S

OMPI

SCCR/10/2 Rev.
ORIGINAL: Inglés
FECHA: 4 de mayo de 2004

ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL
GINEBRA

COMITÉ PERMANENTE DE DERECHO DE AUTOR Y DERECHOS CONEXOS

Décima sesión
Ginebra, 3 a 5 de noviembre de 2003

EVOLUCIÓN RECIENTE EN EL CAMPO DE LA GESTIÓN DE LOS DERECHOS DIGITALES

Documento preparado por el Sr. Jeffrey P. Cunard, Debevoise y Plimpton, Washington, D.C.;

el Sr. Keith Hill, Consultor Principal, Rightscom Limited*, Londres;*

y

el Sr. Chris Barlas, Consultor Principal, Rightscom Limited*, Londres*

INDICE

Página

Página

Página

Página

Página

Página

RESUMEN[*]

En este documento se presenta un estudio sobre la gestión de derechos digitales (DRM, *digital rights management*), tanto sobre las tecnologías que les sirven de base como sobre los instrumentos jurídicos que rigen la utilización de dichas tecnologías y los procesos conexos llevados a cabo en Australia, Europa, Japón y los Estados Unidos de América, y está destinado a cualquier persona que tenga interés en este asunto, especialmente a quienes estén menos familiarizados con la gestión de derechos digitales.

Aunque los autores del estudio son expertos en la materia, debe tenerse en cuenta que muchos aspectos de la gestión de derechos digitales se encuentran aún en una fase teórica. Hasta la fecha no existen implementaciones suficientemente amplias de los mismos, aunque ciertos tipos de contenidos y de servicios de contenidos utilizan alguna forma de DRM y de tecnologías de protección de contenidos. Además, las leyes que rigen el desarrollo y la utilización de las tecnologías DRM son recientes y comparativamente aún existe poca jurisprudencia. Por lo tanto, este estudio debe considerarse una aportación puntual y no una tesis definitiva sobre la materia que pueda utilizarse indefinidamente para la toma de decisiones en el futuro. No obstante, este estudio pretende ser de utilidad para quienes deseen conocer la situación del estado del arte a mediados de 2003.

El estudio comienza con una introducción que proporciona una descripción funcional de alto nivel de las tecnologías DRM, en la que se descomponen las diversas funcionalidades que éstas ofrecen a un usuario, ya sea titular de derechos o consumidor de contenidos. A continuación se presenta una breve historia de Internet y de las tecnologías digitales desarrolladas para dar cabida a los contenidos digitales, incluyendo tecnologías que permiten el intercambio ilícito de contenidos en las redes. Ello permite valorar sucintamente la situación actual de los titulares de derechos en relación con el desarrollo tecnológico.

La última parte de la sección de introducción expone como se complementarán los modelos tradicionales de explotación de contenidos con nuevos modelos cuya introducción es posible gracias a las tecnologías DRM, utilizando como ejemplos diversos casos reales. Esta sección termina con algunas observaciones sobre el concepto de "computación confiable" ("*trusted computing*"), que es previsible que tenga un impacto significativo en el futuro de las transacciones seguras de contenidos digitales.

En la segunda sección, se describe extensamente la situación actual de las tecnologías DRM. En aras de la simplicidad, estas tecnologías se presentan como un conjunto de componentes y herramientas que pueden integrarse para formar un sistema consistente. Al objeto de este estudio, se hace una distinción entre la "gestión de derechos digitales" y la "gestión digital de derechos". La primera incluye las tecnologías de identificación, los metadatos y el lenguaje para la expresión de derechos, mientras que la segunda incluye la encriptación, las filigranas digitales, las firmas digitales, las tecnologías para la privacidad y los sistemas de pago.

La descripción de las tecnologías en que se basa la DRM está seguida de una breve subsección sobre la normalización y su importancia para el despliegue efectivo de la DRM.

---

[*] Las opiniones expresadas en este estudio pertenecen a los autores y no corresponden necesariamente a las de los Estados miembros o a las de la Secretaría de la OMPI.

