Las Consecuencias No Deseadas: Cinco Años Bajo la Digital Millennium Copyright Act*

Electronic Frontier Foundation

Sumario: 1.- Resumen ejecutivo.- 2.- El origen legislativo de la DMCA.- 3.- Libertad de expresión e investigación científica.- 4.- Fair Use bajo sitio.- 5.- Una amenaza a la innovación y la competencia.- 6.- La DMCA se convierte en una prohibición general de acceso a redes informáticas.- 7.- Conclusión.-

1. Resumen ejecutivo

Desde que fueron adoptadas en 1998, las disposiciones anti-elusión de la Digital Millennium Copyright Act ("DMCA"), codificada en la sección 1201 de la Copyright Act, no han sido empleadas como el Congreso pretendía. El Congreso tenía la intención de detener la piratería de los derechos de autor originada de la vulneración de las medidas de protección antipiratería incorporadas en las obras, y prohibir los mecanismos de "caja negra" que cumplían aquel objetivo.[1]

En la práctica, las disposiciones anti-elusión han sido usadas para sofocar totalmente el desarrollo de actividades legítimas, en vez de detener la piratería sobre los derechos de autor. Como resultado, la DMCA se ha transformado en una seria amenaza para prioridades de orden público.

---

* Traducción desde el inglés de Alberto Cerda Silva, Coordinador Académico del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, revisada por Patrick Humphreys Neumann, Abogado.

1 Para ejemplos de los objetivos del Congreso declarados en la promulgación de la DMCA para sus disposiciones anti-elusión, *vid.* 144 Cong. Rec. H7093, H7094-5 (Aug. 4, 1998); Senate Judiciary Comm., S. Rep. 105-190 (1998) at 29; Judiciary Comm., H. Rep. 105-551 Pt 1 (1998) at 18; House Commerce Comm., H. Rep. 105-551 Pt 2 (1998) at 38.

La Sección 1201 obstruye la Libertad de Expresión e Investigación Científica

La experiencia con la sección 1201 demuestra que ella está comenzando a ser usada para ahogar la libertad de expresión y la investigación científica. El litigio contra la revista *2600*, las amenazas contra el equipo de investigación del profesor de Princeton Edward Felten, y el procesamiento del programador ruso Dmitry Sklyarov han impedido legítimas actividades de periodistas, editores, científicos, estudiantes, programadores y miembros del público.

La Sección 1201 pone en peligro el Fair Use

Mediante la prohibición de todos los actos de elusión, y todas las tecnologías y mecanismos que pueden ser usadas para ello, la sección 1201 otorga a los titulares de derechos de autor el poder para unilateralmente eliminar los derechos de fair use del público. La industria de la música ya ha comenzado a desplegar los "CDs protegidos de copia" que prometen reducir la capacidad de los consumidores para hacer copias legítimas y personales de la música que han comprado.

La Sección 1201 impide la Competencia e Innovación

En vez de fijarse en los piratas, muchos titulares de derechos de autor han manejado la DMCA para obstaculizar a sus legítimos competidores. Por ejemplo, Sony ha invocado la sección 1201 para proteger su monopolio sobre las consolas de vídeo juego Playstation, así como su sistema de "regionalización", limitando a los usuarios de un país para jugar con los juegos adquiridos legítimamente en otro.

La Sección 1201 se convierte en una prohibición general de acceso a redes informáticas

Más aún, la sección 1201 ha sido mal usada, al emplearse como una nueva cláusula general que prohíbe el acceso a redes de trabajo computacional, la que, a diferencia de las varias normativas federales "anti-hacking" que ya protegen a los propietarios de redes informáticas de intrusiones no autorizadas, carece de cualquier umbral de perjuicio económico. El uso de la DMCA por el disgustado ex-empleador Pearl Investment's contra un programador contratado que conectó el sistema de computación de la compañía mediante una password protegida Virtual Private Network ilustra el potencial para que personas inescrupulosas mal usen la DMCA para lograr que no sean posibles regímenes de regulación del acceso a computador.

Este documento recoge un número de casos reportados en los que las disposiciones anti-elusión de la DMCA han sido invocadas no contra piratas, sino contra consumidores, científicos y la legítima competencia. Esto será progresivamente considerado a la luz de diversos casos. La versión más reciente puede ser obtenida en www.eff.org.

2. EL ORIGEN LEGISLATIVO DE LA DMCA

El Congreso promulgó la sección 1201 en respuesta a dos presiones. El Congreso estaba respondiendo a la notoria necesidad de implementar las obligaciones impuestas a los Estados Unidos por el Tratado sobre Derechos de Autor de la Organización Mundial de la Propiedad Intelectual (OMPI) de 1996. Sin embargo, la Sección 1201 fue más allá de lo requerido por el tratado de la OMPI.[2] Entonces, los detalles de la sección 1201 fueron una respuesta no sólo a las obligaciones contempladas en los tratados suscritos por Estados Unidos, sino también a las preocupaciones de los titulares de derechos de autor respecto de que sus obras serían ampliamente objeto de piratería en el entorno digital.[3]

La Sección 1201 contiene dos prohibiciones: una sobre los *actos* de elusión y otra sobre la *distribución de mecanismos y tecnologías* usadas para la elusión.

La primera de ellas, contemplada en la sección 1201(a)(1), prohíbe el *acto consistente en la* elusión de una medida tecnológica de protección usada por el titular de derechos de autor para controlar el acceso a sus obras ("control de acceso"). Así, por ejemplo, esta disposición hace ilegal vulnerar los sistemas de encriptado usados en las películas en DVD. Esta prohibición sobre actos de elusión se aplica inclusive donde los objetivos de la desencriptación de películas podrían, al contrario, ser legítimos. Como resultado, cuando el DVD *Tarzan* de Disney evita que alguien adelante el vídeo saltándose los comerciales que preceden a su presentación, los esfuerzos por eludir tales restricciones podrían ser ilegales.

La segunda, secciones 1201(a)(2) y 1201(b), declara ilícita la manufactura, venta, distribución o tráfico de *mecanismos y tecnologías* que hacen posible la elusión. Estas disposiciones prohíben tanto las tecnologías que vulneran el *control de acceso*, como también las tecnologías que vulneran las restricciones impuestas por los titulares de derechos de autor, tal como *controles de copiado*. Estas disposiciones impiden que los vendedores de tecnología tomen pasos para vulnerar las "protecciones de copia" hoy aplicadas sobre muchos CDs, por ejemplo.

La Sección 1201 también incluye un número de excepciones para cierta limitada clase de actividades, incluyendo pruebas de seguridad, ingeniería inversa de software, investigaciones sobre criptografía, y órdenes legales. Estas excepciones han sido extensamente criticadas por ser demasiado reducidas para ser de real utilidad a quienes ellas pretenden servir.[4]

Una violación de cualquiera de tales prohibiciones de *"actos"* o *"mecanismos"* es de relevancia civil y, en algunas circunstancias, amerita la imposición de sanciones de carácter criminal.

