera, sin autorización del titular de derechos de autor o de la ley, cualquier proceso, tratamiento, mecanismo o sistema que impida o inhiba la violación de cualquier de los derechos exclusivos en virtud del artículo 106. La disposición no elimina el riesgo de que los sistemas de protección sean vulnerados, pero lo reducirá.[94]

Desde el White Paper, a través del «lavado de políticas»[95] en la elaboración de los tratados OMPI, el capítulo 12 se añadió a la Ley de Propiedad Intelectual en el año 1998.[96] La sección 1201 de la DMCA prohíbe la «elusión» de medidas tecnológicas de control de acceso y prohíbe el tráfico de herramientas para la elusión de controles de acceso o copia.[97] Se da fuerza legal a las barreras tecnológicas, sin perjuicio de lo fuertes o débiles que sean, y prohíbe la distribución de herramientas de elusión, aun cuando su objetivo no sea la infracción de derechos de autor.[98]

La antielusión ha sido controversial desde sus inicios. Los primeros críticos pusieron en duda su constitucionalidad[99] y la culparon de extender las prerrogativas de los titulares de derechos de autor a expensas del público;[100] mientras que sus defensores argumentaron que era necesaria para mantener la viabilidad de los derechos tradicionales de autor

94. Reporte NII, págs. 139-40.

95. El lavado de la política toma un argumento difícil de aceptar de la política en la esfera doméstica y lo «lava» a través de una organización de tratados internacionales, en este caso, la OMPI, antes de traerlo de vuelta a la legislatura nacional como una «obligación de tratado internacional». Véase Ian Hosein, ponencia presentada en el International Studies Association, Montreal, Quebec, Canadá: «International Relations Theories and the Regulation of International Dataflows: Policy Laundering and other International Policy Dynamics» (17 de marzo de 2004).

96. Ley de 1998 que implementa el Tratado de la Organización Mundial de la Propiedad Intelectual sobre Interpretación o Ejecución y Fonogramas de 1996.

97. Digital Millennium Copyright Act, 17 USC § 1201 (2006).

98. Digital Millennium Copyright Act, 17 USC § 1201 (2006); véase también la sección II.B.

99. Netanel (2001: 78-80). Véase también más adelante la sección III.B.

100. Véase más adelante la sección 3B.

en los nuevos mercados.[101] Por lo general, estos argumentos han tenido lugar *dentro de los derechos de autor*, compartiendo el enfoque de los derechos de autor en la producción, uso y (tal vez) la comercialización de las expresiones creativas, lo que explica por qué tienden a obviar los efectos de la antielusión en el desarrollo tecnológico fuera de la esfera de los derechos de autor.

Tecnólogos y académicos que apoyaban las normas antielusión señalaron que sustentarían los derechos de autor y una ecología de nuevos modelos de negocios alrededor de las obras protegidas por derechos de autor (Stefik, 1997: 78-81). Mark Stefik describió por primera vez un *sistema confiable* para envolver a las obras protegidas y controlar su transferencia:

> El término *sistema confiable* se refiere a equipos en los que se puede confiar para hacer ciertas cosas. Por ejemplo, supongamos que un creador o editor prohíbe todo tipo de copia de una obra digital en particular. Un sistema confiable en este contexto podría segura e infaliblemente llevar a cabo esta estipulación; ninguna forma de coacción provocaría coerción suficiente para copiar la obra (1996: 257).

Del mismo modo, Jane Ginsburg (2003: 115) reconoce que la antielusión proporciona nuevos derechos, pero argumenta que el cambio tecnológico de la posesión de ejemplares físicos a «experimentar obras» requiere de prerrogativas más extensas. Para Ginsburg, la ley antielusión proviene del espíritu de la cláusula de Propiedad Intelectual de la Constitución norteamericana,[102] como una respuesta natural a los cambios en la tecnología y en los mercados que apoya, sugiriendo que «en el entorno digital, el 'derecho exclusivo' que la Constitución autoriza al Congreso a garantizar a los autores no sólo es un derecho de copia, sino también un derecho de acceso» (2003: 115). Mientras los titulares de derechos de autor perdían el control en la diseminación de sus obras, ellos deberían obtener un tipo diferente de control.

101. Véase más adelante la sección 3B.

102. Constitución de los Estados Unidos, art. 1.º, sección 8.ª, cláusula 8.ª

B) LOS CRÍTICOS DE LA ANTIELUSIÓN

1. *La antielusión impide el* fair use *por parte de usuarios finales*

Gran parte de las investigaciones previas sobre antielusión se han centrado en las restricciones directas que los DRM imponen en el uso de los medios digitales y en las limitaciones que impone al *fair use* (Litman, 2001; Cohen, 1998b: 462; Samuelson, 1999: 519). Cuando los medios están disponibles sólo a través de aplicaciones que respetan los DRM, los usuarios se ven obligados a aceptar las limitaciones de uso, incluso si esas limitaciones son más restrictivas que las de los derechos de autor. El usuario que compra una canción atada a la computadora a través de la cual realizó la descarga, nunca podrá revender esa adquisición.[103] A un crítico de cine que desea mostrar un clip de DVD no le será fácil tomar un extracto con este propósito.[104]

Para algunos, esta desventaja es el costo del acceso a copias digitales. Con permisos más especializados vienen un conjunto de costos hechos a la medida de estos permisos —discriminación de precios que ofrece a los usuarios un acceso a más copias y a menor costo (Bell, 1998: 588; Picker, 2003: 296). Para otros, este intercambio es demasiado oneroso, y menoscaba los importantes beneficios públicos del *fair use*: privacidad en la lectura (Cohen, 1995: 1007-10), la libertad de pedir permiso por adelantado y la libertad de criticar (Benkler, 1999: 410; Netanel, 2001: 26). Las externalidades positivas de los medios digitales utilizados bajo el amparo de la doctrina del *fair use*, por ejemplo, significan que la ley debería estar dispuesta a subsidiarla en vez de restringirla. Restringir el *fair use* disminuye los bienes comunes sobre los cuales depende la creatividad futura (Lessig, 2005: 97-9; Aufterheide y Jaszi, 2004).

Los críticos académicos atacaron la antielusión primero desde dentro

---

103. «El aumento del derecho de autor a través de controles de acceso legalmente sancionados podría anular completamente la doctrina del agotamiento de los derechos de autor» (Litman, 2001: 83). Véase también 17 USC § 109 (2006) sobre la doctrina del agotamiento de derechos.

104. Ver las peticiones de exenciones en la trienal de políticas de la Copyright Office, bajo el 17 USC § 1201(a)(1)(C), U.S. Copyright Office, Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works, disponible en <http://www.copyright.gov/1201/>.

del derecho de autor: las protecciones tecnológicas interfieren con las limitaciones de *fair use* incorporadas en la ley de derechos de autor.[105] Mientras que algunos usos no autorizados de obras protegidas no infringen los derechos de autor por disposición legal, los DRM no tienen forma de reconocer la diferencia entre una reproducción justa para efectos de enseñanza, comentario o parodia, y una reproducción que efectivamente infrinja los derechos de autor. El estatuto prohíbe la elusión de los DRM incluso cuando dicho bloqueo impide el acceso para usos que no vulneran las prerrogativas autorales.[106]

Pamela Samuelson, Jessica Litman, Julie Cohen y Yochai Benkler han puesto de relieve la contradicción existente entre la aplicación tecnológica de absolutos y los matices de «caso a caso» y «uso por uso» que las excepciones contenidas en el *fair use* entregan respecto de los derechos de autor (Benkler, 1999; Cohen, 1995, 1998a; Litman, 2001; Samuelson, 1999). Algunos, incluido la autora de este artículo, han argumentado que esta incompatibilidad hace que la DMCA sea inconstitucional, ya que al convertir a los derechos de autor en absolutos, *paracopyright* en términos de David Nimmer, se violaría la Primera Enmienda.[107]

Algunos de estos argumentos se han planteado en recursos de inconstitucionalidad contra la DMCA,[108] pero como muchas de estas alegaciones parecen defender un comportamiento que también podría permitir la reproducción en masa, las afirmaciones de los daños al *fair use* cayeron en oídos sordos. Por ejemplo, la Corte de Apelaciones del Segundo Circuito dijo a los demandados en *Universal v. Corley* que quienes quisieran

105. El derecho de autor no prohíbe todas las reproducciones, sino sólo aquellas que interfieren con los derechos del titular de derechos. Las reproducciones «para propósitos tales como crítica, comentario de noticias, [y] la enseñanza» se permiten como fair use (17 USC § 107 [2006]).

106. «Existen muchas más razones legítimas para eludir un sistema de protección tecnológica que aquellas expresamente reconocidas por la DMCA» (Samuelson, 1999: 524).

107. Brief for Electronic Frontier Foundation as Amici Curiae Supporting Plaintiff's Opposition to Defendant's Motion for Partial Summary Judgment at *321 Studios v. Metro Goldwyn Mayer Studios Inc.*, 307 F.Supp.2d 1085 (N.D. Cal. 2004) (No. C 02-1955 SI); David Nimmer, 3 Nimmer On Copyright § 12A.15[C] (1999 supp.); Netanel (2001: 78).

108. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001); *321 Studios*, 307 F. Supp. 2d 1085.

hacer usos justos de un DVD podrían apuntar cámaras de video a sus pantallas de televisión.[109]

Una segunda camada de críticos inspirados en el *fair use* se han preguntado si la tecnología puede ayudar a resolver los problemas que la tecnología ha creado: ¿puede el *fair use* acomodarse dentro de sistemas DRM híbridos? Mientras no podamos poner a un juez dentro de un chip, algunos han propuesto que podemos acercarnos al régimen anterior a la DMCA (y bien público) más eficazmente mediante la vinculación de los incumplimientos más frecuentes con sistemas construidos para invocar a una autoridad externa o un tercero de confianza. Julie Cohen y Dan Burk identifican las deficiencias de la ley en el ámbito cultural, pero se preguntan si esto es una mera función de implementación (2001: 50-1). ¿Podría una infraestructura de *fair use* para sistemas de gestión de derechos, donde un tercero de confianza adjudicara las solicitudes de acceso para estos fines, capturar los matices y la espontaneidad que requieren el *fair use*? Burk y Cohen hacen un esfuerzo por diseñar una «segunda mejor solución diseñada para sacar lo mejor de una mala situación», pero, en definitiva, rechazan incluso su versión de los DRM modificados (2001: 80). Tim Armstrong (2006: 99-108) propone un sistema que establece valores por defecto con respecto al uso, manteniendo un registro de auditoría de los casos de *fair use*. Deirdre Mulligan y John Erickson describen el posible uso de lenguajes de expresión de derechos, en vez de restricciones automatizadas (2004: 994).

La mayoría de los estudios asociados al *«fair use»* se reduce en la mayoría de los casos a un análisis de costo-beneficio dentro de los derechos de autor: ¿los DRM permiten el aumento de la creación artística, proporcionando una mayor seguridad de beneficiarse de esa obra, y el beneficio sobrepasa el costo de las oportunidades de expresión del público y los creadores derivados? En el decenio transcurrido desde la promulgación de la DMCA, la evidencia en el lado dañino de la balanza ha aumentado (Mulligan, Han y Burstein, 2003; Von Lohmann, 2010). Por otra parte, mientras que las propuestas para el reconocimiento técnico del *«fair use»* mitigan de alguna manera los problemas causados por los DRM y la antielusión, crean por otra parte un nuevo set de problemas. Al establecer el mandato que los desarrolladores de tecnología endurezcan sus

109. *Corley*, 273 F .3d, pág. 459.

dispositivos o *software*, ellos fuerzan el uso de tecnología resistente al usuario y de métodos capaces de ser endurecidos antes de su distribución a usuarios finales.

2. *Los DRM no impiden la copia*

Junto con las críticas referentes al *fair use,*[110] los analistas han añadido otro motivo de preocupación en la esfera de los derechos de autor: los DRM no impiden en los hechos la copia. Incluso si las restricciones técnicas se defienden como «lomos de toro», para «mantener a la gente honesta»,[111] un conductor honesto puede tomar un simple desvío para evitar el golpe. Como Peter Biddle y sus colegas explicaron en *Darknet*, sólo se necesita un usuario para romper la protección de copia y hacer que el contenido esté disponible en las redes P2P; los usuarios posteriores sólo necesitarán encontrar esa copia (2002: 156). Irónicamente, buscar copias ilegales en Internet sigue siendo más sencillo que programar una videograbadora, a pesar de los intentos de la industria del entretenimiento para acabar con esta práctica. Sin perjuicio de la DMCA, populares películas y archivos de música están disponibles sin DRM a través de redes de intercambio de archivos o sitios de descarga tan pronto como son publicadas en formatos con DRM.[112] Al revisar la evidencia del aumento de las copias, Fred von Lohmann concluye que «la DMCA hasta ahora no ha cumplido con su razón política de ser» (2004: 640). Von Lohmann sugiere, en sus propios términos, que como una medida para detener la distribución en masa de obras protegidas, los DRM respaldados por medidas antielusión han fallado, provocando en su lugar que los usuarios finales busquen copias no autorizadas que terminan siendo más funcionales que las versiones licenciadas con DRM (2004: 642-3).

110. Véase antes la sección 3B 1.

111. «Piracy Prevention and the Broadcast Flag: Hearing Before the Subcommittee on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary» (2003). Declaración de Fritz Attaway, Vicepresidente Ejecutivo de Relaciones Gubernamentales, Motion Picture Association. «BBC News, Digital Film: Industry answers», disponible en <http://news.bbc.co.uk/2/hi/entertainment/4691232.stm#7/>.

112. Douglas Wolk (en «Days of the Leak», *Spin Magazine*, agosto 2007, págs 86-8) describe cómo los álbumes son usualmente comunicados al público a través de servicios de transferencia de archivos aun antes de su lanzamiento oficial.

El resultado es que los titulares de derechos de autor están recibiendo poco de los beneficios que reclamaron. Los DRM no están reduciendo la reproducción no autorizada a la vez que añaden más obstáculos a los usos legales, pero quizás no queridos o no anticipados, de sus obras.[113] Unos pocos participantes de la industria han logrado aprovechar el impulso hacia ofertas más abiertas, pero la mayoría siguen utilizando las debilidades de los sistemas de DRM como una excusa para aumentar las «protecciones».[114]

3. *Las medidas antielusión dificultan la innovación tecnológica*

Si los DRM no detienen las copias, entonces, ¿qué hacen? Tanto sus críticos como sus partidarios lo han reconocido como un método de control tecnológico que continúa funcionando, a través del mecanismo de la antielusión, a pesar de su debilidad frente a la piratería.

El *fair use* y el uso sin permiso no son las únicas bajas de los DRM. Una segunda rama de académicos se ha centrado en el impacto de las medidas antielusión en la investigación científica y la innovación en el diseño de productos. Pamela Samuelson criticó el impacto en la ciencia, ya que la opacidad de las exenciones para la investigación de la DMCA, la dificultad de obtener permisos para fines de investigación, y la necesidad de aclarar el derecho de hacerlo sin permiso previo, congeló la investigación en seguridad computacional (2001: 2028-9). Ed Felten se convirtió en un activo crítico de las medidas antielusión después de que un trabajo de investigación en ciencias recibiera amenazas bajo la DMCA (2005: 112).[115] Fred von Lohmann relató las «consecuencias imprevistas» de las

113. Este artículo no defiende la infracción de los derechos de autor. Por el contrario, se concluye que el costo de las medidas tecnológicas de protección contra la violación de derechos de autor es demasiado alto, y que no existe manera de trazar una barrera técnica menos costosa.

114. En algunos ámbitos, el uso de los DRM está disminuyendo, en particular través del reciente cambio de Apple de ofrecer música a través del iTunes Music Store libres de DRM. Este cambio vino de Apple, no de las compañías discográficas, una vez que Apple había logrado el dominio suficiente en el mercado de la música para mantener su control tecnológico sin el bloqueo de los DRM («Steve Jobs, Thoughts on Music», disponible en <http://www.apple.com/hotnews/thoughtsonmusic/>).