La tercera sección del documento presenta el marco jurídico actual en el que se desarrollan las tecnologías DRM. En primer lugar, y en relación con el Tratado de la OMPI sobre Derecho de Autor y el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas (en lo sucesivo, los "Tratados de la OMPI sobre Internet"), se describen las disposiciones sobre las tecnologías contra la elusión y la información para la gestión del derecho de autor. En relación con el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (Acuerdo sobre los ADPIC), se describe el ámbito de dicho acuerdo y los estudios realizados por la Organización Mundial del Comercio sobre el comercio electrónico. Se hace a continuación un análisis de la situación jurídica en Australia, la Unión Europea, Japón y los Estados Unidos de América. En relación con los Estados Unidos de América, se analiza la Ley de Derecho de Autor para el Milenio Digital (*Digital Millennium Copyright Act*) y otras medidas legislativas pertinentes, incluyendo leyes federales y estatales, así como procedimientos reglamentarios relevantes. En relación con la situación en la Unión Europea, se analiza la Directiva de Derechos de Autor, incluyendo un breve resumen sobre su grado de aplicación en los Estados Miembros, así como otras Directivas, tales como la Directiva de Programas de Ordenador y la Directiva de Acceso Condicional. Además, se proporciona información sobre los talleres organizados por la Comisión Europea sobre DRM. Cada uno de dichos análisis sobre ámbitos jurisdiccionales específicos está acompañado, cuando procede, del análisis de la jurisprudencia más significativa.

La cuarta sección del documento se inicia con una revisión de las posiciones de los colectivos interesados, desde los titulares de derechos a los consumidores y usuarios finales, teniendo en cuenta las actividades de las sociedades de gestión colectiva, los intermediarios y los suministradores de tecnología. En una breve subsección se incluyen varios ejemplos de servicios DRM para distintos tipos de contenidos actualmente disponibles en el mercado. Esta sección termina con un breve análisis sobre la interoperabilidad.

En la quinta y última sección se analizan algunos asuntos que han surgido como consecuencia de la utilización de tecnologías DRM, incluyendo los directamente relacionados con la propiedad intelectual. También se identifican y analizan otros asuntos relativos a la privacidad, la jurisdicción y el marco jurídico aplicable, el papel de los gobiernos en la elaboración de normas y, finalmente, las prácticas en materia de concesión de licencias para la utilización de tecnologías.

El estudio concluye con una análisis del papel de las instituciones internacionales y se proponen cuatro recomendaciones con medidas concretas que podrían ser aprobadas en el futuro.

1. INTRODUCCIÓN

En este documento se describen los desarrollos actuales de carácter comercial, técnico y jurídico en el campo de la gestión de derechos digitales (DRM, *Digital Rights Management*). En gran medida, tiene por objetivo desmitificar las tecnologías que se han desarrollado para la gestión de derechos y contenidos en formato digital y para ayudar a que los lectores entiendan cabalmente el objetivo y la aplicación de estas tecnologías en el mundo real. Al mismo tiempo, se describen diversos marcos jurídicos desarrollados en el ámbito internacional en varias jurisdicciones importantes y destinados a proteger las tecnologías DRM y los contenidos que éstas gestionan. El documento termina identificando aspectos relevantes de carácter político que pueden justificar la realización de estudios adicionales.

Este documento no pretende ofrecer una explicación en profundidad de los procesos técnicos involucrados, aunque los autores confían en que ayude a facilitar el diálogo entre lectores no técnicos y especialistas técnicos. Tampoco pretende servir de ayuda para la elección de tecnologías propietarias, estén o no basadas en normas aprobadas.

En su afán por exponer la gran diversidad de aspectos de naturaleza comercial y política, el documento no puede entrar a describir cada una de las tecnologías disponibles en el mercado para cada tipo de contenido, ni puede analizar todas las disposiciones jurídicas ni toda la jurisprudencia aplicable.