---

2 *Vid* WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2280 before the House Subcomm. on Courts and Intellectual Prop., 105th Cong., 1st sess. (Sept. 16, 1997) at 62 (testimonio del Secretario Asistente de Comercio y Comisionado de Patentes de Marcas, Bruce A. Lehman admitiendo que la sección 1201 fue más allá de los requerimientos del Tratado sobre Derechos de Autor de la OMPI).

3 Para una completa descripción de los sucesos que condujeron a la promulgación de la DMCA, *vid* Jessica Litman, Digital Copyright 89-150 (2000).

4 *Vid* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 Berkeley Technology L.J. 519, 537-57 (1999) (http://www.sims.berkeley.edu/~pam/papers.html)

3. LIBERTAD DE EXPRESIÓN E INVESTIGACIÓN CIENTÍFICA

La Sección 1201 está comenzando a ser usada por algunos titulares de derechos de autor para ahogar la libertad de expresión y la legítima investigación científica. El litigio contra la revista *2600*, las amenazas contra el equipo de investigación del profesor de Princeton Edward Felten, y el procesamiento del programador ruso Dmitry Sklyarov han estancado una variedad de legítimas actividades.

Cediendo ante el temor de responsabilidad ante la DMCA, los prestadores de servicios *on line* y operadores de tablones de anuncio han comenzado a censurar las discusiones sobre sistemas de protección de copiado, los programadores han removido programas de seguridad computacional de sus websites, y los estudiantes, científicos y expertos en seguridad han dejado de publicar detalles de sus investigaciones sobre los protocolos de seguridad existentes. Los científicos extranjeros están incrementando su preocupación para viajar hacia los Estados Unidos por el temor a una posible responsabilidad ante la DMCA, y varias conferencias técnicas han comenzado a ser programadas fuera.

Esta evolución finalmente se traducirá en un debilitamiento de la seguridad para todos los usuarios de computadores (incluyendo, irónicamente, a los titulares de derechos de autor que cuentan con medidas tecnológicas para la protección de sus obras), como para los investigadores en seguridad temerosos de que sus estudios puedan entrar en colisión con la sección 1201.[5]

El jefe de cyber seguridad manifiesta la obstrucción a la investigación

Hablando en el MIT en octubre del 2002, el Jefe de Cyber Security de la Casa Blanca Richard Clarke llamó a modificar la DMCA, haciendo ver su preocupación porque la DMCA ha sido empleada para producir el estancamiento de legítimas actividades de investigación en seguridad informática. El *Boston Globe* citando a Clarke ha sostenido: "Yo pienso que mucha gente no se percata que esto podría tener como efecto el estancamiento sobre la investigación relativa a vulnerabilidades".

El equipo de investigación del profesor Felten amenazado

En septiembre del 2000, un grupo multiempresarial conocido como Secure Digital Music Initiative (SDMI) formuló un desafío público alentando a los especialistas a tratar de vulnerar la seguridad de las tecnologías de filigranas propuesta para proteger la música digital. El profesor de Princeton Edward Felten y un equipo de investigadores de Princeton, Rice, y Xerox aceptaron el desafío y tuvieron éxito en remover las filigranas.

Sin embargo, cuando el equipo trató de presentar sus resultados en una conferencia académica, los representantes de SDMI amenazaron a los investigadores con hacer efectiva su

[5] *Vid* la Declaración del Profesor Ross Anderson, de la Universidad de Cambridge, en *Felten v. RIAA* (Oct. 22, 2001), describiendo las maneras en que la DCMA está suprimiendo la investigación sobre fallas de seguridad en la tecnología de filigramas SDMI: (http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011022_anderson_decl.pdf).

responsabilidad bajo la DMCA. La carta de amenaza fue también distribuida a los empleadores de los investigadores y organizadores de la conferencia. Después de extensas discusiones con el abogado, los investigadores a regañadientes retiraron su paper de la conferencia. La amenaza fue finalmente retirada y una parte de la investigación fue publicada en una conferencia posterior, pero sólo después que los investigadores archivaron el caso.

Después de haber tolerado esta experiencia, al menos uno de los investigadores involucrados decidió renunciar a posteriores trabajos de investigación en esta especialidad.

Hewlett Packard amenaza a SNOsoft

Hewlett-Packard recurrió a las amenazas de la Sección 1201 cuando investigadores publicaron su hallazgo de defecto de seguridad en el sistema operativo Tru64 UNIX de HP. Los investigadores, una organización colectiva liberal conocida como Secure Network Operations ("SNOsoft"), recibieron una amenaza de la DMCA tras haber estrenado un software, en julio del 2002, mediante el cual se demostraba las vulnerabilidades de que HP estaba consciente desde hace algún tiempo, pero que no se había molestado en solucionar.

Luego de que la amenaza de la DMCA recibió gran cobertura de la prensa, HP retiró la amenaza. Sin embargo, los investigadores en seguridad recibieron el mensaje —publicar investigaciones sobre vulnerabilidades a su propio riesgo.

Blackboard amenaza a investigadores en seguridad

En abril del 2003, la compañía de software educacional Blackboard Inc. amenazó con la DMCA para detener la presentación de una investigación sobre vulnerabilidades de seguridad en sus productos en la II Conferencia InterzOne en Atlanta. Los estudiantes Billy Hoffman y Virgil Griffith tenían programado presentar su investigación sobre defectos de seguridad en el panel sobre sistemas de tarjetas de identificación usado en sistemas de seguridad de campus universitarios, pero fueron impedidos poco antes de hablar por una carta de cese y desistimiento que invocaba la DMCA. Blackboard obtuvo una orden temporal restrictiva contra los estudiantes y los organizadores de la conferencia en audiencia secreta *"ex parte"* el día antes de comenzar la conferencia, sin dar a los estudiantes y los organizadores del evento la oportunidad de comparecer al tribunal o impugnar la orden antes de la presentación programada. Aunque en el juicio posteriormente iniciado Blackboard no hacía mención a la DMCA, su invocación en la carta de cese y desistimiento original precedente al reclamo contribuyó a detener a los estudiantes y los organizadores de la conferencia consideraron desafiar el reclamo y proseguir con la presentación programada.