115. Véase más adelante la sección 4B.

leyes antielusión, particularmente en la disminución de las oportunidades para innovar en los mercados complementarios en torno a derechos de autor (2010: 1; 2008: 851-39).

Estas críticas amplían las preguntas más allá del *fair use*. Incluso si los DRM promoviesen el propósito de los derechos de autor, fomentando la expresión creativa, existen costos fuera de los derechos de autor que deben añadirse a la ecuación. Estas comparaciones entre distintos ámbitos añaden retos de inconmensurabilidad aún mayor, obligando a los políticos (si es que quieren tomar una decisión plenamente informada) a comparar el valor de una nueva tecnología de reproducción a la de un trabajo creativo.

Las medidas antielusión cambian la estructura del mercado de las expresiones protegibles por derechos de autor, dando al creador de una obra, o, más frecuentemente, a un grupo de titulares, el derecho y la capacidad de controlar el mercado de las tecnologías de reproducción. Permite a los titulares de derechos de autor ampliar su monopolio legal sobre modos de expresión a las tecnologías.[116] Tim Wu considera que la estructura de mercado de los DRM frena la innovación. Dar a los titulares de derechos de autor demasiado control sobre la difusión y comunicación de sus obras niega oportunidades a un amplio grupo de potenciales innovadores (2004: 331-29; 2006:141-6). En un análisis probabilístico, tener menos oportunidades de innovación potencial reduce las probabilidades de una innovación exitosa.[117]

No todos los que miran a los derechos de autor y a la innovación se oponen a esta extensión de control. Randall Picker argumenta que las ataduras tecnológicas pueden crear oportunidades de mercado. Al dar a los creadores un ámbito más amplio para explotar sus monopolios, sugiere que esta atadura puede facilitar la diferenciación de precios y productos (Picker, 2005: 181). Sostiene que sopesando los mayores

116. «Uno de los nuevos derechos que la DMCA entregó a los estudios cinematográficos es el poder de dictar el diseño funcional de dispositivos electrónicos de consumo» (Patry, 2009: 165).

117. «A menudo, la innovación es el resultado de pruebas de error de aprendizaje no planificadas que se produce entre distintas iniciativas, en lugar de una investigación y esfuerzos de desarrollo organizados por parte de grandes organizaciones» (Kling y Schulz, 2009: 8).

incentivos para los creadores de obras protegidas y la disminución de oportunidades para la «distribución», en general, los DRM causan más bien que mal (2005: 181).

Sin embargo, la mayor parte de los académicos cuestiona el impacto de la DMCA en las estructuras de mercado. Las medidas antielusión presuponen que, o bien el creador es quien está en mejor posición para diseñar o reconocer las tecnologías de reproducción, o que los mercados tecnológicos son menos importantes que la iniciativa del creador.[118] Este control tecnológico de los derechos de autor exige un alto precio, sin embargo, dado el carácter multifuncional de muchas tecnologías de reproducción, la «cola larga» y los aspectos comunicacionales de los medios,[119] muchos de los cuales están mayormente vinculados a usos y libertades personales, y no a contenido destinado al mercado de masas.

4. LA APLICACIÓN DE LAS MEDIDAS ANTIELUSIÓN

Las medidas tecnológicas de protección respaldadas legalmente constituyen una traba a las tecnologías, cada vez más asequibles al usuario y que dan un mayor poder «generador» a particulares y pequeños empresarios.[120] Al restringir la posibilidad de hacer retoques, experimentar y explorar sólo a aquellas utilizaciones autorizadas por los titulares de derechos de autor, la ley limita muchas de las posibles mejoras tecnológicas creadas por usuarios.[121] Los ejemplos del MP3 en la música y los controles de copia de las películas demuestran el impacto de la antielusión en la innovación y la investigación. El ejemplo del PDF de Adobe sugiere que objetivos similares para impedir usos no autorizados pueden ser satisfechos de manera menos intrusivas, mediante advertencias y no a través de características obligatorias.

---

118. Burk y Lemley (2009: 73-4) discuten la innovación acumulativa en las mejoras de patentes.

119. Anderson (2006). Véase también Andrew M. Odlyzko, «Content Is Not King», *First Monday* (5 de febrero de 2001), disponible en <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/833/742/>.

120. Véase antes la sección 2 d.

121. Véase más adelante la sección 5 que discute los beneficios de las mejoras tecnológicas creadas por usuarios.

A) CD VERSUS DVD: LOS EFECTOS DE UN FORMATO BLOQUEADO

En la primera parte de este artículo se contrasta el vibrante desarrollo del entorno musical y la gama de dispositivos aptos para reproducir música en contraste a los límites en torno a las películas. La DMCA explica esta pobreza comparativa: en contraste con el CD, que para preservar la compatibilidad con equipos más antiguos se ha mantenido como un vector de contenido no cifrado y no protegido,[122] el DVD nació encriptado. En cuanto el cifrado activa las protecciones antielusión de la DMCA, nadie puede descifrar «sin autorización» o construir reproductores para hacerlo.[123] Con el fin de ejecutar una película grabada comercialmente en formato DVD, el reproductor requiere múltiples claves: reproductor, disco y título.[124] Las claves de los reproductores (que entregan acceso a otras claves en el disco) son distribuidas sólo a través de reproductores licenciados por el consorcio DVD (DVD CCA). Por lo tanto, las condiciones en que el consorcio está dispuesto a licenciar reproductores —incluyendo las limitaciones requeridas para las salidas de los dispositivos, las restricciones a la copia y la ejecución geográficamente limitada por codificaciones— establecen un límite respecto a las capacidades de todos los reproductores, mientras que el requisito de autorización impide el

122. Los vendedores han tratado de implementar CD «protegidos contra copia», al impulsar la especificación del formato de CD en un intento de frustrar la copia pero no la ejecución, como lo hizo Macrovision con el formato VHS, por ejemplo, mediante la introducción de pistas falsas que un usuario puede pasar por encima, pero que detendrá a un copiador que intentará corregirlo (cf. «Low-Tech Pen Foils CD Copy-Protection Device», *Los Angeles Times*, 21 de mayo de 2002). La multitud de CD no protegidos mantiene a los fabricantes de reproductores en el lado correcto de las disposiciones antitráfico de la sección 17 USC § 1201 (a)(2)(B) (2006), sin embargo, ellos desarrollan mejores mecanismos antisaltos de copia.

123. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 444 (2d Cir. 2001). Véase también más adelante la sección 4A.

124. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 317–18 (S.D.N.Y. 2000), aff'd sub nom. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2001). No es posible obtener acceso a una obra en DVD protegida por CSS, sin el uso de las tres claves requeridas por el software. No es posible obtener un acceso legal a las claves sin acordar una licencia con el DVD CCA, bajo la autoridad entregada por los titulares de derechos de autor, o a través de la compra de un reproductor de DVD que contenga las claves acordes a dicha licencia.

desarrollo independiente sin permiso previo.[125] En consecuencia, las opciones del público para la reproducción y manipulación de películas son significativamente más pobres que las de la música.[126]

Bajo la amenaza de que los estudios cinematográficos impedirían la reproducción de sus contenidos en dispositivos que no fuesen lo suficientemente seguros, las compañías de productos electrónicos de consumo y los fabricantes de programas computacionales negociaron protecciones a través de acuerdos con los estudios. Ellos tenían intereses contrapuestos: los estudios querían altos estándares de protección para sus películas, las compañías de productos electrónicos y de *software* querían algo alcanzable en términos de *hardware* y *software*, respectivamente, a un costo comercialmente plausible al tenor de las limitaciones de fabricación existentes al principio de la década de los noventa. Estas discusiones generaron el Content Scramble System (CSS), una combinación de claves de disco y reproductor, y un sistema de codificación que confiaba en ambas claves para descifrar los contenidos de la película en el disco. «Lo que hace el CSS —explica Tarleton Gillespie— es impedir que los consumidores vean el DVD utilizando un dispositivo inadecuado, esto es, uno que no haya sido certificado por los estudios cinematográficos».[127]

Tan importante como la codificación tecnológica fueron las condiciones de autorización de las licencias necesarias para descodificar. La codificación, no importa cuán débil sea, sirve como gancho para un conjunto de normas de uso y limitaciones: si te mantienes dentro de los límites

125. Véase la sección 5.

126. Las diferencias existentes respecto a las opciones disponibles entre música pregrabada y las películas no se refiere sólo a las preferencias de los consumidores. Aunque podemos disfrutar un video de una forma diferente a la música, el mercado refleja importantes innovaciones respecto a los modos de distribución de videos distintos a las películas pregrabadas, tanto en la creación y alojamiento de videos cortos, como la manipulación del tiempo en el que se accede a transmisiones televisivas, las cuales se envían sin cifrar, desde la temprana perturbación creada por Betamax, a través de TiVo y Slingbox. En consecuencia, los videos que no sean películas pueden crecer lo suficiente como para crear su propio ecosistema, añadiendo presión a las películas pregrabadas, aunque no todavía.

127. «El control de copia y redistribución se impone al asegurar que los propios reproductores autorizados de DVD no permitan la copia; el CSS asegura que los consumidores sólo utilizarán estas máquinas autorizadas» (Gillespie, 2007: 171).

de la licencia podrás obtener una autorización para descodificar; o si procedes sin una licencia, o excediendo los términos de la autorización, esta conducta será considerada una elusión.[128] Sólo aquellos licenciados por el consorcio pueden licenciar; y una vez que han sido enganchados, sólo pueden hacer una cantidad limitada de actividades: ejecutar, en un dispositivo de reproducción dividido en regiones, sin permitir la copia ni la omisión de los contenidos promocionales. Y hacerlo con «blindaje», a través de prohibiciones de ingeniería reversa para el usuario final.[129]

Estas condiciones fueron ineficaces para evitar la vulneración del CSS. A finales de 1999, programadores analizaron el esquema de CSS y produjeron el DeCSS, un programa computacional capaz de descifrar el contenido codificado de un DVD.[130] Jon Johansen, un noruego de 15 años perteneciente al equipo que publicó el código del DeCSS en su página, declaró que lo hizo para permitir la reproducción de DVD en Linux, por cuanto ningún reproductor disponible a la fecha podía funcionar en dicha plataforma.[131] La revista *2600 Magazine* tomó el código DeCSS y

128. Uno podría preguntarse si el derecho de patente ya cumple esta función, volviendo a las normas antielusión superfluas. Específicamente, la reproducción de DVD también implica numerosas patentes, licenciadas por la DVD-CCA (cf. Marks y Thurnbull, 1999). Las patentes parecen ejercer menos escalofríos en la investigación independiente y la innovación (cf. «Letter from Joel I. Klein…», en nota 10). MP3 es reivindicado por Fraunhoffer, aunque es ampliamente utilizado sin licencias. Debido a que no se encuentra legalmente vinculado a reglas de uso, el gancho de las patentes se hunde a menos profundidad (cf. Lemley, 2008).

129. *Reimerdes*, 111 F. Supp. 2d, pág. 310.

130. *Reimerdes*, 111 F. Supp. 2d, pág. 311.

131. Mientras que la Corte en *Reimerdes* determinó que «a la fecha del juicio [principio de la década del dos mil], se habían otorgado licencias a numerosos fabricantes de *software* y *hardware*, incluyendo dos compañías que planeaban comercializar reproductores de DVD que funcionaban con sistemas operativos Linux» (p. 310), ningún reproductor de DVD que funcionara en base al sistema Linux se encontraba comercialmente disponible a esa época. En el año 2004, las compañías todavía hablaban del «primer reproductor de DVD Linux», años después de que la reproducción de DVD existiese en plataformas Windows y Mac (el reproductor Xing, implicado en el quebrantamiento del CSS, fue lanzado en el año 1998) («Xing's Premier Software-Only DVD Player Provides Most Complete, Highest-Quality Solution for Multimedia Pcs Bus», *Wire*, 8 de septiembre de 1998, disponible en <http://find-articles.com/p/articles/mi_moEIN/is_1998_Sept_8/ai_50290471/>). Claro que la oferta de cualquier reproductor en plataforma Linux depende de un sistema de amenazas diferente, dado que en un entorno de código

lo publicó en su página web,[132] siendo obligada a removerlo luego de recibir una notificación que exigía la bajada. A pesar de los argumentos referentes al poder comunicativo del código, las Cortes determinaron que esta publicación era una provisión de herramientas para la elusión, en violación a lo prescrito en la sección 1201 (a) (2) y (b) 0.173 (1).[133]

El Tribunal nunca distinguió cuidadosamente entre acceso y copia, determinando que DeCSS eludía ambos tipos de controles. Más aun, la Corte sólo analizó superficialmente la interrogante de la autorización. Dado que decodificar o descifrar sólo constituye elusión cuando se realiza «sin la autorización del titular de derechos de autor»,[134] necesitamos examinar qué significa «autorización» para distinguir entre la legitimidad del reproductor de DVD que descifra el CSS y la elusión del DeCSS a través de operaciones matemáticas que son sustancialmente idénticas. El cliente, después de todo, no es parte en los acuerdos de licencia entre el consorcio, ni se le pide firmar una licencia al momento de comprar un DVD. Por lo tanto, no resulta claro cómo el DVD o sus reproductores transmiten al espectador su autorización para ver el DVD.

La bifurcación de caminos entre el CD y el DVD proviene de la interacción de la ley con la tecnología, en la cual la ley es compatible con sistemas privados de protección de los derechos de autor a través de restricciones tecnológicas. Con acceso a formatos de música abiertos, los desarrolladores pueden inventar primero y negociar la posición de mercado más tarde (en su caso), y los usuarios pueden convertirse en desarrolladores. Por el contrario, frente a películas cifradas, sólo aquellos desarrolladores que pueden prenegociar el acceso pueden ofrecer mejoras, y sólo de formas bloqueadas, aprobadas y licenciadas por los productores cinematográficos. Así, el cifrado de DVD respaldado por la ley (y sus sucesores de alta definición) bloquea la interoperabilidad y las modificaciones de parte de aquellos que aspiran a hacer público su trabajo. Mientras que aquellos que se preocupan poco de las consecuencias jurídicas ya han roto el cifrado y construido soluciones temporales, la

---

abierto, el reproductor puede, con aun menos eficacia, impedir la captura de los datos descifrados entre el reproductor y el espectador de dichos contenidos.

132. *Reimerdes*, 111 F. Supp. 2d, pág. 309.

133. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 455 (2d Cir. 2001).

134. 17 USC §§ 1201 (a)(3)(A), (b)(2)(A) (2006).

ley impide el desarrollo no autorizado de parte de los principales desarrolladores y, por lo tanto, la posibilidad de crear muchos de los usos innovadores que el video podría admitir. Los mercados, tanto de las obras protegidas por derechos de autor y sus herramientas complementarias, como de los reproductores, se ven retrasados por estas condiciones.

B) LA INICIATIVA DE MÚSICA DIGITAL SEGURA (SDMI) Y LA LIBERTAD PARA MODIFICAR

Como las compañías musicales vieron el otro lado de la historia con moraleja del DVD, el grupo denominado Iniciativa de Música Digital Segura (SDMI, por sus siglas en inglés) propuso «desarrollar un marco abierto y voluntario para ejecutar, almacenar y distribuir música digital, necesario para permitir el surgimiento de un nuevo mercado».[135] Respondiendo al «agujero análogo» y a las preocupaciones existentes sobre la redigitalización, el SDMI propuso un ecosistema de dispositivos que pudieran reconocer una marca de agua integrada y rechazar la ejecución de contenido marcado si aparecía fuera del uso autorizado por una licencia. Dentro de este entorno, las marcas de agua podrían impedir la copia u otros usos no permitidos.[136]

---

135. SDMI Fact Sheet, disponible en <http://web.archive.org/web/20040213143259/www.sdmi.org/-who_we_are.htm> (27 de enero de 2004).