1.1 Descripción funcional de la DRM

Desde una perspectiva funcional, la DRM tiene un significado distinto para gente distinta. Aunque para algunos sólo es el proceso técnico que permite proporcionar contenidos seguros en forma digital, para otros es todo el proceso técnico que permite el intercambio de derechos y contenidos sobre redes, como por ejemplo Internet. Por conveniencia, a menudo la DRM se divide en dos áreas funcionales:

– la identificación y descripción de la propiedad intelectual, los derechos de las obras y de partes implicadas en aspectos administrativos (gestión de derechos digitales);

– La observancia (técnica) de restricciones para su utilización (gestión digital de derechos).

Por lo tanto, la DRM puede hacer referencia a tecnologías y/o procesos aplicables al contenido digital para describirlo e identificarlo y/o para la definición, aplicación y observancia de reglas de utilización de forma segura.

Asimismo, es importante distinguir entre “control de acceso,” “protección de copiado” y “gestión de derechos de propiedad intelectual” diferenciando sus respectivos límites.

Un sistema de control de acceso gestiona el acceso de un usuario a un contenido, normalmente utilizando algún tipo de protección mediante contraseña. Sin embargo, una vez que se ha concedido el acceso a un contenido, no es posible determinar qué se hace con dicho contenido. Este tipo de protección se utiliza a menudo en sitios web en los que es suficiente aplicar un mecanismo de control de acceso sencillo.

Un sistema de protección de copiado está diseñado para indicar en qué medida está autorizada la copia y la copia en serie, si es el caso, utilizando para ello la "información de uso" asociada a una instancia del contenido, y para la aplicación y observancia en el equipo de usuario del comportamiento indicado. El concepto de protección de copiado puede ampliarse al control del movimiento del contenido dentro y fuera del dominio del usuario, incluyendo la redistribución del mismo en Internet.

Un sistema completo de gestión de derechos de propiedad intelectual incluye el procesamiento de toda la información sobre los derechos para la administración electrónica de los mismos, incluyendo, a veces, información contractual y personal que permita la gestión extremo a extremo de todos los derechos a lo largo de la cadena de valor. Por su propia naturaleza, la DRM puede requerir el acceso a información comercialmente sensible (en contraposición a información de copia y señalización de utilización). La utilización de dicho sistema permite un control muy granular del contenido, permitiendo que los titulares de los derechos apliquen modelos de uso sofisticados.

Este proceso de gestión de derechos de propiedad intelectual implica inevitablemente una amplia utilización de tecnologías DRM. Dichas tecnologías pueden estar integradas en numerosos componentes, desde los que residen en un único dispositivo, como por ejemplo un Asistente Digital Personal (PDA, *Personal Digital Assistant*), a los que pueden encontrarse en servidores comerciales en Internet explotados por grandes compañías y organizaciones.

Este documento pretende exponer la gama de herramientas que pueden utilizarse en los sistemas DRM, describir como pueden aplicarse y explicar los principios jurídicos relevantes y las diversas políticas públicas que pueden surgir como consecuencia de su utilización.

1.2 Origen, principios conceptuales y objetivos de la DRM

1.2.1 El nacimiento de Internet

Internet y la World Wide Web tienen sus raíces en la investigación gubernamental sobre sistemas de computadoras realizada en los Estados Unidos de América mediados de los años 50. La Agencia de Proyectos de Investigación Avanzada (ARPA, *Advanced Research Projects Agency*) se puso en marcha en 1950 y realizó experimentos con las primeras redes de computadoras en 1965. Más tarde, entre 1967 y 1969, ARPA desarrolló ARPANET. El proyecto había sido aprobado por el Ministerio de Defensa de los Estados Unidos de América (DoD, *Department of Defense*) para la investigación sobre redes de telecomunicaciones. Se estableció una red de cuatro computadoras y, en 1971, ARPANET se amplió a 15 nodos. En ese mismo año, Ray Tomlinson de BBN diseñó la primera aplicación de correo electrónico, que era capaz de enviar y recibir mensajes en una red distribuida. En 1972, se eligió el símbolo @ con el significado de "en " ("at"), que se integró en la aplicación de correo electrónico de BBN.