El Libro de Xbox Hack es desechado por su Editor

El 2003, el editor estadounidense John Wiley & Sons desistió de sus planes para publicar un libro del investigador en seguridad Andrew "Bunnie" Huang, citando inquietudes ante las responsabilidades previstas en la DMCA. Wiley encargó a Huang escribir el libro en el cual se

analizan defectos de seguridad descubiertos por este último en el proceso de ingeniería inversa de la consola de juegos Microsoft X-Box, luego de que Huang publicó su investigación como parte de su tesis doctoral en el M.I.T. Huang no distribuyó las llaves públicas de seguridad de Xbox que él había aislado a través de ingeniería reversa, ni hizo copia de algún código Xbox. Aunque la DMCA incluye excepciones para la elusión respecto de pruebas de seguridad informática e ingeniería inversa, ellas eran demasiado restrictivas para ser usadas por Huang o su editor.

A consecuencia de la acción legal emprendida por Microsoft contra el website vendedor de un Xbox mod chip a comienzos del 2003, y las amenazas del 2001 de la industria de la música contra el equipo de investigación del profesor Felten, Wiley se desistió de la publicación temiendo que la editorial pudiera ser responsabilizada por "dejar disponible" un "mecanismo de elusión". Huang inició esfuerzos para autoeditar, pero posteriormente se frustró su venta *on line,* pues su proveedor también le cerró el acceso, citando inquietudes ante la DMCA. Después de varios meses de negociaciones, Huang finalmente autoeditó el libro a mediados de 2003. Ahora, el libro ha comenzado a ser publicado por No Starch Press.

Investigación sobre censorware obstaculizada

Seth Finkelstein conduce una investigación sobre *"censorware" (i.e.*, programas que bloquean websites que contienen material objetable), elaborando un documento sobre los defectos de tales programas, incluido los productos de N2H2, una compañía líder en censorware. La investigación de Finkelstein, documentando los websites inapropiadamente bloqueados por el software de N2H2, contribuyó al exitoso desafío del programa *Primera Enmienda de la ACLU* para el uso obligatorio de software que filtre la web por bibliotecas públicas subvencionadas federalmente.[6]

N2H2 reclama que su listado encriptado de websites bloqueados está legalmente protegido por la DMCA contra intentos de lectura y análisis. Utilizando un límite de tres años de excepción concedido por la Biblioteca del Congreso y Registro de Derechos de Autor en el año 2000, Finkelstein eludió la encriptación sobre los listados de sitios bloqueados por BESS para analizar los defectos en tales listas.

Sin embargo, el trabajo de investigación de Finkelstein ha sido gravemente limitado por el hecho de que los tres años de la excepción están limitados a los actos de elusión, y no le permite crear o distribuir medios que facilitarían su investigación. Además, la excepción existente debe expirar en octubre del 2003, y como Finkelstein declaró ante la Oficina de Derechos de Autor en su audiencia normativa del 2003, a menos que la excepción sea nuevamente concedida, Finkelstein será incapaz de continuar su investigación, pues él teme que las compañías de censorware podrían iniciar una demanda legal por aplicación de la DMCA para acabar con su investigación. Aun cuando posteriormente se establezca que él no ha violado la sección 1201, la posibilidad de un litigio por aplicación de la DMCA le impediría comprometerse a una nueva investigación.

[6] *Mainstream Loudoun v. Board of Trustees,* 24 F.Supp.2d 552 (E.D.Va. 1998).

Benjamin Edelman también ha dirigido una extensa investigación sobre fallas en varios productos censorware. La investigación de Edelman condujo a proporcionar una prueba pericial para la ACLU en un reciente juicio ante una corte federal en que se cuestionaba la constitucionalidad de la Children's Internet Protection Act (CIPA), la que dispone que las bibliotecas públicas deben usar productos censorware como aquéllos vendidos por N2H2.

En el curso de su trabajo para la ACLU, Edelman descubrió que la DMCA puede interferir con su esfuerzo por aprender qué websites son bloqueados por los productos N2H2. Como él buscaba crear y distribuir herramientas de software para permitir a otros analizar la lista si cambiaba, Edelman no podía confiarse en la excepción de tres años. Como él no estaba dispuesto a correr el riesgo de una acción civil o una sanción penal por aplicación de la Sección 1201, Edelman fue forzado a ir a una corte federal para obtener una aclaración respecto de sus derechos legales antes de proseguir su legítima investigación. Sin embargo, desconociendo el estancamiento de la DMCA sobre su investigación, la Corte rechazó el caso de Edelman por carecer de fundamentos.

Dmitry Sklyarov arrestado

En julio del 2001, el programador ruso Dmitry Sklyarov fue encarcelado por varias semanas y detenido por cinco meses en los Estados Unidos tras haber hablado en la conferencia de DEFCON en Las Vegas.

Los fiscales, instados por el gigante del software Adobe Systems Inc., alegaron que Sklyarov había trabajado en un programa de software conocido como el Advanced e-Book Processor, el cual fue distribuido a través de Internet por su empleador ruso, ElcomSoft Co. Ltd. El software permitía disponer de los libros electrónicos Adobe ("e-books") al convertirlos desde el formato e-Book de Adobe a archivos Adobe Portable Document Format ("pdf"), mediante la remoción de las restricciones grabadas en los archivos por los editores de e-Book.

Sklyarov nunca fue acusado de infringir algún e-Book protegido por derechos de autor, ni de ayudar a alguien más a infringir los derechos de autor. El crimen que se le imputó era que él trabajó en un software que, aun cuando con muchos usos legítimos, permitía a terceros que él no conocía, usar la herramienta para copiar un e-Book sin la autorización del editor.

Finalmente, el Departamento de Justicia permitió a Sklyarov volver a casa, decidiendo proceder contra su empleador, ElcomSoft, bajo las disposiciones criminales de la DMCA. En Diciembre del 2002, un jurado absolvió a Elcomsoft de todos los cargos, concluyendo una odisea de 18 meses de incorrecta acusación para la compañía de software rusa.

Científicos y programadores retienen la investigación

A consecuencia de la amenaza legal contra el equipo de investigación del profesor Felten y el arresto de Dmitry Sklyarov, un número de prominentes expertos en seguridad informática han abreviado sus legítimas actividades de investigación por temor a la responsabilidad potencial de la DMCA.

Por ejemplo, el prominente criptógrafo y analista en seguridad de sistemas alemán Niels Ferguson, descubrió una falla de seguridad principal en un sistema de vídeo encriptación Intel, conocido como High Bandwidth Digital Content Protection (HDCP). Él declinó publicar sus resultados en su website explicando las fallas en HDCP, sobre la base de que viaja frecuentemente a los Estados Unidos y está temeroso de "procesamiento y/o responsabilidad bajo las disposiciones de la DMCA".

A raíz del arresto de Dmitry Sklyarov, Fred Cohen, un profesor de forensías digitales y respetado consultor en seguridad, removió su software de recolección de evidencia "Forensix" de su website, citando el temor por la potencial responsabilidad ante la DMCA.