136. Las marcas de agua son una respuesta al «agujero análogo» provocado por el problema de la redigitalización. Al marcar el contenido como protegido de origen, ellos pueden indicar que el contenido estaba originalmente restringido. Si las restricciones iniciales nunca permiten que el contenido pueda ser intercambiado de una forma descifrada, entonces los dispositivos que acepten estas restricciones pueden ser programados para rechazar la reproducción de contenido descifrado y con marcas de agua. Por supuesto que los dispositivos que no acepten estas restricciones pueden simplemente ignorar la marca de agua. Otras propuestas del SDMI sugerían que las marcas de agua podrían ser utilizadas para indicar que una pista de audio no había sido sujeta a compresión desde la aplicación de la marca (véase Craver y otros, 2001). El SDMI invitó a participar a «compañías que tuvieran una actividad directa y relevante en la música digital o en la tecnología de la música digital. Estas compañías deberían expresar su compromiso con el SDMI al aceptar los Términos de Participación y pagar una suma anual de membresía, de veinte mil dólares» (SDMI.org, Frequently Asked Questions, http://web.archive.org/web/20020924-131640/www.sdmi.org/faq.htm; originalmente disponible en <http://www. sdmi.org/faq.htm>).

Las marcas de agua de audio deben cumplir dos metas potencialmente contrapuestas: por una parte, no deben interferir perceptiblemente con el sonido de la música en el cual son aplicados, y a la vez deben ser detectables mecánicamente.[137] Por lo tanto, alguien decidido a frustrar el propósito de una marca de agua, apuntaría a tratar de removerla sin alterar la calidad auditiva de la pista, para que tanto los dispositivos como los oyentes estuviesen satisfechos con esto.

El 6 de septiembre de 2000, el SDMI identificó cuatro tecnologías de marcas de agua como posibles componentes de su estrategia de protección de música, emitiendo una «Carta abierta a la comunidad digital», invitando a la gente a «atacar» las marcas de agua propuestas.[138] Un grupo de científicos en computación e ingenieros eléctricos asumieron el reto, descargando las muestras provistas y analizándolas utilizando métodos de procesamiento de señales para determinar cómo las marcas de agua habían sido aplicadas y cómo podrían ser removidas imperceptiblemente. Este ataque no fue simplemente solicitado por el SDMI, es parte

137. Véase Craver y otros (2001: 3). Las tecnologías de marcado son aquellas en las cuales se incorporan modificaciones sutiles a un archivo de audio sin incorporar cambios perceptibles en la forma en que suena el archivo. Las marcas de agua pueden ser robustas o frágiles: las marcas robustas están diseñadas para sobrevivir transformaciones comunes, como la conversión digital a audio, compresión y descompresión, y la adición de pequeñas cantidades de ruido al archivo; mientras que las marcas frágiles no sobreviven dichas transformaciones, y son utilizadas para indicar una modificación al archivo.

138. Leonardo Chiariglione, «An Open Letter to the Digital Community», <http://web.-archive.org/web/20040216013811/http://www.sdmi.org/pr/OL_Sept_6_2000.htm>, 6 de septiembre de 2000, accedido a través de la búsqueda de sdmi.org en Archives.org). «Aquí hay una invitación para demostrar sus habilidades, hacer algo de dinero, y ayudar a formar el futuro de la economía de la música digital. La Iniciativa de la Música Digital Segura es una iniciativa multindustria trabajando para desarrollar un marco seguro para la distribución digital de música. El contenido protegido del SDMI será acoplado a una marca de agua robusta e inaudible, o a otro tipo de tecnología diseñado para prevenir su copia, uso y distribución no autorizada. Estamos ahora en el proceso de probar las tecnologías que permitirán estas protecciones. Las tecnologías propuestas deberán pasar varias pruebas: deben ser inaudibles, robustas y tener la capacidad de ser ejecutables en distintas plataformas, incluyendo PC. Ellas también deberán ser probadas por ustedes. Por lo que aquí hay una invitación: ataquen las tecnologías propuestas. Vulnérenlas. Al quebrantar exitosamente el contenido protegido del SDMI, ustedes jugarán un rol en la tecnología que el SDMI adoptará definitivamente».

de un estándar de investigación en materia de seguridad computacional. La revisión por pares de las tecnologías constituye una herramienta crítica para determinar su fuerza y mejorar su seguridad.[139] Antes que los titulares de derechos de autor, los fabricantes de dispositivos y los compradores públicos se sumen al esquema creado por el SDMI, querrán saber cuán efectivo será en la consecución de sus metas preestablecidas.

El equipo de Edward Felten rompió exitosamente las cuatro tecnologías de marca de agua, creando nuevas muestras a partir de los originales marcados, que eran auditivamente indistinguibles, y que no presentaban rastros detectables de las marcas de agua (Craver y otros, 2001: 12). El equipo eligió presentar su trabajo como una presentación académica, asegurando su aceptación en el arbitrado *Fourth International Information Hiding Workshop*.[140] Sin embargo, antes que pudieran presentar el trabajo, Felten recibió una carta de parte de la Asociación de la Industria Discográfica de América (RIAA, por sus siglas en inglés), amenazándolo con una demanda basada en la DMCA.

> Cualquier divulgación de información obtenida al participar en el Desafío Público se encontraría fuera del ámbito de las conductas permitidas por el Acuerdo y podrían sujetarlo a usted y a su equipo investigativo a las acciones establecidas en la Digital Millennium Copyright Act.
>
> Desafortunadamente, la revelación que usted está contemplando podría provocar significativas consecuencias, que podrían dar lugar a la distribución ilegal de material protegido por derecho de autor. Dicha revelación no se encuentra autorizada en el Acuerdo, pudiendo constituir una violación de éste, sujetando a su equipo de investigación a las acciones establecidas en la DMCA, y posiblemente a otras leyes federales.
>
> Adicionalmente, debido a que la divulgación pública de su investigación excede el ámbito de la Autorización, usted podría ser objeto de acciones coercitivas establecidas en la Ley Federal, incluyendo la DMCA.

---

139. Véase la declaración de Ed Lazowska, en *Felten v. Recording Indus. Ass'n Am.*, CV-01-2669 (D.N.J. 13 de agosto de 2001), disponible en http://w2.eff.org/IP/DMCA/Felten_v_RIAA/-20010813_cra_decl.html. Véase, en general, Schneier (1996), quien discute la seguridad computacional.

140. Véase «Janelle Brown, Is the RIAA running scared?», *Salon*, 26 de abril, 2001, disponible en <http://www.salon1999.com/technology/log/2001/04/26/felten/index.html>; «Reading Between the Lines: Lessons from the SDMI Challenge», <http://www.cs.princeton.edu/sip/-sdmi/>.

> El Acuerdo específicamente reserva a los proponentes de la tecnología atacada cualquier derecho que puedan tener «bajo cualquier ley aplicable, incluyendo, sin limitación, la Digital Millennium Copyright Act de los Estados Unidos de América, por cualquier acto que no haya sido expresamente autorizado en el Acuerdo». El Acuerdo simplemente no «autoriza expresamente» a los participantes a revelar información e investigación desarrollada a través de la participación en el Desafío Público y, por lo tanto, tal revelación podría ser objeto de una acción prevista en la DMCA.[141]

Los investigadores y los organizadores de la conferencia quedaron lo suficientemente preocupados por estas amenazas legales como para retirar su trabajo de la conferencia de abril del año 2001. La RIAA prontamente emitió un comunicado señalado que su intención nunca fue demandar. Sin embargo, los investigadores se sintieron gravemente preocupados frente a las futuras presentaciones de su trabajo, como para presentar una solicitud de juicio declarativo, que declarase que su trabajo no violaba la DMCA.[142]

El incidente demostró el escalofriante efecto que provoca la prohibición amplia de la DMCA sobre la diseminación de tecnología y sus «componentes». Aunque los investigadores finalmente publicaron y presentaron su trabajo, la RIAA y el SDMI fueron capaces de utilizar alegatos basados en la DMCA para retrasar su publicación y presentación en medio año, y perfectamente podrían haber asustado a equipos completos de investigación que no estuviesen respaldados por un profesor universitario y por asistencia legal gratuita. La ley antielusión, entonces, bloqueó el examen científico y educacional de tecnología, incluyendo la interoperación antielusión.

¿Y con qué fin? La investigación demostró que las fallas en estas marcas de agua apuntan a falencias en la estrategia final. Si incluso las mejo-

---

141. «Letter from Matthew Oppenheim, Secretary, SDMI Foundation, to Edward Felten, 9 de abril, 2001», disponible en <http://cryptome.org/sdmi-attack.htm>.

142. Ver «First Amended Complaint, Felten v. Recording Indus. Ass'n Am.», CV-01-2669 (D.N.J. 26 de junio, 2001), disponible en http://w2.eff.org/IP/DMCA/Felten_v_RIAA/-20010626_eff_felten_amended_complaint.html. La demanda fue rechazada por falta de fundamentos. «Felten v. Recording Indus. Ass'n Am.», No. 01-CV-2669 (D.N.J. Nov. 30, 2001).

res marcas de agua que pudo diseñar el SDMI eran vulnerables al análisis y remoción, es poco probable que estos investigadores fuesen los únicos que pudiesen hacerlo. Entre los sujetos que comparten música objeto de limitaciones tecnológicas, podrían existir otros capaces de eludir estos controles y que podrían compartir los archivos libres de restricciones con otros.

Desde la ruptura de sus tecnologías de marcado, la iniciativa SDMI se ha disuelto hasta la insignificancia como fuerza tecnológica. Una nota de su ahora difunta página web indicaba que el «Foro SDMI se encuentra suspendido desde junio de 2001, y no está aceptando nuevos miembros».[143] Por otra parte, la investigación de Felten ha sido citada por otros, tanto en investigaciones asociadas a seguridad informática como en protección de derechos de autor (Popescu y Farid, 2004; Haldermann y Felten, 2006).

La expansión al estilo SDMI no es la única alternativa. Las respuestas tecnológicas a la ley no necesitan ser llevadas a extremos ilógicos, pero pueden dejar espacio para desarrollo independiente si renuncian al respaldo legal para sus pruebas. El uso por parte de Adobe de un control tecnológico limitado en su *software* PDF, ilustra esa opción y señala los lugares donde la tecnología respaldada por la ley podría bloquear el desarrollo abierto, así como las ventajas de alejar a los sabuesos de la DMCA.

C) UNA ALTERNATIVA: MEDIDAS DE ADVERTENCIA NO ROBUSTAS

Autores de documentos utilizando versiones de alta calidad de Acrobat, la aplicación PDF creada por Adobe, pueden elegir controlar el «acceso» inicial, cifrar y proteger los documentos por contraseñas; y también controlar el «uso», al restringir la impresión, la selección de texto e incluso el uso de las aplicaciones de lectura en pantalla.[144] Las diferentes implementaciones de controles (de acceso o de uso) —y sus interacciones con el código abierto y con la ley antielusión— dan una idea de la forma en que la ley afecta el desarrollo independiente.

---

143. SDMI.org, Frequently Asked Questions, disponible en <http://web.archive.org/web/20040213073219/www.sdmi.org/faq.htm> (27 enero, 2004)

144. Véase Adobe, «Adobe Acrobat Pro Extended: Features», <http://www.adobe.com/products/acrobat-proextended/features/>.

El control de acceso de PDF es proporcionado por cifrado, utilizando públicos y modernos algoritmos. A todos se les puede asignar una burbuja cifrada, la cual sólo puede ser descifrada por aquellos a quienes se les ha entregado la clave correspondiente. Pero el «acceso» es binario: encendido o apagado. Una vez que el lector ha descifrado el documento, él o ella tienen el documento descifrado en toda su gloria digital, con el potencial de imprimir, guardar y reenviar.

Este cifrado es robusto: incluso implementado en un código abierto, *software* completamente modificable, entrega acceso al documento sólo a aquellos que cuentan con la contraseña o el certificado correcto. La fuerza de la codificación es independiente del carácter público de su implementación; de hecho, los algoritmos públicos y las implementaciones que han estado sujetas a pruebas son probablemente más fuertes que aquellas que han sido desarrolladas en forma privada.[145] Con un espacio de claves lo suficientemente grande como para bloquear ataques de fuerza bruta, un autor puede estar relativamente confiado en que sus documentos serán accesibles sólo a aquellos con la contraseña. El autor puede crear una clave de acceso diferente para cada usuario y documento, o usar infraestructura de clave pública para cifrar a un receptor con una clave privada preexistente.

A medida que se desee compartir el documento de manera más amplia, sin embargo, el autor puede preocuparse que un receptor autorizado pueda compartir el documento con otro, hacer copias extras, o dejar impresiones repartidas por ahí. Por sí mismo, el cifrado no se hace cargo de esas preocupaciones.

En el sistema de Adobe, algunos de estos controles de uso son proporcionados por banderas que marcan restricciones respecto a lo que el software Adobe puede hacer con el documento. El *software* lector de Adobe hace cumplir estas restricciones, por lo que el receptor que utiliza Acrobat para abrir un documento marcado «Impresión: no se admite; Selección: no se admite» encontrará que las opciones usuales de impresión y selección de texto están en gris y no disponibles. En el *software* lector de Adobe, un documento tal puede ser visto en la pantalla, pero no puede imprimirse, extractarse o convertirse a otros formatos. El ar-

145. «Cualquiera puede diseñar un sistema de seguridad que él mismo no pueda vulnerar» (Schneier, 2008).

chivo en sí mismo puede copiarse infinitas veces, pero cada copia tendrá el mismo set de restricciones.[146]

La especificación PDF es revelada públicamente[147] y ha sido implementada en otras aplicaciones, incluyendo el Preview de Apple y el XPDF, licenciado a través de una licencia GPL.[148] Preview, el lector por defecto de PDF del Apple Macintosh, responde a una bandera de «no imprimir» al impedir la impresión y solicitando una contraseña. Asimismo no permite la selección de texto en un documento cuyo autor ha establecido esa bandera.

De la forma en que se distribuye, el XPDF se comporta de manera similar, cumpliendo con las banderas también. Los intentos de imprimir documentos marcados desde una copia no modificada de XPDF serán recibidos con un mensaje de error que señalará: «La impresión de este documento no se encuentra permitida». Pero la implementación de XPDF no es «robusta». Por cuanto el código fuente del XPDF se encuentra disponible a aquellos que quieran modificarla, los usuarios frustrados por las marcas de un documento XPDF pueden compilar sus propias versiones. Entre otras personalizaciones, se puede ordenar a una versión modificada del XPDF que ignore las banderas del programa, haciendo mínimas modificaciones en cinco simples líneas de código.[149]

---

146. El documento puede estar codificado, pero el usuario que obtiene los privilegios de «sólo ver» no necesita insertar una clave y, por lo tanto, debe estar incluida en el programa en sí mismo, y compartido por cada copia del programa. Por lo que el efecto es meramente el de una bandera.

147. Ver «PDF Reference», <http://www.adobe.com/devnet/pdf/pdf_reference.html>.

148. Ver «Apple, What is Mac OS X. Graphics and Media», <http://www.apple.com/macosx/what-is-macosx/graphics-media.html>; XPDF, Home, <http://www.foolabs.com/xpdf/home.html>.