En 1972 se realizó una demostración de ARPANET entre 40 máquinas durante la Conferencia Internacional sobre Comunicaciones por Computadora (ICCC, *International Conference on Computer Communications*). El mismo año, se realizó el primer diálogo ("*chat*") entre computadoras. En 1974, BBN lanzó Telenet, un servicio público de datos en modo paquete que era la versión comercial de ARPANET.

Durante los años 80, la tecnología de Internet creció exponencialmente. A principios de la década, se inició el desarrollo de redes paralelas a ARPANET. Así surgieron BITNET, CSNET y Minitel en Francia. Al mismo tiempo, muchas organizaciones adoptaron el recientemente introducido protocolo de transporte, TCP/IP, que constituye la base de la actual Internet. En 1983, la Universidad de Wisconsin inició el desarrollo de la tecnología de nombres de dominio. En 1984 se introdujo el Sistema de Nombres de Dominio (DNS, *Domain Name System*), que es otra piedra angular de la Internet de hoy en día. Los primeros nombres de dominio se asignaron en 1985.

En 1987, el número de computadoras anfitriones de Internet alcanzó la cifra de diez mil, y en 1988 se creó la Autoridad de Asignación de Números de Internet ("IANA", *Internet Assigned Numbers Authority*) para administrar el Sistema de Nombres de Dominio. En 1989 , varios proveedores de servicio europeos constituyeron el consorcio RIPE (*Reseaux IP Europeens*), al tiempo que el número de computadoras anfitriones de Internet alcanzaba a nivel mundial la cifra de 100.000. En 1990, "*The World comes on-line* (world.std.com)," se convirtió en el primer proveedor comercial de acceso conmutado a Internet.

Posiblemente el hito público más importante fue la invención de la World Wide Web ("Web") en 1991. Esta tecnología fue desarrollada por Tim Berners-Lee de los laboratorios del CERN en Ginebra, utilizando hiperenlaces para que los documentos pudieran estar disponibles en todo Internet. La tecnología, originalmente desarrollada para ser utilizada internamente en el CERN, fue rápidamente propuesta a los organismos de normalización internacionales. Ello ha llevado al actual proceso de normalización de la World Wide Web, incluyendo HTML y HTTP, que constituyen las bases de la web tal como hoy la conocemos.

En 1992, el número de computadoras anfitriones en Internet alcanzó el millón, y en 1993 apareció el primer navegador web ("*browser*"), denominado Mosaic. Ello constituyó una revolución de primer orden pues permitió que personas sin conocimientos técnicos pudieran utilizar la tecnología sin necesidad de un entrenamiento especial. Durante ese mismo año, el tráfico en la Web creció a un ritmo anual del 341,634%.

En 1994 se difundió el primer programa de radio por Internet. En los años siguientes, aparecieron tecnologías tales como los motores de búsqueda y la telefonía por Internet, así como software para programación especialmente adaptados a Internet, como por ejemplo, JAVA de Sun Microsystems.

Durante el período entre 1995 y 2003, se ha producido un enorme crecimiento de Internet. El número de dominios ha crecido exponencialmente, así como el número de usuarios de Internet. Según el *Internet Software Consortium*, en julio de 2002 había 162.128.493 computadoras anfitriones en Internet identificados en el DNS, en comparación con los 147.344.723 anfitriones que había en enero del mismo año. Según OCCL, Alexa Internet e IDC, cada día se crean 4.400 nuevos sitios Web.