Otro respetado experto en seguridad en redes, Dug Song, también removió contenido de su website por la misma razón. El señor Song es autor de diversos papers sobre seguridad, incluyendo uno en que describe una vulnerabilidad frecuente en muchos firewalls.

A mediados del 2001, un programador anónimo descubrió una vulnerabilidad en el código de administración de libros digitales de propiedad de Microsoft, pero rechazó publicar los resultados, citando sus inquietudes por la responsabilidad prevista en la DMCA.

Científicos extranjeros evitan Estados Unidos

Los científicos extranjeros han expresado su preocupación respecto de viajar a Estados Unidos a consecuencia del arresto del programador ruso Dmitry Sklyarov. Algunos de ellos han llamado a boicotear las conferencias desarrolladas en tal país y varios organizadores de conferencias han decidido trasladar sus actividades fuera del mismo. Rusia ha emitido una alerta a los programadores rusos que viajan a los Estados Unidos.

El altamente respetado programador británico de Linux, Alan Cox, renunció al Comité USENIX de la Advanced Computing Systems Association, el comité que organiza muchas de las conferencias sobre informática en los Estados Unidos, por su temor a viajar a ese país. Cox ha recomendado a USENIX trasladar su conferencia anual fuera del país. La International Information Hiding Workshop Conference, la conferencia en la cual el equipo del profesor Felten deseaba presentar su paper original, optó por romper con la tradición y trasladar su próxima conferencia fuera de los Estados Unidos, a consecuencia de la amenaza de SDMI al profesor Felten y su equipo.

IEEE se enfrenta con la DMCA

El Institute of Electrical and Electronics Engineers (IEEE), que publica el treinta por ciento de todas las revistas sobre ciencias de la computación del planeta, recientemente ha introducido la controversia en el ambiente científico en relación con la DMCA. Aparentemente preocupados por la posibilidad de una responsabilidad bajo la Sección 1201, la IEEE en noviembre del 2001 instituyó una política requiriendo a todos los autores indemnizar al IEEE por cualquier responsabilidad en que se incurriere como resultado de una acción legal emprendida por aplicación de la DCMA.

Después de una protesta generalizada de los miembros de IEEE, la organización finalmente revisó sus políticas de sumisión, eliminando la mención a la DMCA. Según Bill Hagen, gerente de derechos de propiedad intelectual de IEEE, "La Digital Millennium Copyright Act se ha convertido en un asunto sensible entre nuestros autores. Ella ha intentado proteger el contenido digital, pero su aplicación en algunos casos específicos parece haber enajenado a un amplio segmento de la comunidad de investigación".

La revista *2600* censurada

El caso *Universal City Studios* v. *Reimerdes* ilustra el efecto de estancación que la sección 1201 ha tenido sobre la libertad de la prensa.[7]

En este caso, las ocho principales compañías cinematográficas llevaron un caso por aplicación de la DMCA contra *2600* Magazine, solicitando se impidiera la publicación de DeCSS, software por el cual se elude la encriptación usada en las películas en formato DVD. *2600* ha dejado el programa disponible en su website en el curso de un reportaje sobre la controvertida DMCA. La revista no estaba involucrada en el desarrollo del software, ni fue acusada de hacer uso del mismo por alguna infracción a los derechos de autor.

A pesar de la garantía a la libertad de prensa prevista en la Primera Enmienda, el juzgado de distrito impidió permanentemente a *2600* publicar, o siquiera hacer un link hacia el código de DeCSS. En noviembre del 2001, la Corte de Apelaciones del Segundo Circuito decidió revocar la decisión del juzgado.

En esencia, los estudios cinematográficos efectivamente obtuvieron una orden para "detener la impresión" prohibiendo la publicación de información verídica por los noticieros referentes a un asunto de interés público: una reducción de los bien establecidos principios de la Primera Enmienda sin precedentes.

Reportero de CNET siente estancamiento

El prestigioso reportero del Noticiero CNET Declan McCullagh recientemente encontró cuatro documentos disponibles públicamente en la página web de Transportation Security Administration (TSA). El website anunciaba que los documentos contenían información relacionada con los procedimientos de seguridad del aeropuerto, la relación entre las policías federal y local, y una "planilla con información de responsabilidades" *("liability information sheet")*. Una nota en el sitio declaraba que esta "información está restringida a la dirección del aeropuerto y a la aplicación de leyes locales". No era necesario disponer de una password para bajar los documentos, pero ellos estaban distribuidos crípticamente y una password era necesaria para abrirlos y leerlos.

McCullagh obtuvo las passwords de una fuente anónima, pero el temor a la DMCA lo detuvo de leer los documentos: usar una password sin autorización podía violar la Sección

[7] 111 F. Supp. 2d. 294 (S.D.N.Y. 2000), *aff'd* 273 F.3d 429 (2d Cir. 2001).

1201. Esta situación es particularmente irónica, ya que cualquier periodista extranjero fuera del alcance de la DMCA podría libremente usar la password.

"Los periodistas tradicionalmente no se han preocupado tanto respecto de las leyes sobre derechos de autor", dijo McCullagh, "Pero hoy en día los derechos de propiedad intelectual han ido demasiado lejos, y posiblemente interfieren con el proceso de recogida de noticias".

Microsoft amenaza a Slashdot

En la primavera del 2000, Microsoft invocó la DMCA contra el foro de publicaciones en Internet Slashdot, demandando que los moderadores del foro borraran materiales relacionados con la implementación de un estándar de seguridad abierta de propiedad de Microsoft conocida como Kerberos.

En el foro de Slashdot, varias personas alegaron que Microsoft había cambiado las especificaciones abiertas y no propietarias de Kerberos a efectos de prevenir que los servidores que no sean Microsoft interoperasen con Windows 2000. Muchos hicieron especulaciones de que esta jugada estaba destinada a forzar a los usuarios a comprar el software servidor de Microsoft. Aunque la empresa respondió a estas críticas mediante la publicación de sus especificaciones Kerberos, ésta condicionaba el acceso a las especificaciones de acuerdo a un contrato de licencia "click-wrap" que expresamente prohibía la revelación de las especificaciones sin el consentimiento previo de Microsoft.

Slashdot respondió mediante una nueva publicación de las especificaciones Microsoft. Entonces, Microsoft invocó la DMCA, demandando a Slashdot para que removiera las especificaciones vueltas a publicar.

En palabras de Julie Cohen, profesora de derecho de Georgetown, "Si la interpretación de la prohibición sobre elusión de tecnologías de la DMCA sostenida por Microsoft es correcta, entonces no parece importar demasiado si publicar copias no autorizadas de las especificaciones Kerberos de Microsoft serían un fair use. Un editor puede prohibir el fair use consistente en comentarios simplemente mediante la implementación de restricciones de acceso y revelación que encadena al público por completo. Cualquiera que revele la información, o inclusive cuente a otros cómo obtenerla, es un criminal".