149. Incluso para aquellos sin conocimiento de programación, este código fuente es bastante directo:

```
if (! doc->okToPrint()) {
error(-1, «Printing this document is not allowed.»);
exitCode = 3;
goto err1;
}
```

En español: Si el documento no tiene la indicación de «está bien imprimir», enviar mensaje de error y abortar, de otra forma, continuar con la solicitud del usuario. Un usuario que quiera imprimir un documento que no admita impresión, podría simplemente remover este bloque condicional:

El código de XPDF podría haber sido «ofuscado» para hacer que esta modificación fuese más difícil de lograr, pero eso sólo significaría algo más de trabajo para el aspirante a impresor. Se permita o no la impresión, el *software* debe contar con acceso suficiente al documento para poder desplegarlo en la pantalla. En este punto, el formato se basa en el *software* para hacer cumplir sus restricciones, y el *software* puede ser modificado para ignorar una simple bandera y redirigir en el documento tanto a la impresora como a la pantalla.[150]

La apertura de la especificación PDF contribuye a su popularidad como un formato estándar de intercambio y exhibición de documentos. Incluso antes que Adobe proporcionase aplicaciones para la mayoría de las plataformas, los usuarios podían leer y crear archivos PDF en sistemas Unix y GNU/Linux, así como en Macintosh y Windows. Apple podía decidir, con gastos bajos, proporcionar respaldo para PDF en su sistema operativo OSX. Los usuarios de sistemas operativos GNU/Linux como Ubuntu pueden elegir entre Adobe Reader, XPDF, y Ghostview, entre otros.[151] Desarrolladores independientes pueden añadir caracterís-

---

// if (! doc->okToPrint()) {
// error(-1, «Printing this document is not allowed.»);
// exitCode = 3;
// goto err1;
// }

Si no se mantiene la presencia o el valor del «okToPrint», un documento marcado se puede imprimir tan fácilmente como se despliega en la pantalla.

Esta autora tuvo que compilar una versión amigable a la impresión del XPDF cuando, siendo editora del *Harvard Journal on Law & Technology* (JOLT), fue contactada por uno de los autores de la revista. Ese autor había creado una versión PDF de su propio artículo con las especificaciones «impresión no permitida» y «selección de texto no permitida». Después que JOLT hubiese publicado el artículo en su página web, el autor perdió el original y quería recuperar el texto. Una versión modificada del XPDF le permitió hacer esto. Esta autora entiende que funciones similares se encuentran disponibles actualmente en programas de distribución comercial.

150. Es posible que incluso si el lector estuviese disponible sólo en formato binario, podría de todas maneras ser sujeto de ingeniería reversa, descompilado y editado para remover la bandera. El código binario y ofuscado solo serviría como un obstáculo menor para un ignorador de banderas determinado a remover esta marca.

151. Véase «Ubuntu Linux, Details of Package Pdf-viewer in Karmic», <http://packages.ubuntu.com-/karmic/virtual/pdf-viewer/>, que lista siete visores de PDF de código abierto.

ticas al XPDF de código abierto o incorporar sus funciones a los nuevos programas, como la página de Internet generadora de pdf PDF2HTML. Los usuarios pueden crear índices de texto completo de los archivos PDF, facilitando una mejor búsqueda o programas independientes para anotar los documentos PDF. Aplicaciones de lectura en pantalla pueden leer el texto en voz alta. Google y otros motores de búsqueda pueden analizar los archivos PDF para incluir su texto en la búsqueda. Mientras tanto, Adobe se beneficia de este entorno a través de las regalías obtenidas de versiones mejoradas de su lector de PDF y su creador de PDF. Autores de documentos se benefician de la amplia disponibilidad de herramientas, reduciendo los obstáculos a la lectura de las obras que ponen a disposición. El formato DRM abierto de Adobe es exitoso debido a que Adobe no insiste en hacerlo robusto. Contraste este formato con mínimas medidas DRM de advertencia con otras estrategias DRM más robustas, incluyendo el formato de *eBook* de Adobe. Estos atan las dos ramas de la estrategia, mediante el cifrado y la sección 1201, para obligar al lector autorizado a usar una aplicación en particular o obedecer las restricciones de esta aplicación.

Las medidas de advertencia anticopia pueden tener un lugar, especialmente si no invocan la DMCA. Pero la actitud de Adobe a los quebrantamientos de la propiedad antiimpresión de PDF contrasta con la persecución —mediante la utilización de la DMCA— que ha llevado en contra de Elcomsoft, luego que Dmitry Sklyarov rompiera el cifrado de su formato de *e-book*. Sklyarov, un estudiante de doctorado ruso, estaba en el país para una conferencia sobre seguridad computacional en el cual hizo una presentación respecto a la inseguridad de la tecnología de cifrado del *e-book* de Adobe. Luego de la presentación, él fue arrestado y acusado de traficar un producto diseñado para eludir protección de derecho de autor, en una violación de naturaleza criminal de la DMCA, fundado en la venta por parte de su empleador de un *software* diseñado para leer *e-books* cifrados.[152] Adobe había alentado la acusación, pero

152. «Criminal Complaint, U.S. v. Sklyarov», No. 5-01-257 (N.D. Cal. 17 de julio, 2001); ver también «Press Release, Dep't of Justice, First Indictment Under Digital Millennium Copyright Act Returned Against Russian National, Company, in San Jose, California» (28 agosto, 2001), disponible en http://www.cybercrime.gov/Sklyarovindictment.htm.

después solicitó al gobierno que los cargos en contra de Sklyarov, en particular, fuesen desechados, luego que se produjeran protestas públicas. Un jurado federal finalmente rechazó los cargos basados en la DMCA en contra de la compañía.[153]

A muchas empresas, la DMCA las induce a comportamientos como el de Adobe para proteger de cerca su formato de *e-book*, en vez de promover la apertura de las especificaciones del formato PDF, en desmedro de la tecnología de código abierto y accesible al usuario. Con estos ejemplos en mente, este artículo examina las consecuencias de las normas antielusión en el desarrollo abierto a través de la óptica de las investigaciones económicas y legales realizadas sobre la innovación distributiva.

5. NUEVA CRÍTICA: LAS LEYES ANTIELUSIÓN DE MEDIDAS TECNOLÓGICAS DE PROTECCIÓN GRAVAN EL DESARROLLO ABIERTO Y LA INNOVACIÓN DE USUARIO

Más allá del *fair use*, la DMCA provoca costos al impedir un modo completo de desarrollo. La DMCA y los vínculos contractuales construidos en torno a su régimen antielusión, impide el desarrollo de *software* y *hardware* de código abierto, ya que es imposible construir el secreto que requieren los DRM en un producto diseñado para la modificación de usuario y el desarrollo colaborativo. Con todo, esta limitación añade otro conjunto de cargas al balance estructural descrito por Tim Wu (2006) y Yochai Benkler (2003): los costos no sólo de centralizar la creación e innovación, sino que también de excluir a los usuarios, aquellos más familiarizados con sus necesidades y deseos tecnológicos, del proceso de diseño. Contra toda lógica, las medidas antielusión ejercen este efecto de limitar el desarrollo tecnológico justo cuando los juristas, al igual que economistas y académicos en materia de administración, están reconociendo las importantes contribuciones derivadas del desarrollo del código abierto, la innovación de usuario y la colaboración en masa (Benkler, 2007; Von Hippel, 2005; Lakhani y von Hippel, 2003; Lerner y Tirole, 2002).

El impacto concreto de las limitaciones inducidas por las normas an-

153. Lisa M. Bowman, «ElcomSoft Verdict: Not Guilty», Cnet News.Com, (17 de diciembre, 2002), http://news.cnet.com/2100-1023_3-978176.html.

tielusión pueden haber sido pasadas por alto al momento de determinar los costos de los DRM debido a que no han sido reconocidas, o porque el impuesto al «modo de desarrollo» no ha sido distinguido del impacto global que los DRM tienen sobre la innovación. Si bien este problema comparte muchos de los elementos del daño generalizado a la innovación, posee elementos que distintivamente se encuentran más profundamente arraigados; no es la clase de problema que pueda ser resuelto dentro del marco de las medidas antielusión. Incluso si los diseñadores de DRM hicieran eco de las críticas académicas y trataran de hacer un espacio a la innovación, en última instancia, se enfrentarían a una brecha irreconciliable entre los DRM y la apertura a la innovación.

Este artículo, por lo tanto, añade a la literatura existente sobre este tema un análisis sobre el impuesto al «modo de desarrollo». Las secciones anteriores describieron la progresión a través de la cual la gestión de derechos digitales, apoyada por las leyes antielusión, se orienta incluso a niveles más altos de limitaciones. Cada reacción a cualquier amenaza percibida (ya sea al control de los medios de difusión o a la rentabilidad) empuja los intentos de limitación al núcleo mismo del diseño de productos: de dispositivos simples que dificulten la copia, a diseños más complicados, a mecanismos «blindados» para proteger dichos dispositivos y asegurar que operen de la forma en que fueron concebidos, y finalmente a mandatos arquitectónicos e incompatibilidad forzada. En esta parte se analizará ahora el costo de estas limitaciones. Cambiando no sólo quién puede innovar, sino que también la forma en que pueden hacerlo, limita severamente el espacio de desarrollo y su zona de potencial. Caracterizar a las medidas antielusión como una barrera al «modo de desarrollo» explica por qué estas leyes son problemáticas incluso cuando los DRM que apoyan son elegidos por privados en lugar del Estado. La antielusión provee el gancho a través del cual se pueden requerir algunos DRM, y sin importar cuán abierto fue el proceso para desarrollar el estándar DRM, los dispositivos que los implementan deben necesariamente ser cerrados.[154]

154. Ésta es la falla detrás del supuesto modelo de «código abierto» detrás de la plataforma DREAM de Sun. Incluso si cualquiera puede construir una implementación de la especificación, sólo obtendría «autorización» para reproducir contenido protegido, luego de probarse que no puede ser modificado por otros. Los desarrolladores escribiendo este

Mientras que los DRM son ineficaces en contra de la redistribución de masa,[155] imponen costos varios en todos los aspirantes a desarrolladores de dispositivos interoperables: los costos de licencias o los costos de eludir la licencia solicitada, incluyendo los costos de romper los DRM (o la búsqueda de una ruptura existente); los costos de asegurar que otros usuarios también podrán utilizar la modificación si ésta fue desarrollada más allá que para el uso personal; y los costos de la inseguridad jurídica. Los DRM —respaldados por la ley— limitan el potencial de crecimiento de la innovación, ya que si un desarrollador espera comercializar un

---

código serían incapaces de cumplir con la condición de «libertad para modificar» de la licencia GPL de la Free Software Foundation (cf. Fernando, Jacobs y Swaminathan, 2005).

155. Mientras los DRM traten de proteger contenidos destinados a su distribución en masa, enfrentarán un reto asimétrico de adversarios tan ampliamente distribuidos como los intereses que protegen (Lewis, 2004). Incluso con los mecanismos de DRM más fuertes existentes actualmente, el principio BORA (*rompe una vez ejecuta dondequiera*) se mantiene. Una vez que el contenido es obtenido de un sistema DRM, y recodificado en una forma no protegida por DRM, la duplicación de dicho contenido es tan fácil como mover bits. Esto significa que el costo de vulnerar o romper DRM en una pieza particular de contenido sólo debe ser soportado una vez. Los costos marginales de la duplicación para el consumidor que puede obtener el contenido son cercanos a cero y, más aún, el consumidor no necesita gastar en recursos para quebrantar los DRM (Lewis, 2004; Schechter y otros, 2003, describen el costo de los bienes pirateados como una función de costos en los que se incurre una sola vez —o costos de la primera copia— y costos de distribución por cada copia). ¿Entonces por qué los DRM no son igualmente ineficientes en contra de la innovación? Un tipo diferente de hackeo es necesario para la distribución del original extraído versus la innovación de los usos alrededor de ese original. Para impedir la copia y distribución en masa permitida por Darknet, sería necesario parar a cada posible copista, porque una vez que una copia ve la luz, puede ser compartida con otros a costos considerablemente más bajos. Mientras que para impedir la innovación de usuario, se pueden levantar barreras que impidan a un grupo alcanzar la masa crítica necesaria para superar la barrera —y de esta manera cada persona deberá superar la barrera. Desde luego, algunos quebrantamientos, en programas computacionales que no se encuentren individualizados, pueden ser compartidos en lugar de tener que ser recreados (cf. Pash, 2007). También puede ser más fácil quebrantar que interoperar, encontrando un desbordamiento del búfer en lugar de entender el código ofuscado. Mientras que el *Myth of the Superuser* de Paul Ohm (2008) establece un argumento persuasivo en contra del enfoque en el «superusuario» de las leyes criminales informáticas, en un contexto de DRM sólo se necesita un moderadamente «súper» usuario para poner a disposición de todos contenidos no cifrados. Fred von Lohmann (2005) se refiere a esto como el problema de la «vaca inteligente» de Mike Godwin.

producto, puede predecir que tendrá que solicitar una licencia y, de tener éxito en la obtención de dicha licencia, tendrá que compartir las rentas provenientes de la innovación.[156]

Incluso si las reglas de uso no supusieran restricciones prácticas de uso, como por ejemplo que un dispositivo «debe permitir menos de seis mil millones de ejemplares» las reglas de blindaje, obligando su implementación a través de mandatos tecnológicos, de todas maneras atarían las manos de los desarrolladores. Para construir un sistema capaz de asegurar que no tiene más de 5.999.999.999 reproducciones, el constructor debe bloquearlo, prohibiendo al usuario final la manipulación del sistema y anulando las garantías. Para que un sistema fiable sea confiable, debe ser endurecido en contra de sus usuarios (Schoen, 2005).

El mismo reto tienen aquellos que quieren diseñar sistemas para adjudicar usos protegidos por *fair use* o para confirmar con un árbitro en calidad de tercera parte antes de permitir nuevos usos.[157] Incluso si el arbitraje es perfecto, el juez está en sintonía con todos los matices de la libertad de expresión, el sistema debe ser endurecido para ser capaz de hacer cumplir esas determinaciones en forma robusta. Los usuarios de la tecnología aún estarán impedidos de modificar el núcleo de sus dispositivos de reproducción. Del mismo modo, la estandarización de la infraestructura DRM podría acabar con los DRM hechos a medida, haciendo más fácil la interoperabilidad y comercialización de obras entre licenciatarios para sus plataformas, pero este estándar continuaría impidiendo la modificación de los usuarios.

No es posible endurecer las medidas técnicas de protección, sin cerrar los dispositivos a la modificación de usuario.[158] La «computación confia-

156. El potencial de retraso es similar a aquel consistente en el bloqueo de patentes a través de medidas precautorias. Lemley y Shapiro (2006) argumentan que las medidas precautorias de patentes «fomentan la búsqueda de utilidades por *trolls* de patentes y desincentivan la innovación de parte de firmas que diseñan y fabrican productos complejos».

157. Véase antes la sección 3B.

158. «Una vez disociado de su protección, el contenido puede ser libremente reproducido, modificado y redistribuido, aun cuando se produzcan violaciones a los términos de la licencia. En consecuencia, para hacer cumplir políticas de DRM típicas, no debe ser posible para el usuario de la plataforma el acceso a los bits en lenguaje de texto que representan el contenido, a pesar de que en la práctica la plataforma se encuentra bajo

ble» propone un núcleo cerrado con interfaces abiertas. Un sistema que ofrezca a los usuarios acceso a diversas funciones, manteniendo a la vez oculto el flujo de decodificación de medios, puede ser mejor que nada pero no es código abierto. En esencia, permite a los usuarios cambiar las carátulas de la radio de un auto, pero no modificar los sintonizadores. De este modo, donde los usuarios no pueden manipular el flujo de los medios directamente, ellos se encuentran impedidos de implementar modificaciones más profundas, como la modulación de audio para que coincida con la versión acelerada de un vídeo o añadir cancelación de eco (Seltzer, 2005; Gutmann, 2007).