1.2.2 Desarrollo de Internet para el comercio electrónico

En 1986, una empresa de compraventa filatélica denominada "*International Stamp Exchange"*inició la explotación del primer servicio comercial en Internet. La componente de "comercio electrónico" de la compañía filatélica se realizaba mediante terminales télex o con computadoras personales. En 1996 se forjó el término comercio electrónico. Sin embargo, para muchos el año en que se produjo la irrupción del comercio electrónico fue 1998,

iniciándose la adopción del mismo entre los consumidores. Un informe reciente de la firma de investigación comercial Jupiter, estima que el gasto en servicios en línea en los Estados Unidos de América aumentará un 28% en 2003 hasta los 52 mil millones de dólares. Jupiter estima asimismo que en 2007 el gasto en línea de los consumidores podría alcanzar los 105 mil millones de dólares de los EE.UU., aproximadamente el 5% del gasto de los consumidores de dicho país. En Europa también se está produciendo un gran crecimiento del gasto en línea de los consumidores.

Desde una perspectiva tecnológica, la puesta a disposición por parte de los gobiernos de tecnologías de encriptación para ser utilizadas públicamente ha permitido el desarrollo de transacciones seguras para el comercio electrónico. El protocolo de capa de conexión segura (SSL, *Secure Socket Layer*), desarrollado por Netscape Communication, fue la primera tecnología significativa para proporcionar seguridad y privacidad a las transacciones financieras en Internet, utilizando técnicas de encriptación. En 1994 se presentó la versión 1 de la especificación de SSL. En el mismo año, la versión 2 del SSL fue la primera aplicación comercial del protocolo. En 1995 se publicó una versión sustancialmente modificada, la versión 3 del SSL.

1.2.3 Desarrollo de medios de almacenamiento digital

Los medios de almacenamiento digital, es decir, los soportes capaces de almacenar propiedad intelectual (IP, *Intellectual Property*) en forma digital, constituyen otra tecnología fundamental que ha sido esencial para el desarrollo del comercio electrónico de bienes digitales. Los medios de almacenamiento digital incluyen discos duros, medios ópticos, tales como discos compactos (CD, *compact disk*) y discos digitales versátiles (DVD, *digital versatile disks*), y tarjetas de memoria.

Conforme ha aumentado la capacidad de almacenar información en forma digital, ésta ha ido sustituyendo al almacenamiento mecánico, como por ejemplo, bibliotecas físicas de CD de audio o las colecciones personales de fotos. Las computadoras personales, que son muy flexibles para manejar información, proporcionan muchas oportunidades para crear compilaciones individualizadas en sus discos duros o mediante sus lectores de CD-ROM grabables. Si bien no existe problema en la medida en que dichas compilaciones sólo contienen información personal o creaciones del titular, cuando la tecnología se utiliza para almacenar grandes cantidades de información infringiendo los derechos de propiedad intelectual, se convierte en un auténtico quebradero de cabeza para los titulares de los derechos. La situación se hace aún más problemática cuando la computadora personal está conectada a Internet, debido a que las compilaciones del titular puede quedar disponibles para cualquiera mediante una red de uso compartido o intercambio de ficheros.

1.2.4 Desarrollo de la tecnología de conversión de formato de codificación

La tecnología de conversión del formato de codificación ("*ripping*") consiste en el proceso de extracción del contenido digital (audio o video) de un CD o de un DVD que se traspasa al medio de almacenamiento del propietario, como por ejemplo su disco duro.

El desarrollo de esta técnica está asociado a la proliferación del uso de MP3, un formato de audio comprimido (capa 3 normalizada de MPEG-1), que permite a los usuarios almacenar música de alta calidad comprimida en un disco duro o en cualquier otro medio digital.

Originalmente, los usuarios realizaban la conversión del formato de audio de CD para crear compilaciones personales de música en sus computadoras. Sin embargo, tal como se ha señalado anteriormente, el desarrollo de aplicaciones basadas en la web, como por ejemplo, Napster, Kazaa y otras, que permiten a los usuarios compartir sus compilaciones, ha hecho que el fenómeno de la conversión del formato de codificación (*ripping*) se desarrolle enormemente, exponiendo a los titulares de derechos de autor a una situación cada vez más peligrosa.