AVSforum.com censura la discusión de TiVo

El fantasma de la DMCA también ha contenido la conversación en los más pequeños boletines de noticias de la web. En junio del 2001, por ejemplo, el administrador de AVSforum.com, un popular foro donde los propietarios de grabador de vídeo digital TiVo discuten sobre las características de TiVo, censuró toda la discusión sobre un software que permitía a los usuarios de TiVo mover el vídeo desde sus TiVos a sus computadores personales. En palabras del administrador del foro: "Mi temor con esto es más o menos que no tengo idea de qué está protegido en un sistema de TiVo por derechos de autor –¿qué tienes tú?– y qué no. De ahí mi temor por el sitio".

El foro Mac censura la discusión sobre iTunes Store

El entusiasta website Macintosh, Macosxhints, censuró la publicación de información sobre métodos para evadir la protección de copiado sobre las canciones compradas desde Apple iTunes Music Store en mayo del 2003, citando la preocupación por la responsabilidad prevista en la DMCA. Las canciones adquiridas desde Apple iTunes Music Store son bajadas por los propietarios de Apple en archivos con formato AAC, cubiertos con una protección de copiado digital. Esto impide a los compradores tocar las canciones si no es en iPod portátil MP3 o transferir las canciones hacia computadores que no sean Mac OS para un uso personal no comercial, aun cuando tal conducta sería considerada fair use bajo la legislación sobre derechos de autor. Como sostuvo el webmaster del sitio, aun cuando la información circulante sobre protección de copiado estaba ya disponible en Internet en tal momento, una nueva publicación arriesga traer un caso por aplicación de la DMCA y severas penas.

4. *Fair Use* bajo sitio

El *"fair use"* es un elemento crucial en la legislación sobre derechos de autor estadounidense –el principio según el cual el público está facultado, sin necesidad de requerir permiso, para usar obras amparadas por el derecho de autor de manera transformativa o de otros modos que no interfiera indebidamente con la comercialización de una obra del titular de los derechos de autor–. El fair use incluye usos personales no comerciales, tal como utilizar un VCR para grabar un programa de televisión para verlo más tarde. El fair use también incluye actividades aceptadas para objetivos tales como la crítica, comentario, reportajes, enseñanza, aprendizaje e investigación.

Mientras detener las infracciones a los derechos de autor es un importante objetivo político, la Sección 1201 echa por el caño el fair use con el agua de la piratería digital. Mediante el empleo de medidas de protección tecnológica de control de acceso y de uso de las obras amparadas por derechos de autor, y usando la sección 1201 en juicios contra cualquiera que tantee con tales medidas, los titulares de derechos de autor pueden unilateralmente eliminar el fair use, volviendo a escribir los derechos de autor acordados gracias a su desarrollo por el Congreso y los tribunales por más de un siglo.

La protección de copia de los CDs

La introducción de "protector de copias" en CDs en el mercado ilustra la colisión entre el fair use y la DMCA. Los sellos discográficos están incorporando agresivamente "protección de copiado" en sus nuevos lanzamientos musicales. Sobre 10 millones de discos con protección de copiado están ya en circulación, según Midbar Technology Ltd. –ahora Macrovision–, un vendedor de esta tecnología. Sony sostiene que ha lanzado sobre 11 millones de discos con protección de copiado en el mundo. Ejecutivos de los principales sellos discográficos EMI y BMG han afirmado que para fines del 2003 una proporción significativa de todos los CDs lanzados en los Estados Unidos serán protegidos de copiado.

Cualquiera sea el impacto que estas tecnologías de protección de copiado pueda tener sobre infracciones cometidas *on line*, ellas ciertamente están interfiriendo con las expectativas de fair use de los consumidores. Por ejemplo, la protección de copias en discos hará desaparecer los cientos de miles de consumidores que han comprado reproductores MP3, a pesar del hecho que hacer una copia MP3 de un CD para uso personal es precisamente un fair use. Hacer "mix CDs" o copias de CDs para la oficina o el automóvil son otros ejemplos de fair uses que están potencialmente menoscabados por las tecnologías de protección de copiado.

Las compañías que distribuyen mecanismos para "reparar" estos CDs disfuncionales, restituyéndo a los consumidores sus privilegios de fair use, corren el peligro de litigios bajo las prohibiciones de la sección 1201 sobre mecanismos y tecnologías de elusión.

Mecanismos de *fair use* prohibidos

Estamos ingresando a una era en la cual libros, música y películas estarán progresivamente "protegidos de copiado" y, de uno u otro modo, restringidos por medios tecnológicos. Si estudiosos, investigadores, comentaristas y el público continuarán siendo capaces o no de hacer legítimos fair uses de tales obras dependerá de la disponibilidad de medios de acceso digital.

Sin embargo, las disposiciones anti-elusión de la DMCA, prohíben la creación o distribución de tales mecanismos, aun cuando ellos sean esenciales para el fair use. Entonces, mientras los titulares de derechos de autor usan la tecnología para presionar en el siglo XXI, el público será menoscabado respecto del fair use mediante el empleo de sellos digitales que pretendan "prevenir la piratería". Quizá aún más importante, en el futuro el fair use no será desarrollado –después de todo, antes del VCR, ¿quién podía haber imaginado que el fair use "relevo de tiempo" de la televisión llegaría a ser normal para el consumidor promedio?

Los titulares de derechos de autor argumentan que tales mecanismos, en manos de infractores de los derechos de autor, pueden traducirse en "piratería en Internet". Pero la respuesta tradicional a la piratería bajo la legislación sobre derechos de autor ha sido pesquisar y procesar a los infractores, no prohibir los medios que permiten hacer fair use. Después de todo, fotocopiadoras, VCRs, y grabadores CD-R pueden también ser mal usadas, pero nadie sugeriría al público abandonarlos simplemente porque ellos podrían ser usados por otros para infringir la ley.

DeCSS, DVD Copy Plus y DVD CopyWare

Los mecanismos de fair use ya han sido arrojados fuera del mercado. En el caso *Universal v. Reimerdes*, antes mencionado, el tribunal sostuvo que la Sección 1201 prohibía el software DeCSS. Este software desencripta las películas en DVD, haciendo posible su copia en un PC. En otro caso, 321 Studios LLC han interpuesto una acción declarativa en San Francisco después de haber amenazado con la responsabilidad prevista en la DMCA por la MPAA por distribuir DVD Copy Plus, el cual permite a los dueños de DVD hacer copias de su contenido. Los principales estudios cinematográficos desde entonces se han opuesto demandando, alegando que los mecanismos de copia vulneran la DMCA.