Los titulares de derechos de autor quieren una configuración que no pueda alterarse para permitir la fuga de la obra, excepto a través de dispositivos de salida autorizados. Ellos preferirían tener garantías de que sus dispositivos autorizados llegaran directamente hasta los ojos y oídos del espectador, pero como los implantes quirúrgicos no son viables, ellos exigen que por lo menos existan conductos encriptados que lleguen hasta los puntos de salida analógicos de pantallas y parlantes. Mientras que el *software* y *hardware* cerrado pueden participar en la

---

el control directo del usuario. Este es un problema de control de acceso, que no puede ser resuelto sólo a través de criptografía. En plataformas computacionales abiertas que pueden ejecutar programas computacionales arbitrariamente, es un problema para el cual no se ha desarrollado una solución, particularmente en los términos de técnicas de «sólo *software*». Recientemente, iniciativas de «computación confiable», en particular, la Next-Generation Secure Computing Base de Microsoft Next Generation (NGSCB) y el Trusted Computing Group (TCG), anteriormente conocido como TCPA, apuntan en parte a enfrentar este problema a través de métodos de *hardware* y *software*.

«La meta de la "computación confiable" es entregar sistemas que sean altamente resistentes a la subversión por parte de adversarios maliciosos, permitiendo la operación confiable y predecible bajo casi cualquier circunstancia. La computación confiable es un ingrediente confiable de los DRM porque provee de una base sensata para la coercibilidad de licencias. Dada la forma en que las iniciativas NGSCB y TCG han sido promovidas, uno podría ser disculpado por pensar que la computación confiable constituye un concepto completamente nuevo. Como discutimos en la sección 3.1, la computación confiable tiene, de hecho, una larga historia, pero las lecciones que esta historia puede enseñar han sido ignoradas en su mayor parte durante los últimos veinte años, particularmente en el diseño de sistemas operativos para PC. Consecuencialmente, dichos sistemas se encuentran mal equipados para proveer el nivel de protección que un sistema DRM robusto requiere» (Reid y Caelli, 2005: 1-2).

carrera, apareciendo como seguros hasta que venga un *hacker* más inteligente, el *software* de código abierto y el *hardware* modificable por el usuario ni siquiera pueden participar de esta carrera. Sus secretos serían intencionalmente revelados. La «computación confiable» ofrecida como la solución de próxima generación para medios digitales en *hardware* de propósitos generales, no permite una mayor apertura, simplemente empuja el cierre a «módulos de plataforma confiable» y «certificación a distancia», y todavía excluye el desarrollo abierto de *software* y *hardware* asociado a soportes de medios.[159] Más aún, la «computación confiable» no permitiría el *hardware* de código abierto, tal como lo señala Peter Gutmann (2007) en su catálogo de los costos de la protección de contenido de Windows Vista. Ni el *software* ni el *hardware* en una plataforma de «computación confiable» es realmente abierto y modificable, incluso si sus partes se encuentran visiblemente bajo un cristal. Esta clase de transparencia de una sola vía no podría apoyar el vibrante entorno de innovación que vemos alrededor de *software* y *hardware* genuinamente abierto. La apertura se encuentra excluida por las reglas de diseño de los DRM.

A) LOS COSTOS OCULTOS DE LOS DRM

Más allá de impedir el *fair use*, las restricciones impuestas por las medidas antielusión son problemáticas porque excluyen un modo específico de desarrollo: el modo público del *software* abierto y libre, que ha sido cada vez más exitoso tanto en producciones comerciales como no comerciales (Lerner y Tirole, 2002). La antielusión excluye las alteraciones y modificaciones por parte de los usuarios finales y establece una estructura industrial centralizada, justo cuando la tecnología nos ofrece los medios y las oportunidades de hacer más, a partir de los confines de Internet (Benkler, 2007; Shirky, 2008; Zittrain, 2006).

159. La «computación confiable» provee una plataforma de confianza, autenticada para estar en un estado seguro con vías de entrada y salida seguras, un código fuente auditado que pueda «certificar» su integridad, chequeando con un servicio remoto para verificación en tiempo real antes de ejecutar la entrada de medios digitales (cf. Schoen, 2005: 4-5). En este caso, el código fuente para esta aplicación puede ser entregado, pero dado que una versión modificada no puede aprobar el chequeo, éste no sería capaz de funcionar. Este tipo de código no podría aprobar las definiciones de código abierto o de software libre.

Mientras que las grandes empresas ya tienen muchas ventajas económicas sobre los competidores más pequeños, incluyendo operaciones a gran escala y la minimización de los costos de transacción, investigaciones recientes sugieren que una diversidad de fuentes puede fomentar de manera más efectiva la innovación.[160] Las empresas menos poderosas y los usuarios-innovadores pueden estar mejor posicionados para expandir límites, explorar vías que pueden no haber sido exploradas por los actores dominantes de las industrias. Entonces, compañías sin una base de clientes pueden estar en mejor posición que una compañía con una posición más dominante para generar innovaciones disruptivas que encuentren apoyo fuera de una base de clientes preestablecida; aunque las innovaciones disruptivas al principio no sean usadas por clientes preexistentes, ellos pueden, a la larga, cumplir de mejor manera la demanda tanto de los clientes antiguos como de los nuevos.[161] Mientras tanto, los propios usuarios pueden adaptar o innovar productos preexistentes, utilizando información y motivaciones disponibles de mejor manera para ellos que para las corporaciones.[162] Bajo un régimen de antielusión, sin embargo, cualquier innovador que quiera retar a la industria dominante es excluido por la ley que centraliza el «permiso para innovar» en el titular de derechos de autor.

Las medidas antielusión afectan a diferentes tipos de innovadores de forma diferente. La innovación disruptiva por empresas de escala comercial puede aún ser posible en circunstancias limitadas: si el posible innovador disruptor puede obtener una autorización anticipada. Un novato en materia de medios digitales que es a su vez un actor establecido en otra área puede que tenga el poder para negociar una autorización con un número suficiente de titulares de derechos de autor, y a través de esa autorización, convertir sus acciones en no elusivas; siendo muy poco probable que usuarios individuales puedan hacer esto. Incluso en un mercado de medios digitales no concentrado y no coordinado, ni las compañías ni los usuarios serán capaces de obtener un «permiso para

160. Véase más adelante la sección 5B.

161. Para el exponente líder en material de innovación disruptiva, vease Christensen (1997: 79-81, 132-34).

162. El líder en investigación de innovación es Eric von Hippel (cf. Von Hippel, 2005: 19-229).

alterar» o para ofrecer productos de acceso a medios de uso general que puedan ser modificables por otros usuarios, porque es precisamente ese acceso al flujo subyacente de medios digitales lo que los DRM buscan impedir. En un mercado concentrado y coordinado, unos pocos participantes privilegiados pueden obtener acceso a la mayor parte de los medios digitales, pero incluso entonces no estarán en condiciones de ofrecer productos abiertos modificables por los usuarios.

B) LOS DRM LIMITAN LA INNOVACIÓN DISRUPTIVA

Numerosas industrias se han reconfigurado dramáticamente debido a innovaciones disruptivas, desarrollos no lineales que benefician al público a través de mayores niveles productividad, eficiencia o elección. Como lo describe Clayton Christensen (1997: 79-86), las tecnologías disruptivas son a menudo descartadas como inferiores inicialmente por aquéllos en la industria, pero rápidamente alcanzan y superan a las antiguas. Estas tecnologías tienen dos características esenciales: «en primer lugar, por lo general poseen un conjunto de atributos de rendimiento diferentes, los que, por lo menos al principio, no son valorados por los clientes existentes. En segundo lugar, los atributos de rendimiento que los clientes existentes efectivamente valoran, mejoran a un ritmo tan rápido que aquella nueva tecnología puede, posteriormente, invadir aquellos mercados preestablecidos» (Bower y otros, 1995: 44). Por lo general, señala Christensen, las innovaciones disruptivas son pasadas por alto o dejadas de lado por los productores existentes, incluso en compañías «buenas» (1997: 207). Las fortalezas de una empresa en escuchar las demandas de los clientes existentes («mantener» las innovaciones) pueden ensordecerla frente a los llamados de un nuevo producto con diferentes características y objetivos (1997: 20). Entonces, industria tras industria, los competidores han usurpado los lugares de los antiguos gigantes (Christensen y Raynor, 2003: 34-43).

Los productos o servicios disruptivos parecen al principio ser una alternativa inferior para los clientes principales. Las aplicaciones de mercado a las que estos productos podrían ajustarse, ofrecen menores márgenes de ganancias, haciéndolos menos atractivos para empresas establecidas. Un recién llegado, enfrentando un conjunto diferente de costos de oportunidad, podría estar dispuesto a experimentar, vendiendo sin

embargo a clientes pertenecientes a un segmento con menores márgenes de ganancias (Christensen, 1997: 26). Al hacerlo, mejora su producto competidor. La «disrupción» ocurre cuando alguno de estos competidores mejorados atrae la atención del público general, migrando desde los márgenes del mercado, venciendo al estándar anterior (Christensen, 1997: 77-95). El antiguo líder del mercado se queda lamentándose de no haber prestado más atención a los más pequeños, a discos y minicomputadoras de menor tamaño, antes vistos como tecnología inferior (Christensen, 1997: 134-38).

Christensen sugiere que los operadores tradicionales pueden aprender a innovar de forma disruptiva (Christensen y Raynor, 2003: 33-5), pero los números y el apetito por el riesgo de sus competidores hacen más probable que los cambios radicales provengan desde fuera. Un líder de la industria que reconoce este patrón de innovación disruptiva, pero que no es capaz de identificar la tecnología disruptiva potencialmente exitosa (y obtener las utilidades para él mismo) puede preferir bloquear completamente las nuevas tecnologías. Si ese líder de la industria puede hacerlo sirviéndose de la propiedad intelectual, puede preservar su propia posición por un poco más de tiempo, a expensas de denegar al público de las oportunidades que importan estas mejoras tecnológicas. Requiere menos visión la búsqueda de estabilidad a través del bloqueo de innovaciones de terceros, que tener que innovar uno mismo.

Tanto el VCR como el MP3 pueden ser considerados como tecnologías disruptivas. La calidad y capacidad de grabación inicial del sistema Betamax lo convertían en una alternativa pobre para las emisoras de televisión y estudios de cine para uso interno, pero para lo televidentes sin más opciones para grabar *shows*, la mala calidad era mejor que nada (Lardner, 1987: 95-7).[163] Mientras que la calidad mostraba ser lo suficientemente buena, y ésta mejoraba, una red virtual de propietarios de VCR se desarrolló, proveyendo oportunidades para el arriendo de películas también.[164] Del mismo modo, el audio comprimido del MP3 fue des-

163. Este argumento, que considera en conjunto a Betamax y al VHS, es distinto al debate referente al triunfo del VHS sobre el formato Beta, ilustra la dependencia del camino. Véase Liebowitz y Margolis (1995).

164. Véase Lardner (1987: 312-209. Respecto a los efectos de la red en la tecnología, véase Shapiro y Varian (1998).

cartado como inferior para escuchar música por los audiófilos, pero su menor tamaño de archivo lo hizo popular entre los fanáticos, que podían «extraer» archivos MP3 en reproductores de música e intercambiarlos a través de conexiones a Internet más lentas (Levy, 2006; Levine, 2007). Con el tiempo, por supuesto, ambas encontraron amplias audiencias.

La respuesta de las compañías de entretenimiento tanto al VCR como al MP3, a medida que fueron volviéndose populares, fue similar a su reacción frente a nuevas tecnologías bajo la DMCA: intentar aplacarlas a través de demandas.[165] Sin embargo, ninguna de las leyes de autor existentes en esa época les dio la razón. La Corte Suprema estableció que Sony no era responsable por permitir una combinación de usos de su sistema Betamax, que no podían ser considerados como no infractores de los derechos de autor, o podían ser encuadrados dentro del *fair use* o, en algunos casos, ser considerados efectivamente como infracciones. En su lugar, la Corte determinó que un dispositivo «capaz de usos sustancialmente no infractores», incluyendo la práctica de «diferir horarios» de transmisiones televisivas, era legal su comercialización.[166]

El Diamond Rio, introducido al mercado en 1998, ofrecía a los usuarios almacenamiento portátil para archivos MP3, equivalentes a una hora de reproducción, importados desde un computador (Levy, 2006: 27). La RIAA demandó, alegando que el dispositivo violaba las disposiciones de la Ley de Grabaciones Caseras de Audio (AHRA).[167] La Corte de Apelaciones del Noveno Circuito rechazó los argumentos en base a fundamentos estatutarios: La ley AHRA requiere que los «dispositivos de grabación digital» contengan una serie funciones de gestión de derechos de autor que impidan la copia de segunda generación de la copia, pero debido a que el Diamond Rio obtuvo su música a través de una computadora personal (y no de un dispositivo de copia de música) se encontraba fuera del ámbito de aplicación de la ley AHRA.[168] Esta sentencia correctamente determinó el ámbito de la ley AHRA a dispositivos digitales especialmente

165. Por ejemplo, *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984); *Recording Industry Ass'n of Am. v. Diamond Multimedia Sys. Inc.*, 180 F. 3d 1072 (9th Cir., 1999).

166. *Sony*, 464 U.S. pág. 456.

167. *Diamond*, 180 F. 3d, pág. 1075.

168. *Diamond*, 180 F. 3d, pág. 1078.

dedicados a la grabación de audio, en lugar de exigir que cada computador, de uso general, sea restringido a vigilar y responder frente a marcas de agua anticopia. En el caso Diamond Rio, la Corte determinó que la característica de «cambiar el lugar» del dispositivo no infringía los derechos de autor: «de hecho, la forma en que opera el dispositivo Rio es completamente consistente con el propósito principal de la ley, la facilitación del uso personal».[169] Los titulares de derechos de autor antes de la DMCA no podían reclamar control sobre los usos personales, incluso si estos incidentalmente involucraran una copia.

Estas tecnologías provocaron una disrupción de los modelos de negocios existentes de producción y distribución de entretenimiento, a la vez que proveían al público de mayor arte y entretenimiento. Bajo las leyes de derecho de autor anteriores, las compañías en el negocio del entretenimiento debían adaptarse o fracasar. Pero frente aquello que la ley de derechos de autor no podría controlar, las normas antielusión entregan nuevas armas para luchar en su contra.

Aunque todavía puede accederse a música a través de CD sin cifrar, sin la carga de medidas de tecnológicas de protección la innovación sobre y alrededor de otros tipos de contenido se ha vuelto cada vez más difícil. La diferencia que ha provocado la DMCA ha sido aparente desde el primer caso decidido bajo el nuevo sistema normativo, en el año 2000: Real Networks versus Streambox.[170] Streambox desarrolló el *VCR Streambox,* un *software* para reproducir y almacenar transmisiones de video en formato *Real*, el que hasta ese entonces era el formato dominante de video. Real demandó por elusión y ganó. Para recibir los videos de *RealNetworks,* el *VCR Strambox* debía imitar el «código secreto» del cliente del reproductor Real, una conducta que la Corte de distrito determinó que constituía una elusión.

A lo menos parte del *VCR Streambox* elude las medidas tecnológicas de protección que RealNetworks asegura a los titulares de derechos de autor. Donde un archivo RealMedia es almacenado en un RealServer, el *VCR Streambox* pasa por alto el código secreto para acceder al archivo. El VCR entonces elude las limitaciones de copia, permitiendo al usuario

169. *Diamond*, 180 F. 3d, pág. 1079.