En casos separados, los estudios Paramount Pictures y Twentieth Century Fox han usado la DMCA para demandar a Tritton Technologies, el fabricante de DVD CopyWare, y a tres sitios web distribuidores de otro software que los consumidores pueden usar para copiar los DVDs que ellos han comprado.

Hay razones legítimas para copiar DVDs. Una vez que un vídeo está en un PC, por ejemplo, varios fair uses son posibles—un experto puede analizar digitalmente el film, los viajeros pueden cargar la película en sus laptops, y los padres pueden adelantar el vídeo, saltándose los "inevitables" comerciales que preceden a ciertas películas. Sin embargo, sin los mecanismos necesarios para copiar DVDs estos fair uses se hacen imposibles.

e-Books y Advanced e-Book Processor

El futuro del fair use sobre los libros estaba en cuestión en el procesamiento criminal de Dmitry Sklyarov y ElcomSoft. Como hemos mencionado precedentemente, ElcomSoft produjo y distribuyó un mecanismo llamado Advanced e-Book Processor, el cual traducía los e-books desde el formato e-Book de Adobe a PDF –Portable Document Format– de Adobe. Este procedimiento de traducción removía varias restricciones (contra copiado, impresión, procesamiento de texto a voz, etc.) que los editores pueden imponer sobre los e-Books. El programa está diseñado para trabajar solamente con e-Books que han sido legalmente comprados en locales de ventas.

El Advanced e-Book Processor permitió a quienes tenían e-Books adquiridos legítimamente hacer fair uses de sus e-Books, que de otro modo no sería posible con el formato corriente de e-Book de Adobe. Por ejemplo, el programa permite a la gente involucrarse en las siguientes actividades, todas las cuales son fair uses:

- leerlo en un laptop o computador distinto de aquél en el cual el e-Book fue inicialmente bajado;
- continuar accediendo a la obra en el futuro, si la tecnología por la cual el e-Book era comprado llegaba a quedar obsoleta;
- imprimir un e-Book sobre papel;
- leer un e-Book sobre un sistema operativo alternativo tal como Linux (el formato de Adobe trabaja solamente sobre Macs y Windows PCs);
- tener un computador leyendo un e-Book usando un software lector, el cual es particularmente importante para personas con discapacidad visual.

Relevos de tiempo y Streaming Media

Como muchos consumidores reciben "a raudales" contenidos de audio y vídeo desde recursos media de Internet, ellos podrían demandar medios para preservar sus expectativas relativas a fair use, incluyendo la facultad para "relevos de tiempo" programados para escucharlos o verlos más tarde. Sin embargo, como resultado de la DMCA el equivalente digital de los VCRs, las copias de seguridad de los media puede que nunca lleguen.

La emergente compañía de software Streambox desarrolló exactamente tal producto, conocido simplemente como Streambox VCR, diseñado para relevar el tiempo streaming media. Cuando el competidor RealNetworks descubrió que Streambox había desarrollado un reproductor de streaming media competitivo, invocó la DMCA y obtuvo una orden judicial contra Streambox VCR.

La DMCA también ha sido invocada para amenazar al desarrollador de un software de aplicación en código abierto, no comercial, conocido como Streamripper, que graba pistas de audio de MP3 para escucharlas posteriormente.

Grabados y Tipografías

En enero del 2002, el vendedor de estilos de impresión Agfa Monotype Corporation amenazó a un estudiante con responsabilidad ante la DMCA por la creación de un "grabado", un software libre, programa de código abierto y no comercial diseñado para manipular las fuentes TrueType.

Según el estudiante: "Yo escribí el "grabado" en 1997, descubriendo después que no estaba permitido incorporar la totalidad de mis fuentes en documentos. Desde mis fuentes disponía de libertad, esto era estúpido, pero yo no deseaba tomar tiempo para ... cambiar la bandera, y luego reinicializar todas las propiedades extendidas de las tipografías con un programa distinto. ¡Qué aburrimiento! En cambio, yo escribí este programa para convertir la totalidad de mis fuentes en una. El programa es muy simple; solamente requiere fijar unos cuantos bits en cero. De hecho, me percaté de que otras fuentes que estaban licenciadas para distribución ilimitada también prohibían el incrustamiento... Así, yo puse este programa en la web esperando que pudiese servir a otros desarrolladores de tipografías también".

No obstante, Agfa Monotype amenazó al estudiante autor con responsabilidad en el marco de la DMCA por distribuir el programa. Según Agfa, en los hechos tal incorporación puede ser usada para permitir la distribución de fuentes protegidas elaboradas en oposición a las prohibiciones de la Sección 1201, no obstante el hecho de que tales medios tienen muchos usos legítimos en manos de los aficionados desarrolladores de fuentes.

5. Una amenaza a la innovación y competencia

La DMCA está siendo usada para impedir el esfuerzo de legítimos competidores por crear productos compatibles.

Por ejemplo, la división de vídeo juego Blizzard de Vivendi-Universal invocó la DMCA en un esfuerzo por intimidar a los desarrolladores de un software derivado de legítima ingeniería inversa. Sony ha usado la DMCA para amenazar a los aficionados que crearon un software competidor para el perro robot Aibo de Sony, tal como demandó a los desarrolladores del software que permite jugar Playstation en PCs. En cada uno de estos casos, la DMCA fue usada para detener un competidor del mercado, en vez de serlo para combatir la piratería.

Lexmark Demanda a los Cartridges de Toner

Lexmark, el segundo más grande distribuidor de impresoras en los Estados Unidos, ha tratado de eliminar vendedores de toner de impresión láser reciclados que ofrecen a los consumidores cartridges a precios más bajos que los de Lexmark. En enero del 2003, Lexmark empleó la DMCA como una nueva arma de su arsenal. La empresa obtuvo una orden judicial DMCA prohibiendo al fabricante de microchip de impresión Static Control Components la venta de chips alegando que era una "tecnología" que "evadía" ciertas "rutinas de autenticación" entre los cartridges e impresoras Lexmark.

Lexmark agregó tales rutinas de autenticación explícitamente para obstaculizar a los vendedores de toner reciclados. Static Control hizo ingeniería reversa de tales medidas y vendió "Smartek" chips que posibilitaba a cartridges reciclados para trabajar en impresoras Lexmark. La empresa usó la DMCA para obtener una orden judicial prohibiendo que Static Control vendiera su chip de ingeniería inversa para cartridge reciclados.[8] Static Control ha apelado la decisión y contraatacado a través de la iniciación de un caso por anti-trust. Cualquiera sea el mérito de la posición de Lexmark, es de justicia decir que la eliminación de toner reciclados para impresoras laser no era aquello que el Congreso tenía en mente cuando promulgó la DMCA.

Chamberlain demanda al fabricante de un abridor universal de puertas de garage

El fabricante de abridores de puertas de garaje Chamberlain Group invocó la DMCA contra el competidor Skylink Technologies después que los principales comerciantes minoristas estadounidenses bajaron los abridores remotos de Chamberlain a favor del menos costoso "clickers" universal Skylink.[9] Chamberlain reclamó que el control remoto compatible de Skylink violaba la DMCA por poner en circulación un "régimen de autenticación" entre el abridor remoto Chamberlain y la unidad receptora de la puerta de garaje.

Skylink hizo ingeniería reversa del algoritmo usado por el programa computacional del receptor de la puerta de garaje. El transmisor de Skylink envía tres códigos estáticos, los cuales gatillan una función de sincronización y abren la puerta de garaje. Aun cuando el clicker Skylink no usa el "código de rodado" enviado por el transmisor Chamberlain, éste reclama que se "pone en circulación" su "rutina de autenticación" para usar el programa de computación que controla el motor de la puerta. Desde este punto de vista, a un consumidor que reemplazara su clicker Chamberlain perdido o dañado con uno más barato de Skylink no le estaría permitido "acceder" a su propio garaje. El mismo argumento podría aplicarse igualmente para prohibir los controles remotos universales de televisión.

---

8 *Lexmark International, Inc. v. Static Control Components, Inc.*, (E.D. Ky Civil Action No. 02-571 KSF, unreported decision, Febrero 27, 2003), disponible en la página web de EFF: http://www.eff.org/Cases/Lexmark_v_Static_Controls/

9 *The Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, (N.D. Ill., Civil Action No. 02 C 6376). La demanda, la moción de juzgamiento sumario sin apertura de probatorio de Plaintiff y oposición del demandado a tal petición, están disponible en el sitio web de EFF: http://www.eff.org/Cases/Chamberlain_v_Skylink/

Auque Skylink ganó a Chamberlain una *motion for summary judgment*,[10] Chamberlain ha solicitado prohibir la importación y venta de clickers Skylink en los Estados Unidos mediante la prosecución de casos simultáneamente contra Skylink y los fabricantes chinos de clickers ante la Comisión Internacional de Comercio. Cualquiera sea el desenlace de este caso, es claro que al promulgar la DMCA, el Congreso no deseaba dar a los titulares de derechos de autor el derecho a vetar la creación de bienes y tecnologías compatibles no amparadas por los derechos de autor.

Sony demanda a Connectix y Bleem

Desde la aprobación de la DMCA en 1998, Sony ha usado demandas invocando la DMCA para presionar a los competidores que crearon software que permitían a los propietarios de PC jugar aquellos juegos desarrollados para la consola de vídeo juego Sony Playstation. En 1999, Sony demandó a Connectix Corporation, el fabricante de Virtual Game Station, un programa emulador que permitía que los juegos de Sony Playstation fuesen jugados en un computador Apple Macintosh. Sony demandó también a Bleem, el líder de ventas del software emulador de Playstation para Windows PCs.

En ambos casos, Sony retiró posteriormente los reclamos por elusión contra sus competidores que han creado sus productos mediante compromisos de legítima ingeniería inversa, los cuales se ha reconocido que no infringen el fair use en una serie de casos del Noveno Circuito. De hecho, Connectix finalmente ganó en el Noveno Circuito que resolvió que su ingeniería inversa constituía en realidad fair use.[11] Sin embargo, tanto Connectix como Bleem fueron incapaces de soportar los altos costos de litigación contra Sony y finalmente fueron forzadas a retirar sus productos del mercado. Cualquiera fuera el mérito que la posición de Sony pudiera tener al amparo de derechos de autor, marcas, patentes, u otros arbitrios legales, los esfuerzos competitivos de Connectix y Bleem estaban ciertamente algo lejos de la eliminación de la "caja negra" como dispositivo de piratería que el Congreso quiso brindar como objetivo a la sección 1201.

Sony amenaza a un aficionado de Aibo

Sony también ha invocado la DMCA contra un aficionado que desarrolló programas a medida para el robot de perro mascota Aibo de Sony. El aficionado crackeó el encriptado del código fuente que maneja el Aibo mediante un programa de ingeniería reversa que permite a los propietarios personalizar el reconocimiento de voz para sus Aibos. El aficionado no reveló el código fuente desencriptado ni el código usado por él para vulnerar el encriptado, distribuyó como de costumbre libremente su programa, y no lucró por ello. No obstante, Sony alegó que el acto de evasión del encriptado del código fuente violaba la DMCA y demandó que los aficionados removieran sus programas desde su website.

En respuesta a la protesta pública generalizada, Sony finalmente permitió a los aficionados reponer algunos de sus programas (en el entendido que Sony tendrá los derechos de

[10] Una *motion for summary judgment* es una petición de juzgamiento sumario en que se omite la recepción de la causa a prueba, sobre el entendido de no existir controversia en cuanto a los hechos.

[11] Sony Computer Entertainment, Inc. v. Connectix Corporation, 203 F.3d 596 (9th Cir. 2000).

desarrollo comercial sobre ellos). Sin embargo, el incidente ilustró el deseo de Sony de invocar la DMCA en situaciones no relacionadas con "piratería".

Blizzard demanda a bnetd.org

La Sección 1201 ha sido invocada en un caso federal por la división de videojuegos de Blizzard Entertainment de Vivendi-Universal contra un grupo de entusiastas jugadores voluntarios, quienes usaron ingeniería inversa para crear un software libre y de código abierto para permitir a los propietarios de juegos Blizzard jugarlos en Internet. El software, un servidor llamado "bnetd", proporciona una alternativa al servidor Battle.net de propiedad de Blizzard.

Tanto el servidor Battle.net como el bnetd están disponibles libremente y permiten a los propietarios de juegos Blizzard jugar con otros a través de Internet. El grupo de voluntarios decidió crear bnetd para superar las dificultades que habían experimentado intentando usar Battle.net. El software bnetd es libremente distribuido, de código abierto y no comercial.

Blizzard sometió el caso en St. Louis para prohibir la distribución de bnetd, alegando que el software es un mecanismo de elusión que viola la DMCA. Según Blizzard, el software bnetd ha sido usado por algunos para permitir el juego en red de juegos Blizzard pirateados. Sea o no ello verdad, los desarrolladores no están usando el software con tal objetivo, ni han diseñado el mismo para ello. El software tiene numerosos usos legítimos para los propietarios de juegos Blizzard. Cuanto más se pueda decir sobre el software bnetd, es evidente que él no es un mecanismo de "caja negra" para la piratería.[12]

Sony ataca a Playstation "Mod Chips"

Aparte del uso de la DMCA contra vendedores de computadores personales emuladores de Playstation, Sony ha demandado a numerosos fabricantes de los llamados "mod chips" alegando la elusión prevista en la DMCA. Al hacer esto, Sony ha sido capaz de hacer cumplir un sistema de restricciones geográficas regional que plantea asuntos sobre anticompetitividad.