170. *RealNetworks, Inc. v. Streambox, Inc.*, No. C99-2070P, 2000 U.S. Dist. Lexis 1889 (W.D. Wash. Jan. 18, 2000).

hacer una copia de un archivo que el titular de derecho de autor busca proteger.[171]

En contraste al mundo antes de la DMCA, cuando los estudios no pudieron detener al Betamax,[172] ahora bastaba que Real señalara que su código secreto (no tan secreto, ya que cada cliente de dichos contenidos lo conocía) y código de copia, eran medidas tecnológicas para ganar una medida precautoria en contra del *VCR Streambox*. Los usuarios que querían diferir el tiempo en el cual accedían a videos en línea —y las compañías que querían ofrecerles esa y otras opciones, más allá de las posibilidades de Real— quedaron sin opción.[173]

Otros innovadores disruptivos han logrado negociar con los que controlan los derechos de autor del entretenimiento: la tienda de música iTunes de Apple se convirtió en la primera tienda de música exitosa, luego que varias compañías de música lo intentaran y fallaran (Levy, 2006: 168-70). Apple pudo obtener licencias de derecho de autor, y luego, valiéndose de la DMCA, crear un formato con el que otros no pudieran interoperar (Burrows, 2008). A través de esa combinación, Apple podía utilizar la música para vender sus reproductores de música iPod, los únicos con «autorización» para decodificar las pistas en formato AAC, y entonces excluir a otros innovadores de esa tajada del mercado.[174]

Aunque la disrupción es dolorosa para aquellos negocios que se quedaron atrás, generalmente beneficia a los usuarios finales. A través de la

171. *RealNetworks, Inc. v. Streambox, Inc.*, pág. 20.

172. Véase *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

173. La Corte que decidió el caso Streambox determinó que la DMCA eliminaba la defensa de «usos legítimos sustanciales». «La defensa principal de Streambox es que el VCR tiene usos legítimos… [pero] los fabricantes de equipos en el siglo XXI deberán probar que sus productos se encuentran acorde a lo dispuesto en la sección 1201 de la DMCA, para evitar alegaciones de elusión, en lugar de negar alegaciones de derecho de autor como en el caso Sony». Idem, citando a David Nimmer, Nimmer On Copyright § 12A.18[B] (1999 Supp.).

174. La reciente decisión de Apple de eliminar los DRM de su tienda iTunes no contradice esta historia. Los DRM servían para encerrar al principio a los usuarios en un entorno Apple, a medida que el iPod iba creciendo en popularidad, pero ahora molesta a aquellos mismos usuarios, en la medida que intentan mover sus pistas de música a través de un número creciente de productos Apple. Mientras tanto, la compatibilidad con *softwares* hechos a la medida y con dispositivos periféricos, sirve ahora para perpetuar este encierro (cf. Stone, 2009).

competencia obtienen acceso a una gama más amplia de productos, mejor adaptados a sus necesidades, ya sea en selección de características o precio (Viscusi, Harrington y Vernon, 2005). Los clientes que no puedan atraer la atención de productores importantes, en cuya escala sólo constituyen una cantidad insignificante de clientela, pueden encontrar en otra parte a un proveedor que los vea como oportunidades para entrar en un nuevo mercado. Algunos aspirantes a disruptores fallan, por supuesto, pero a mayor número de innovadores que puedan intentarlo cuando las barreras de entrada son más bajas, mayores son las oportunidades para éxitos inesperados.[175]

Armados con las leyes antielusión, sin embargo, las compañías de medios digitales pueden atrincherarse en contra de la disrupción de tales advenedizos. Al negar la crítica «autorización» a cualquiera que pueda operar en forma diferente, los actuales controladores pueden dejar fuera a posibles retadores. Menos innovadores autorizados significa menos emprendedores libres para perseguir sus propios experimentos en aquello que los mercados y el público pudieran apoyar. El requisito de autorización previa, y la posibilidad que ese permiso sea denegado o sujeto a condiciones, impone un obstáculo que detendrá a muchos. Particularmente en el entorno de los medios digitales, en donde muchos son frustrados por la lenta adopción de nuevas tecnologías por parte de las compañías de entretenimiento, es el público quien en definitiva pierde cuando se prohíbe la experimentación a los competidores.

Aun cuando las circunstancias son malas para compañías que podrían ser disruptivas, éstas son peores para individuos o para aquellos que buscan la innovación de los usuarios finales. Aunque la innovación todavía es posible para aquellos que logran convencer a los controladores del mercado que compartirán las ganancias, la innovación por parte del usuario final queda completamente recluida en los ámbitos donde

175. La innovación distribuida funciona entonces como un portafolio diversificado de opciones, entregando mayores oportunidades para tener éxito, en un escenario de incertidumbre. Algunos podrían alegar que los incentivos para competir son menores cuando la ganancia potencial es menor. Sin embargo, como veremos, las motivaciones para innovar son más variadas que sólo el tamaño de las ganancias, sugiriendo que la innovación y el emprendimiento continuarán floreciendo incluso si no puede asegurar un resultado en donde el ganador se lo lleva todo.

existan medidas tecnológicas de protección funcionando. Las reglas de blindaje excluyen cualquier tipo de diseño en base a código abierto, o accesible al usuario.

C) LOS DRM LIMITAN LA INNOVACIÓN DE USUARIO

Eric von Hippel ha liderado el campo de la investigación acerca de la forma en la que los usuarios, y no sólo los fabricantes, mejoran e innovan los productos que utilizan (Von Hippel, 2005, 1988). Debido a que están más cerca de sus problemas y se benefician directamente de sus soluciones, los usuarios finales suelen tener mejor información y una mayor motivación para mejorar los productos que los propios fabricantes de éstos. Como concluye von Hippel, de diez a cuarenta por ciento de los usuarios, a través de una amplia gama de áreas, participan en el desarrollo o modificación de productos, y no sólo «consumiéndolos» (2005: 20).

Al innovar por sí mismos, los usuarios finales pueden obtener productos no disponibles en el mercado, productos que pueden no estar disponibles porque los fabricantes no han llegado a ese punto todavía, o porque no es rentable para los fabricantes ofrecer la variedad de productos requerida por las preferencias individuales de cada uno de sus usuarios. Una vez que algunos usuarios han demostrado el valor de las innovaciones y su potencial comercial, sin embargo, los fabricantes o una comunidad de usuarios podrían desarrollarlos a una escala mayor. Von Hippel y sus colegas han encontrado este patrón de innovación de usuario de la misma forma en negocios y en productos de consumo, en campos que van desde instrumentos científicos y médicos, a bicicletas de montaña y kayaks (von Hippel, 1988; Hienerth, 2006; Lüthje, Hersttat y von Hippel, 2005).

El entorno tecnológico actual es particularmente fértil para la innovación de usuario en todos los productos de consumo, particularmente en los medios digitales. Internet reduce los costos de comunicación, permitiendo a las comunidades de usuarios compartir información y desarrollo a más bajo costo y más rápido (Zittrain, 2006: 1988). Cuando el producto se compone de bits, Internet también reduce a casi cero los costos de distribución. Los usuarios finales pueden involucrarse con poco capital inicial. Hemos visto que la cultura «hágalo usted mismo» se re-

vigorizó a medida que la gente aprendió a manejar la complejidad de la tecnología informática y aprovecharla para sus propios fines: la innovación de usuario está habilitada y se manifiesta en proyectos electrónicos y mecánicos de naturaleza «hágalo usted mismo», desde *Make Magazine* y sus ferias *Maker* hasta *Lego Mindstorms*.[176] En línea, la World Wide Web ha acelerado el desarrollo de la expresión, el *software* y de las aplicaciones web híbridas (blogs, *scripting*, fotografía, video y cartografía, por nombrar algunas) (Zittrain, 2006: 1994). Yochai Benkler (2002) sugiere que estas condiciones de toma de decisiones descentralizadas permiten que la producción entre pares basada en la igualdad de acceso, mejoren respecto a esquemas basados en el mercado y en la organización jerarquizada.

La creciente popularidad del *software* de código libre y abierto refleja el interés existente en productos accesibles para el usuario, proporcionando herramientas para ello. Con el código fuente disponible y modificable libremente, los usuarios pueden configurar los productos de *software* o contratar a consultores independientes para hacerlo por ellos, incluso cuando sus requerimientos de modificación no alcanzan la escala o la rentabilidad suficiente para interesar a un proveedor comercial. Tanto los aficionados como los proveedores comerciales han estado dispuestos a compartir el código fuente de sus programas computacionales, a menudo colaborando en el mismo proyecto. Mientras que sus motivos pueden ser diferentes, los usuarios-productores de ambas clases reconocen el valor de permitir la investigación y la modificación por parte de los usuarios finales (Lakhani y Wolf, 2005; Lerner y Ritole, 2002).

La innovación de usuario no es sólo una interesante fuente alternativa de productos, sino que también aumenta el valor social. Joachim Henkel y Eric von Hippel «concluyen que un sistema de innovación donde existe la innovación de usuario provoca un mayor nivel de bienestar que en aquellos sistemas donde no existe» (2004: 74). Incluso si evaluamos sólo el valor agregado, el ingreso total por parte de una sociedad y no su distribución, los productos en donde ha existido innovación de usuario

176. «Los geeks Alpha ejecutan una idea o dispositivo, la empujan más allá de sus límites, la reinventan y eventualmente allanan el camino a emprendedores que vislumbran la forma de crear versiones comercializables de esas nuevas ideas» (O'Reilly, 2009); *Makezine.com*, About Make, <http://makezine.com/about/>.

tienden a satisfacer a sus consumidores de forma más precisa, dejando menos peso muerto en la falta de correspondencia habitual entre el producto y su función (Henkel y von Hippel, 2004: 78). La innovación de usuario está menos sujeta a los «efectos de excedente del consumidor», que puedan limitar los incentivos de los fabricantes a innovar cuando sienten que no serán capaces de capturar la valor total de nuevos productos; siendo productores y consumidores a la vez, los usuarios-innovadores no sienten la pérdida de este efecto. La innovación de usuario, por lo tanto, aumenta el bienestar social a través de diferentes vectores, incluyendo mejores productos, mejores índices de I + D, y, lo que no debe subestimarse, el disfrute de la innovación en sí misma (Henkel y von Hippel, 2004: 78).

En primer lugar, la innovación de usuario puede producir, en forma directa, productos de mayor valor. Es decir, los usuarios-innovadores pueden convertirse en fuentes de productos, para ellos mismos o para otros, a través de intercambios no comerciales, o de emprendimiento empresarial. Ellos aportan nuevos productos o versiones mejoradas de productos existentes, a menudo, de productos que no habrían sido creados, o a lo menos, no tan pronto o no con los mismos atributos, si el desarrollo tuviese un carácter comercial o impulsado por oferentes comerciales (von Hippel, 1988: 14-5). Los usuarios tienen ventajas en el desarrollo, como la capacidad para implementarlos rápidamente para mejorar y responder a las necesidades cambiantes. Tienen mejor información sobre lo que ellos necesitan sin filtrar esas necesidades a través de barreras de comunicación interdisciplinarias, ni solventar los costos asociados a la desagregación de información «pegajosa» (Henkel y von Hippel, 2004: 75; von Hippel, 1994: 430).

Eric Raymond, programador informático y defensor del código abierto, explica por qué empezó a desarrollar el programa *fetchmail*:

> Necesitaba un cliente POP3. Así que busqué en Internet y encontré uno. En realidad, me encontré con tres o cuatro. Usé uno de ellos por un tiempo, pero faltaba lo que parecía una característica evidente, la capacidad para «hackear» las direcciones de correo recogido para que las respuestas funcionasen correctamente. Esto era claramente algo que el computador debería estar haciendo por mí. ¡Sin embargo, ninguno de los clientes POP existentes sabía cómo hacerlo!» (2001: 23).

Trabajando para «rascar su picazón de desarrollador», y solicitando los informes de fallos y las contribuciones de código de otros usuarios-desarrolladores, Raymond transformó su trozo de código en un programa de entrega de correos electrónicos robusto, adaptado a las características que él y la comunidad necesitaban en la práctica (2001: 23-7).

Eric von Hippel cuenta historias similares de innovación, desde químicos clínicos diseñando sus propios ensayos para fines de investigación, a ciclistas de montaña, construyendo o modificando su equipamiento (von Hippel, 1988: 11; Lütje, Hersttat y von Hippel, 2005: 951). Más de la mitad de los resultados experimentales reportados en la literatura química, deriva de pruebas diseñadas y adaptadas por usuarios (von Hippel, 1988: 11). Diecinueve por ciento de entusiastas de las bicicletas de montaña reportaron haber desarrollado y construido componentes para sus equipos, a menudo utilizando habilidades provenientes de *hobbies* o de sus profesiones (Lütje, Hersttat y von Hippel, 2005: 961-2).

Así, los usuarios, ya sea en su papel de aficionados, científicos profesionales o programadores, a menudo construyen o adaptan herramientas para su propio uso, para atender necesidades previamente insatisfechas. Algunos usuarios se convierten en desarrolladores-distribuidores, como Raymond lo hizo manteniendo el cliente *fetchmail* para una creciente base de usuarios. Sus innovaciones pueden más tarde ser seguidas y compartidas con otros usuarios en situaciones similares.

En segundo lugar, los usuarios finales pueden contribuir a la innovación comercial indirectamente, sirviendo como laboratorios de investigación de los proveedores comerciales. Incluso cuando los usuarios finales no producen en gran escala, sus innovaciones pueden ser adoptadas por empresas establecidas. Como lo describe von Hippel, esta difusión se ve facilitada porque los usuarios-innovadores a menudo «revelan libremente» sus mejoras, ya sea porque es más conveniente hablar abiertamente que hacerlo en secreto, o porque ganan más de la facilidad con que otros usuarios pueden contribuir que lo que ganarían en un entorno competitivo. Especialmente si ellos mismos no planean producir el producto comercialmente o utilizarlo como un componente clave de un proceso comercial, los usuarios finales pueden no ver inconvenientes en esta revelación —y ninguna ventaja en el secreto comercial que justifique los costos de mantener secretos— y pueden ver los beneficios que sus pequeños esfuerzos sean adoptados con fines comerciales (Lüt-

je, Hersttat y von Hippel, 2005: 954). Así, los usuarios de *software* de código abierto a menudo contribuyen de vuelta con modificaciones en forma de parches a la fuente matriz (Lakhani y von Hippel, 2003: 926). Junto con el reconocimiento y las ventajas en materia de reputación, los contribuyentes pueden ahorrarse trabajo, obteniendo una mejor garantía de compatibilidad continua con una gama más amplia de posibles aplicaciones complementarias,[177] atrayendo «más ojos» a sus errores y, quizás, mejorando más aún los arreglos. Las pruebas desarrolladas independientemente por los químicos clínicos están ahora disponibles para su compra, preempaquetadas por sus desarrolladores y la comunidad científica en general. La libre revelación permite a los usuarios obtener tanto apoyo no comercial como comercial y las firmas comerciales que aporten su experiencia en materia de fabricación y distribución a gran escala, usando a la comunidad de usuarios líderes como un banco de pruebas o un laboratorio de investigación de campo.

Además, el proceso de innovación en sí puede ser gratificante para el usuario-innovador, pues ofrece un sentido de comunidad, estimulación intelectual y el desarrollo de nuevas habilidades, y una vinculación con la tecnología (Benkler, 2007: 122-7; Dibona, Ockman y Stone, 1999).[178] Un compromiso con el desarrollo puede hacer a los usuarios más felices con los resultados al modificar las expectativas base de los productos: un usuario puede estar más satisfecho con un producto hecho o mejorado por él mismo y más indulgente de los errores que pueda tener, que si hubiera obtenido el mismo producto en el comercio (von Hippel, 2005: 33-43).

Además de las diferencias en la calidad y variedad de los productos y servicios desarrollados, la innovación de usuario produce beneficios distributivos. La distribución de la riqueza y el acceso puede ser más justa en un ambiente abierto a la innovación de los usuarios que en una cerrada a ésta. El acceso puede ser más democrático y abierto a aquellos con tiempo disponible y recursos limitados (y que ofrecen nuevas formas de

177. En materia de *software*, los parches de contribución a la base de código principal ahorra a los desarrolladores el trabajo de reaplicar los parches con cada nuevo lanzamiento.