Los denominados *"mod chips"* son accesorios comercializados en el mercado que modifican las consolas Playstation para permitir que juegos adquiridos legítimamente en otras partes del mundo sean jugados en las consolas de regiones geográficas distintas. Sony ha demandado a los fabricantes de *mod chip* en Estados Unidos, Reino Unido y Australia. En los Estados Unidos, Sony demandó a Gamemasters Inc., distribuidor del periférico Game Enhancer, el cual permitía a los usuarios estadounidenses de Playstation jugar los juegos comprados en Japón y otros países. Aunque no había infracción a los derechos de autor de Sony, el tribunal concedió una orden judicial en aplicación de las disposiciones anti-elusión de la DMCA, prohibiendo el uso de una tecnología que permitiría a los usuarios hacer un uso legítimo de los juegos adquiridos en otras regiones sin infracción.

[12] EFF está representando a los desarrolladores de bnetd.

Reconociendo el potencial anticompetitivo del sistema de control regional, la autoridad australiana antimonopolio, la Comisión Australiana de Consumidores y Competencia, intervino en un caso que Sony finalmente ganó contra un fabricante australiano de mod chip mediante la aplicación de disposiciones anti-elusión de Australia, equivalentes a las contempladas en la DMCA.

Sony ha argumentado que los mod chips pueden también ser usados para posibilitar el uso de copias no autorizadas de juegos Playstation. Pero la mayor parte de los mod chips Playstation no son un mecanismo de "caja negra" apropiado solamente para piratería. El potencial uso ilegítimo debe ser equilibrado con los usos legítimos, tal como la vulneración del sistema de codificación regional de Sony para jugar aquellos juegos adquiridos en otros países.

Apple persigue la inventiva de comerciante minorista

Cuando Other World Computing (OWC), un pequeño vendedor minorista especializado en computadoras Apple Macintosh, desarrolló un software parche que permitía a todos los propietarios de Mac usar el software iDVD de Apple, ellos pensaron que estaban haciendo un favor a los aficionados de Apple. Para su preocupación, ellos obtuvieron una amenaza de aplicación de la DMCA formulada por Apple.

El software iDVD de Apple fue diseñado para trabajar sobre los más nuevos Macs que incluían grabadores internos de DVD fabricados por Apple. OWC descubrió que una modificación menor al software permitiría que el iDVD trabajara con un grabador externo de DVD, brindando con ello a los propietarios de los más antiguos modelos Mac un parche de actualización. Apple reclamó que ello constituía una violación a la DMCA y requirió que OWC detuviera tal práctica inmediatamente. OWC fue complaciente.

En vez de prevenir la infracción a los derechos de autor, la DMCA facultó a Apple para forzar a los consumidores a comprar nuevos computadores Mac, en lugar de simplemente actualizar sus máquinas más viejas con un grabador externo de DVD.

6. La DMCA se convierte en una prohibición general de acceso a redes informáticas

En una diferente categoría del mal uso, las disposiciones anti-elusión de la DMCA recientemente han sido utilizadas como una prohibición general de acceso a redes informáticas. Varios estatutos federales "anti-hacking" ya protegen a los propietarios de redes informáticas de intrusiones no autorizadas. Ellas incluyen la Computer Fraud and Abuse Act, la Wiretap Act, y la Electronic Communications Privacy Act. Además, la doctrina del common law de intrusión a la propiedad también ha sido ampliamente usada con este objetivo. Sin embargo, cada uno de estos distintos regímenes busca equilibrar la importancia de los objetivos de orden público mediante la proscripción tan sólo de aquella conducta que reúne ciertas condiciones y causa un significativo perjuicio financiero a los propietarios de computadores, la DMCA carece de un umbral de daño financiero.

Dada la existencia específica de regímenes legales que regulan este tipo de conducta, es claro que el Congreso no pretendía que la DMCA fuera usada de tal modo, creando una nueva y absoluta prohibición de acceso a redes informáticas a falta de cualquier otro tipo respecto de las obras amparadas por el derecho de autor.

Disgustado ex-empleador demanda por acceso no autorizado a redes

En abril del 2003, una compañía proveedora de comercio automatizado demandó a un antiguo programador contratado por ella por aplicación de la DMCA, alegando que su acceso al sistema computacional de la compañía mediante una password protegida Virtual Private Network a través de un túnel de conexión era un acto de elusión. Pearl Investments había empleado al programador para crear un módulo de software para su sistema. A efectos de completar el trabajo remotamente, el programador conectó un servidor separado a aquél de la compañía, al cual él se conectó desde un túnel VPN desde su oficina. Aunque el contratista creó con bastante éxito el módulo de software para la compañía, la relación se congeló después que la compañía corrió por dificultades económicas y terminó el contrato del contratista.

La compañía demandó al contratista cuando descubrió que el servidor del contratista estaba conectado a su sistema, alegó intrusión electrónica no autorizada, violación de la legislación anti-hacking, la *Computer Fraud and Abuse Act* (CFAA) y violación de las disposiciones anti-elusión de la DMCA. Pearl alegó que había retirado la autorización que previamente había dado al contratista para acceder a su sistema a través de la password protegida VPN y que la conexión VPN era, por consiguiente, no autorizada. La Corte desestimó la intromisión electrónica de la compañía y la aplicación de la CFAA debido a carecer de evidencia de haberse producido cualquier daño actual. Aun cuando el segundo servidor no estaba siendo usado por el programador en tal momento, y su disco duro había sido borrado accidentalmente, la corte estuvo de acuerdo con Pearl en cuanto a que la *existencia* de la VPN constituía una elusión prohibida a una medida tecnológica de protección que controlaba el acceso a un sistema que contenía software protegido por derechos de autor.

Como la DMCA no contempla un umbral de perjuicios, las disposiciones anti-elusión están abiertas a ser mal usadas por compañías inescrupulosas que ambicionan evitar el pago a sus antiguos empleados o contratistas mediante la revocación de la autorización previamente concedida y alegando enseguida elusión.

7. Conclusión

Los cinco años de experiencia con las disposiciones "anti-elusión" de la DMCA demuestran que la normativa está yendo demasiado lejos, entorpeciendo una amplia variedad de actividades de maneras que el Congreso no se propuso. Como un número creciente de obras amparadas por los derechos de autor están revestidas de medidas tecnológicas de protección, es de presumir que las disposiciones anti-elusión serán aplicadas en más contextos imprevistos, impidiendo las legítimas actividades de innovadores, investigadores, la prensa y del público en general.

EFF desearía agradecer a quienes han contribuido a crear y actualizar esta publicación: Samuelson Law, Technology & Public Policy Clinic, Deirdre Mulligan, Nicky Ozer, y Nicolai Nielsen.