178. Véase en general Ed Felten y otros, «Freedom to Tinker», en <http://freedom-to-tinker.com>.

iniciativa empresarial mediante la cual las personas pueden convertir el tiempo en dinero). Especialmente los usuarios con necesidades especiales estarán mejor atendidos a través de la autoinnovación. Por otra parte, el usuario-innovador se sentirá inclinado a pensar en sí mismo como más que un mero consumidor y, quizás, se sienta más involucrado en la forma en que se gobierna el entorno de la información.[179]

Esa sociedad en su conjunto está mejor cuando los campos están abiertos a la innovación de usuario pero, sin embargo, no asegura que existan los incentivos para que un suficiente número de participantes los provean. Mientras que algunas compañías han reconocido las oportunidades que entrega la innovación de usuario (IBM, reconocidamente contribuye a la plataforma Linux porque mejores programas computacionales, abiertamente distribuidos y de código abierto, es mejor para su *hardware* propietario; véase Berlind, 2002), otras se sienten amenazadas por la posible competencia. Ellas pueden temer perder la ventaja del primer movimiento que otorgan los secretos comerciales o preferir los ingresos por licencias a su ausencia (por ejemplo, licenciar una cantidad más pequeña de tecnología en lugar de fabricar una parte de un mercado más grande u obtener ingresos accesorios; véase Eisenmann, 2008: 5). Jonathan Zittrain (2008) sugiere que incluso los usuarios reaccionarán contra la generación de plataformas abiertas si esas plataformas fuesen más fácilmente operadas por malos actores.[180]

Para aquellos reticentes a que la innovación actúe en su contra, las medidas antielusión han probado ser un poderoso medio para bloquear la innovación de usuario, ya sea deliberada o incidentalmente. La innovación de usuario depende de la apertura y accesibilidad de los productos respecto de los cuales se pretende hacer la innovación.[181] Christina

---

179. Esta autora usa el término gobierno como referencia a *Governing the commons* (1990) de Elinor Ostrom, para significar la organización voluntaria para superar los problemas colectivos y administrar los recursos comunes. [En español, Elinor Ostrom, *El gobierno de los bienes comunes*, Fondo de Cultura Económica, México, 2011.]

180. Entonces no podemos invocar la mano invisible para preguntar, «¿si es tan bueno, por qué no ha sucedido todavía?»

181. Las características que hacen que un producto sea idóneo a la innovación de usuario son similares a aquellos que Zittrain (2006: 1981) identifica como claves a la capacidad «generativa» de una tecnología: capacidad para apalancar, adaptabilidad, facilidad de dominio, y accesibilidad. Donde algunas de las características de la «gene-

Raasch (2008: 390) describe el impacto de la accesibilidad técnica en el desarrollo de veleros de carreras «International Moth». Esta clase de bote se encuentra marcada por un alto grado de innovación de usuario, pero a medida que la complejidad tecnológica de los materiales del casco de estos botes aumentó (en un cambio de madera a fibra de plástico reforzada a fibra de carbón), la mayoría de los usuarios dejaron de innovar en el diseño del casco, aunque continuaron innovando en otras partes de los botes. Las reglas de blindaje de forma similar aumentan las barreras a la innovación de usuario en la tecnología de medios.

D) LOS COSTOS GLOBALES: LOS DRM CENTRALIZAN LA INNOVACIÓN, EN CONTRA DE LOS OBJETIVOS ORIGINALES DE LAS LEYES DE DERECHO DE AUTOR

Contrario a uno de los objetivos centrales del derecho de autor, las medidas antielusión centralizan la facultad decisional de autoridad. El derecho de autor, como un todo, descentraliza las elecciones respecto a los tipos y las cantidades de obras creativas que debieran ser producidas. Al ofrecer derecho de propiedad de exclusión, el derecho de autor permite el establecimiento de mercados de las obras creativas, a pesar de la naturaleza básicamente no excluyente que tiene la expresión creativa (Gordon, 1982: 1610-2). Los mercados descentralizan la toma de decisiones (Hayek, 1945: 526): en lugar de esperar por el Ministro de Cultura de un Estado o por un mecenas que financie una nueva obra cinematográfica, Walt Disney puede escuchar las demandas de millones de niños que quieren películas de princesas y la de sus padres indulgentes. El derecho de autor tradicional entonces permite a los productores de obras creativas en el campo de las artes, la literatura y la música, organizarse para satisfacer lo que ellos perciben ser los intereses de sus audiencias (Wu, 2006: 146-7). En un mundo de información imperfecta, la descentralización nos entrega más oportunidades para cumplir los intereses de los consumidores y una oportunidad más democrática para servirlos.[182] Tim Wu sugiere que

---

ratividad», particularmente la «capacidad de apalancar», se encuentran dirigidas a la creación de algo distinto, utilizando la tecnología, la innovación de usuario se enfoca en cambiar el producto tecnológico directamente.

182. Incluso aquí, el derecho de autor no es sin costo. Los economistas discuten las

los regímenes de propiedad intelectual debieran ser examinados por sus efectos sobre la estructura en la toma de decisiones (2006: 123-4).

Junto con los beneficios económicos de permitir que los mercados organicen la producción y permitan la innovación disruptiva, la descentralización tiene un valor social y cultural. Ayuda a producir un ambiente de información democrático, en donde cualquiera es un creador y consumidor en potencia (Fisher, 2004), una cultura de leer y escribir (Lessig, 2008: 28). Permite a los usuarios organizarse a sí mismos, en los términos de Yochai Benkler «producción de iguales basada en los comunes» (2002: 376).

Mientras que el derecho de autor descentraliza la producción independiente, algunos también han notado que centraliza el control sobre la expresión consecuencial. A través de los derechos exclusivos existentes sobre la reproducción y las obras derivadas, el creador inicial puede controlar el uso de su obra si tal uso excede el *fair use* (Boyle, 2008; Bambauer, 2007; Benkler, 1999; Nadel, 2003). Ahí, ellos concluyen, los problemas se tornan más serios (alza de costos contra los beneficios) donde las restricciones de los derechos de autor se vuelven más severas, aplicables a más conductas y de duración más extensa.[183]

Aun si el derecho de autor básico, al crear mercados, descentraliza a lo menos la producción independiente de obras expresivas, las normas antielusión de la DMCA centralizan el control de las tecnologías que funcionan con estas obras, cambiando un set de problemas de coordinación por otro. Donde celebramos al «autor romántico» del derecho de autor y la resistencia a la toma de decisiones centralizada respecto de obras de expresión creativa (Coombe, 1988: 219), hemos a la vez centralizado la innovación alrededor de los medios tecnológicos para disfrutar los textos, sonidos y películas creadas.

---

ventajas y desventajas existentes entre costos estáticos y beneficios dinámicos. Nosotros aceptamos la ineficiencia de monopolios existentes sobre obras individuales a cambio de la innovación derivada de la competencia entre éstos sobre el mercado más amplio del entretenimiento.

183. Para un análisis ficticio de los problemas derivados de esta extensión, ver Spider Robinson, «Melancholy Elephants» (1983), disponible en http://www.spiderrobinson.com/melancholyelephants.html, que describe un futuro en donde nada puede ser compuesto debido a que todo lo imaginado es demasiado similar a obras bajo un dominio privado perpetuo.

Wu realiza una crítica similar a la «política de comunicaciones» del derecho de autor, interpretando a la actual ley como un producto de las actividades de búsqueda de ingresos realizadas por los diseminadores dominantes del mercado, para dejar fuera de éste a posibles advenedizos (2004: 325-8). El patrón se ajusta a las medidas antielusión, ayudando a explicar la expansión de la zona de autorización y control desde los autores de obras protegidas, a desarrolladores de tecnologías de protección de copia. No sólo los autores y los titulares de derechos de autor buscan obtener todas las rentas posibles de sus creaciones, los no autores tratan de usar derechos de autor ajenos como una garantía de ganancias. En el mercado centralizado, unas pocas compañías de medios (Patry, 2009: 173) pueden hacer uso del poder de mercado continuado, a través de sus catálogos de obras, para impedir que los desarrolladores de tecnologías y competidores independientes puedan inventar nuevos modelos de uso de medios digitales.

6. CONCLUSIONES

Cuando otorgamos control antielusión a los titulares de derechos de autor, eliminamos un conjunto de posibilidades y un espacio de soluciones a los desafíos que presenta el intercambio cultural y la productividad técnica.[184] Es difícil cuantificar aquello que aún no existe,[185] pero a partir de comparaciones respecto de otros mercados menos regulados, y del pasado no tan distante de la tecnología de medios, han sugerido varias razones para preferir la apertura.

Las normas antielusión de la DMCA centralizan la producción de la tecnología de reproducción de medios, entregando a los titulares de derechos de autor, la facultad de autorizar, o prohibir, la interoperabilidad con sus obras protegidas. Este es un nuevo fenómeno. En el «viejo mundo» del derecho de autor, una vez que el titular de derecho había ejercido sus derechos de primera venta, el público adquiría la facultad y la oportunidad de usar la obra en una variedad de formas que no involucraban derechos de autor.

184. «La mayoría [de las tecnologías de propósitos generales] juegan el rol de 'tecnologías habilitadoras', abriendo nuevas oportunidades en lugar de ofrecer soluciones completas y finales» (Bresnahan y Trajtenberg, 1995: 84).

185. Y más difícil aún realizar lobby a favor de tecnología pendiente de ser inventada.

Las medidas antielusión cierran las fronteras de la innovación de medios. La frontera abierta no es sólo una posibilidad específica, sino que una inspiración, una invitación a explorar.[186] No todos quienes buscaron oro en California lo encontraron, pero sus exploraciones alimentadas por el riesgo establecieron el escenario para el desarrollo comercial del oeste norteamericano. En el curso de la exploración y el mapeo del espacio, los innovadores pueden hacer descubrimientos inesperados y encontrar nuevas fuentes de riqueza. Incluso si no encuentran oro, la exploración del espacio puede dar lugar a otras innovaciones de gran valor agregado.

Las medidas antielusión alientan a los titulares de derechos de autor a estacar la frontera de la innovación tecnológica con letreros de «no cruzar», no porque ellos hayan explorado y utilizado el territorio de forma productiva, sino porque sienten como una amenaza que otros lo hagan. Las medidas antielusión envían un mensaje a los desarrolladores, tanto comerciales como usuarios-innovadores, que ciertas actividades y oportunidades se encuentran no permitidas, que incluso si es técnicamente posible mejorar la interoperabilidad con una amplia variedad de medios, les está prohibido hacerlo sin una autorización previa. Los caprichos (y los costos de transacción) de los mecanismos de otorgamiento de licencias disuaden a los innovadores, como asimismo el prospecto de tener que compartir los beneficios.

Las normas antielusión sirven como ley pública que hace cumplir normas de carácter privado, de prohibir la distribución de innovación de usuario. Como una materia de diseño regulatorio, esta clase de regulación arquitectónica externaliza los costos. Permite a aquellos que reciben los beneficios, un grupo de titulares de derechos de autor, pretender que el imperfecto sistema de DRM es bueno, mientras que impone un impuesto al «modo de desarrollo» sobre todo el público. En todo el análisis costo-beneficio de las medidas antielusión, la pérdida de la innovación de usuario abierta supera las ganancias provenientes de este sistema imperfecto de coerción de derechos de autor. Tratar al código literalmente como ley deja al ordenamiento jurídico con demasiados efectos secundarios dañinos.

186. Turner (1921) atribuía el éxito democrático a la disponibilidad de un «dominio público» de tierra libre.

REFERENCIAS

Armstrong, Timothy K. (2006). «Digital Rights Management and the Process of Fair Use». *Harvard Journal of Law & Technology*, 20 (1): 49-121.

Anderson, Chris (2006). *The Long Tail. Why the Future of Business is Selling Less of More*. Nueva York: Hyperion.

Aufterheide, Patricia, y Peter Jaszi (2004). *Untold Stories. Creative Consequences of the Rights Clearance Culture for Documentary Filmmakers*. Disponible en <http://www.centerforsocialmedia.org/files/pdf/untoldstories_report.pdf>.

Baldwin, Carliss Y., y Kim B. Clark (2000). *Design Rules. Vol. 1: The Power of Modularity*. Cambridge: The mit Press.

Bambauer, Derek (2007). «Faulty Math: The Economics of Legalizing 'The Grey Album'». Alabama Law Review, 59.

Bell, Tom (1998). «Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine». *North Carolina Law Review*, 76.

Benkler, Yochai (1999). «Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain». *New York University Law Review*, 74.

— (2001). «The Battle over the Institutional Ecosystem in the Digital Environment». *Communications of the acm*, 44 (2): 84-90.

— (2002). «Coase's Penguin, or Linux and The Nature of the Firm». *Yale Law Journal*, 112.

— (2003). «Freedom in the Commons. Towards a Political Economy of Information». *Duke Law Journal*, 52.

— (2007). *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. Yale University Press.

Berlind, David (2002). «Open Source: ibm's Deadly Weapon, zdnet». 8 de abril. Disponible en <http://news.zdnet.com/2100-10532_22-296366.html>.

Biddle, Peter y otros (2002). «The Darknet and the Future of Content Distribution». En Joan Feigenbaum (ed.), *Digital Rights Management Workshop*. Washington: acm.

Bower, Joseph L. y otros (1995). «Disruptive Technologies: Catching the Wave»,. *Harvard Business Review*, enero-febrero.

Boyle, James (2008). *The Public Domain: Enclosing the Commons of the Mind*. New Heaven: Yale University Press.

Bresnahan, Timothy F. y Manuel Trajtenberg (1995). «General Purpose Technologies: 'Engines of Growth'?», Journal of Econometrics, 65.

Bryers, Simon y otros (2003). «Analysis of Security Vulnerabilities in the Movie Production and Distribution Proces's». En Moti Yung (ed.), *Digital Rights Management Workshop*. Washington: acm.

Burk, Dan L., y Mark A. Lemley (2009). *The Patent Crisis and How the Courts Can Solve It*. Chicago: University Of Chicago Press.

Burk, Dan L., y Julie E. Cohen (2001). «Fair Use Infrastructure for Rights Management Systems». *Harvard Journal of Law & Technology*, 15 (19): 41-83.

Burrows, Peter (2008). «DoubleTwist is Dancing in Dangerous Legal Territory». *Business Week*, 19 de febrero. Disponible en <http://www.businessweek.com/technology/ByteOfTheApple/blog/-archives/2008/02/doubletwist_is.html/>.

Christensen, Clayton M. (1997). *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Nueva York: Harvard Business Review Press.

Christensen, Clayton M., y Michael E. Raynor (2003). *The Innovator's Solution: Creating and Sustaining Successful Growth*. Nueva York: Harvard Business Review Press.

Cohen, Julie (1995). «A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace». *Connecticut Law Review*, 28.

— (1998a). «Copyright and the Jurisprudence of Self-Help». *Berkeley Technology Law Journal*, 13: 1089-1143.

— (1998b). «Lochner in Cyberspace: The New Economic Orthodoxy of Rights Management». *Michigan Law Review*, 97 (2).

Coombe, Rosemary (1998). *The Cultural Life of Intellectual Properties: Authorship, Appropriation, and the Law*. Duke University Press Books.

Craver, Scott y otros (2001). «Reading Between the Lines: Lessons from the sdmi Challenge». Disponible en <http://www.usenix.org/events/sec01/craver.pdf>.

Crawford, Susan (2003). «The Biology of the Broadcast Flag». *Hastings Communications and Entertainment Law Journal*, 25 (2): 603-52.

DIBONA, Chris, Sam OCKMAN y Mark STONE (1999). *Open Sources: Voices from the Open Source Revolution*. Sebastopol: O'Reilly Media.

DUNN, Ashley (1998). «The Cutting Edge Gift Guide». *Los Angeles Times*, 30 de noviembre, pág. C6.

EISENMANN, Thomas R., Geoffrey PARKER y Marchall VAN ALSTYNE (2008). «Opening Platforms: How, When and Why?». Harvard Business School, Working Paper nro. 09-030.

ERICKSON, John S., y Deirdre K. MULLIGAN (2004). «The Technical and Legal Dangers of Code-based Fair Use Enforcement». *Proceedings of the IEEE*, 92 (6).

FELTEN, Edward W. (2005). «DRM and Public Policy». *Communications of the Association for Computing Machinery*, 48.

FERNANDO, Gerard, Tom JACOBS y Vishy SWAMINATHAN (2005) «Project dream, an architectural overview». Disponible en <http://www.openmediacommons.org/collateral/DReaM-Overview.pdf>.

FISHER III, William (2004). *Promises to Keep. Technology, Law, and the Future of Entertainment*. Stanford: Stanford Law and Politics.

— (2007). «When Should We Permit Differential Pricing of Information». *UCLA Law Review*, 55.

FOWLER, Geoffrey A. (2009). «An Orwellian Moment for Amazon's Kindle». *Wall Street Journal Blog*, 17 de julio de 2009, disponible en <http://blogs.wsj.com/digits/2009/07/17/an-orwellian-moment-for-amazons-kindle/>.

FOX, Barbara L., y Brian A. LAMACCHIA (2003). «Encouraging Recognition of Fair Uses in DRM Systems». *Communications Assoc. Computing Mach.*, 46: 61-3.

GILLESPIE, Tarleton L. (2006). «Designed to 'Effectively Frustrate': Copyright, Technology, and the Agency of Users». *Journal New Media Society*, 8: 651-69.

—. *Wired Shut. Copyright and the Shape of Digital Culture*. Cambridge: The MIT Press.

GENTILE, Gary (2004). «Studios Eye New Anti-piracy Technology». *USA Today*, 2 de julio. Disponible en <http://www.usatoday.com/tech/news/2004-07-02-anti-piracy_x.htm>.

GINSBURG, Jane (2003). «From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law». *Journal of the Copyright Society of the USA*, 50.

Gordon, Wendy (1982). «Fair Use as Market Failure», *Columbia Law Review*, 82.

Gutmann, Peter (2007). «A Cost Analysis of Windows Vista Content Protection». Disponible en <http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html>.

Hachman, Mark (2009). «TV Digital Rights Management Surfaces Again», *PCMag.com*, 4 de noviembre. Disponible en <http://www.pcmag.com/article2/0,2817,2355382,00.asp>.

Haldermann, J. Alex y Edward W. Felten (2006). «Lessons from the Sony cd drm Episode». Disponible en <https://jhalderm.com/pub/papers/rootkit-sec06.pdf>.

Hayek, F. A. (1945). «The Use of Knowledge in Society». *American Economy Review*, 35.

Henkel, Joachim y Eric von Hippel (2004). «Welfare Implications of User Innovation». *Journal Technology Transfer*, 30.

Hienerth, Christoph (2006). «The Commercialization of User Innovations: The Development of the Rodeo Kayak Industry». *Research & Development Management*, 36.

Huang, Andrew (2003). *Hacking the Xbox. An Introduction to Reverse Engineering*. San Francisco: No Starch Press.

Kling, Arnold, y Nick Schulz (2009). *From Poverty To Prosperity. Intangible Assets, Hidden Liabilities and the Lasting Triumph over Scarcity*. Nueva York: Encounter Books.

Lakhani, Karim, y Eric von Hippel (2003). «How Open Source Software Works: «Free» User- to-user Assistance». *Research Policy*, 32 (6): 923-43.

Lakhani, Karim y Robert Wolf (2005). «Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects». En Joseph Feller, Brian Fitzgerald, Scott A. Hissam y Karim Lakhani (eds.), *Perspectives on Free and Open Source Software*. Cambridge: The mit Press.

Landro, Laura (2008). «Get Set for Laser Videodisks, Round Two». *Wall Street Journal*, 6 de diciembre, pág. b1.

Lardner, James (1987). *Fast Forward: Hollywood, the Japanese, and the Onslaught of the vcr*. Nueva York: W. W. Norton & Co.

Leach, Britt (2007). «Screeners for My Consideration». *Veritas*, 30 de noviembre. Disponible en <http://www.veritas-anydaynow.com/reconsideringscr.html>.

LEMLEY, Mark A. (2008). «Ignoring Patents». *Michigan State Law Review*, 2008 (19).

LEMLEY, Mark A., y Carl SHAPIRO (2006). «Patent Holdup and Royalty Stacking», *Texas Law Review*, 85.

LERNER, Josh y Jean TIROLE (2002). «Some Simple Economics of Open Source», *The Journal of Industrial Economics*, 50.

LESSIG, Lawrence (2000). *Code and Other Laws of Cyberspace*. Nueva York, Basic Books.

— (2005). *Free Culture. The Nature and Feature of Creativity*. Nueva York: Penguin.

— (2008). Remix. Nueva York: Penguin.

LEVINE, Robert (2007). «The Death of High Fidelity». *Rollingstone.com*, 27 de diciembre. Disponible en <http://www.rollingstone.com/news/story/17777619/the_death_of_high_fidelity>.

LEVY, Steven (2006). *The Perfect Thing: How the iPod Shuffles Commerce Culture, and Coolness*. Nueva York: Simon & Schuster.

LEWIS, Stephen (2004). «How Much Is Stronger DRM Worth?» En L. Jean Camp y Stephen Lewis (eds.), *Economics of Information Security*. Boston: Kluwer Academic Publihers.

LIEBOWITZ, S. J. y Stephen E. MARGOLIS (1995). «Path Dependence, Lock-in, and History». *Journal of Law, Economics & Organization*, 11.

LITMAN, Jessica (2001). *Digital Copyright: Protecting Intellectual Property on the Internet*. Prometheus Books.

LÜTHJE, Christian, Cornelius HERSTATT y Eric von Hippel (2005). «User-innovators and 'Local' Information: The Case of Mountain Biking». *Research Policy*, 34.

MACAULAY, Thomas (1952). «Speech Delivered in the House of Commons on the 5th of February, 1841». En *Prose and Poetry* (edición de G. M. Young), Harvard University Press.

MARCOM JR., John (1985). «Sales of Consumer Electronics to Grow Modestly in 1985, Industry Group Says». *Wall Street Journal*, 7 de enero, pág. 7.

MARKS, Dean S., y Bruce H. THURNBULL (1999). *Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses*. Génova: WIPO. Disponible en <http://www.wipo.int/edocs/mdocs/copyright/en/wct_wppt_imp/wct_wppt_imp_3.pdf>.

Messmer, Ellen (2010). «Black Hat: Researcher Claims Hack of Processor Used to Secure Xbox 360, Other Products». *Network World*, 2 de febrero. Disponible en <https://www.networkworld.com/news/2010/020210-black-hat-processor-security.html>.

Meurer, Michael J. (1997). «Price Discrimination, Personal Use and Piracy: Copyright Protection of Digital Works». *University at Buffalo School of Law*, 45: 845-98.

Milian, Mark (2009). «Which 'Avatar' to see? A look at imax, Dolby 3-D, RealD (and, yeah, boring old 2-D)». *Los Angeles Times blog*, 29 de diciembre. Disponible en <http://latimesblogs.latimes.com/herocomplex/2009/12/which-avatar-to-see-a-look-at-imax-dolby-3d-reald-and-boring-old-2d.html>.

Mulligan, Deirdre K., John Han y Aaron J. Burstein (2003). «How drm-based Content Delivery Systems Disrupt Expectations of 'Personal Use'». En Moti Yung (ed.), *Digital Rights Management Workshop*. Disponible en <http://www.law.berkeley.edu/files/Drm_personal_use.pdf>.

Musgrove, Mike (2001). «Everything Seems to Play mp3s Lately». *Washington Post*, 7 de diciembre, pág. e1.

Nadel, Mark (2003). «Questioning the Economic Justification for (and thus Constitutionality of) Copyright Law's Prohibition Against Unauthorized Copying: § 106». AEI-Brookings Joint ctr, Related Publ'n, 3-1. Disponible en <http://www.reg-markets.org/admin/pdffiles/Nadel.pdf>.

Netanel, Neil W. (2001). «Locating Copyright Within the Fair Use in the First Amendment Skein». *Stanford Law Review*, 54.

Nimmer, David (2003). *Copyright: Sacred Text, Technology, and the dmca*. La Haya: Kluwer Law International.

Ohm, Paul (2008). «The Myth of the Superuser: Fear, Risk, and Harm Online», *University of California Davis Law Review*, 41.

O'Reilly, Tim (2009). «Where Real Innovation Happens». *Forbes.com*, 2 de febrero. Disponible en <http://www.forbes.com/2009/02/03/innovation-tim-oreilly-technology-breakthroughs_0203oreilly.html>.

Pash, Adam (2007). «Jailbreak Your iPhone or iPod Touch with One Click». *Lifehacker*, 29 de octubre. Disponible en <http://lifehacker.com/316287/jailbreak-your-iphone-or-ipod-touch-with-one-click/>.

Patrizio, Andy (1999). «Why the Dvd Hack Was a Cinch, Wired».

Wired, 2 de noviembre. Disponible <http://www.wired.com/science/discoveries/news/1999/11/32263>.

Patry, William (2009). *Moral Panics and the Copyright Wars*. Nueva York: Oxford University Press.

Picker, Randal (2003). «From Edison to the Broadcast Flag: Mechanisms of Consent and Refusal and the Propertization of Copyright». *University of Chicago Law Review*, 70.

— (2005). «Copyright and the dmca: Market Locks and Technological Contracts, in Antitrust». En Francois Leveque y Howard Shelanski (eds.), *Antitrust, Patents and Copyrights. EU and US Perspectives*. Cheltenham: Edward Elgar.

Popescu, Alin C. y Hany Farid (2004). «Statistical Tools for Digital Forensics». En Jessica Fridrich (ed.), *Information Hiding*. Nueva York: Springer.

Raasch, Christina, Cornelius Herstatt y Phillip Lock (2008). «The Dynamics of User Innovation», *International Journal of Innovation and Technology Management*, 12.

Raymond, Eric (2001). *The Cathedral and the Bazaar*. Sebastopol: O'Reilly Media.

Reid, Jason F. y William J. Caelli (2005). «drm, Trusted Computing and Operating System Architecture», *ACSW Frontiers '05 Proceedings of the 2005 Australasian Workshop on Grid Computing and e-Research*, 44: 127-36. Disponible en <http://crpit.com/confpapers/crpitv44Reid.pdf>.

Samuelson, Pamela (1999). «Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised». *Berkeley Technology Law Journal*, 14.

— (2001). «Anticircumvention Rules: Threat to Science». *Science*, 293.

Schechter, Stuart E. y otros (2003). «Trusted Computing, Peer-To-Peer Distribution, and the Economics of Pirated Entertainment». Disponible en <http://www.eecs.harvard.edu/~stuart/papers/eis03.pdf>.

Schneier, Bruce (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Nueva York: John Wiley & Sons.

— (2006). «Quickest Patch Ever». *Wired News*, 7 de septiembre. Disponible en <http://www.wired.com/politics/security/commentary/securitymatters/2006/09/71738>.

— (2008). «The Ethics of Vulnerability Research». *Info. Security Mag.* Disponible en <http://www.schneier.com/essay-211.html>.

Schoen, Seth David (2003). «Trusted Computing, Promise and Risk». The Electronic Frontier Foundation. Disponible en <http://www.eff.org/files/20031001_tc.pdf>.

— (2005). «Trusted Computing, Promise and Risk». Disopnible en <http://www.eff.org/files/2003 1001_tc.pdf>.

Seltzer, Wendy (2005a). «The Broadcast Flag: It's Not Just TV». *Federal Communications Law Journal*, 57.

— (2005b). «Why Open Source Needs Copyright Politics». En Chris Dibona, Danese Cooper y Mark Stone (eds.), *Open Sources 2.0: The Continuing Evolution*. Charleston: Nabu Press.

Shapiro, Carl y Hal R. Varian (1998). *Information Rules: A Strategic Guide to the Network Economy*. Nueva York: Harvard Business School Press.

Shapiro, Carl y Hal R. Varian (1998). *Information Rules: A Strategic Guide to the Network Economy*. Nueva York: Harvard Business School Press.

Shirky, Clay (2008). *Here Comes Everybody: The Power of Organizing Without Organizations*. Nueva York: Penguin.

Stefik, Mark (1996). «Letting Loose the Light: Igniting Commerce in Electronic Publication». En Mark Stefik (ed.), *Internet Dreams: Myths, and Metaphors*. Cambridge: The mit Press.

— (1997). «Trusted Systems». *Scientific American*. Disponible en <http://www.sciam.com/0397issue/0397stefik.html>.

Stone, Brad (2009). «Want to Copy iTunes Music? Go Ahead, Apple Says». *New York Times*, 7 enero, pág. B1.

Taub, Eric A. (2001). «Encryption Schemes Aimed at Film Piracy». *New York Times*, 30 de agosto, pág. G6.

Turner, Frederick J. (1921). *The Frontier in American History*.

Viscusi, W. Kip, Joseph E. Harrington y John M. Vernon (2005). *Economics of Regulation and Antitrust*. 4.ª ed. Cambridge: The mit Press.

von Hippel, Eric (1988). *Sources of Innovation*. Nueva York: Oxford University Press.

— (1994). «'Sticky Information' and the Locus of Problem Solving: Implications for Innovation», *Management Science*, 40.

— (2005). *Democratizing Innovation*. Cambridge: The MIT Press.
VON LOHMANN, Fred (2004). «Measuring the Digital Millennium Copyright Act Against the Darknet: Implications for the Regulation of Technological Protection Measures». *Loyola of Los Angeles Entertainment Law Review*, 24.
— (2005). «Licensing in the Digital Age: The Future of Digital Rights Management». *The Fordham Intellectual Property, Media & Entertainment Law Journal*, 15.
— (2008). «Fair Use as Innovation Policy». *Berkley Technology Law Journal*, 23.
— (2010). «Unintended Consequences: Ten Years Under the DMCA». EFF. Disponible en <http://www.eff.org/wp/unintended-consequences-ten-years-under-dmca/>. [Hay versión en español publicada en *Revista Chilena de Derecho Informático*, nro. 4, 2004. Disponible en <http://www.derechoinformatico.uchile.cl/index.php/rchdi/article/viewFile/10671/10949>.]
WATERMAN, David y otros (2007). «Enforcement and Control of Piracy, Copying, and Sharing in the Movie Industry». *Rev. Indus. Org.*, 30.
WU, Timothy (2004). «Copyright's Communications Policy». *Michigan Law Review*, 103.
— (2006). «Intellectual Property, Innovation, and Decentralized Decisions». *Virginia Law Review*, 92.
ZITTRAIN, Jonathan (2006). «The Generative Internet». *Harvard Law Review*, 119: 1974-2040.

SOBRE LA AUTORA

WENDY SELTZER pertenece al Berkman Center for Internet & Society de la Harvard University, y al Silicon Flatirons Center de la University of Colorado Law School, Estados Unidos. Su correo electrónico es <wendy@seltzer.org>. La autora agradece a Yochai Benkler, Michael Carroll, Rashmi Dyal-Chand, Peter Jaszi, Fred von Lohmann, Benjamin Maki Hill, Paul Ohm, Betsy Rosenblatt, Seth David Schoen, Eric von Hippel, Jonathan Zittrain y a los participantes de la Telecommunications Policy Research Conference, Northeastern Law School's Colloquium y del almuerzo en el Berkman Center for Internet & Society.

Este artículo fue publicado originalmente en *Berkeley Technology Law Journal*, vol. 25, 2010, con el título «The Imperfect is the Enemy of the Good: Anticircumvention Versus Open Innovation», y fue traducido al castellano por Sebastián Molina y Bárbara Soto, ayudantes del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, conforme los términos de la licencia Creative Commons Atribución 3.0 utilizada por la autora.