La conversión de formato no se limita actualmente al audio. Hoy día es relativamente fácil copiar una película en DVD a un disco duro o a otro DVD mediante alguno de los recientemente aparecidos grabadores de DVD. Si el DVD original dispone de una protección contra copias o un control de acceso sencillo, existen herramientas asequibles que permiten a los usuarios eliminar la protección y copiar el contenido del DVD en otros medios. Un contenido de vídeo puede comprimirse mediante un programa de compresión especializado, como el DiVX, (tecnología de compresión basada en MPEG-4) que reduce drásticamente el tamaño de la película sin perder demasiada calidad.

1.2.5 Intercambio de ficheros entre particulares (peer-to-peer)

Tal como se ha señalado anteriormente, la combinación de computadoras personales de elevada potencia, medios de almacenamiento digital, aplicaciones de red (como la web) y tecnología de conversión de formato (*ripping*), proporciona la oportunidad de transferir contenidos desde el medio original a medios controlados por el usuario. Una vez hecho esto, el contenido queda a libre disposición del usuario, a pesar de estar jurídicamente protegido por el derecho de autor.

La primera red de uso compartido o intercambio de ficheros que fue utilizada por un elevado número de usuarios de Internet fue Napster, que inició sus operaciones en mayo de 1999. La compañía proporcionaba un servicio por el cual los usuarios descargaban un programa que les permitía intercambiar ficheros de música sin cargo entre ellos. Constituía un primer servicio entre particulares (*peer-to-peer*), en el que los ficheros de música eran indexados en los servidores de Napster, permitiendo que los usuarios fueran direccionados hacia la fuente de los ficheros de su interés. Napster se consideró el pionero de dicho tipo de servicio para particulares.

Napster fue desde el principio extraordinariamente popular entre los usuarios. Sin embargo, desde el inicio de sus actividades, se enfrentó a cuestiones jurídicas al descubrirse que sus usuarios comerciaban con ficheros protegidos por derechos de autor sin el permiso de los titulares de dichos derechos. Nunca antes la industria de la música se había enfrentado con un fenómeno como éste, es decir, una gran comunidad de usuarios comerciando con contenidos en una red de intercambio de ficheros.

Napster fue denunciada por compañías productoras y discográficas por contribuir a la vulneración de los derechos de autor. El juez paralizó las actividades de Napster y dicha sentencia fue posteriormente confirmada por la corte de apelación. Napster entró en bancarrota y sus activos fueron vendidos a Roxio, una compañía de software.

La derrota de Napster no impidió que otras empresas proporcionaran servicios de intercambio de ficheros y programas conexos. Surgieron otras redes de servicios entre particulares (*peer-to-peer*), con tecnologías que no requerían de un servidor central, lo cual

hizo que las demandas legales fueran mucho más complicadas. Kazaa, Morpheus y StreamCast suministran programas o servicios que permiten el intercambio de ficheros, atrayendo a millones de usuarios que desean compartir contenidos diariamente en cantidades enormes. Se estima que actualmente se descargan de forma ilegal cada mes más de 2,6 miles de millones de ficheros de música, principalmente mediante servicios entre pares[1]. IFPI estima, además, que el 99% de todos los ficheros de música intercambiados en Internet son ficheros pirateados[2]. La industria de producción musical ha litigado agresivamente contra estos suministradores de servicios y de software, aunque en abril de 2003 un juez de los Estados Unidos de América emitió una sentencia favorable a Morpheus y StreamCast, concluyendo que al margen de distribuir software, no consideraba que dichas empresas fueran directamente responsables ya que no contribuían, ni activa ni materialmente, a las actividades ilícitas de los usuarios finales[3]. A principios de 2003, la industria ha denunciado ante los tribunales de los Estados Unidos de América a numerosos particulares (con los que se ha llegado rápidamente a acuerdos), los denominados usuarios "supernodo", responsables de facilitar la distribución de enormes cantidades de contenidos en campus de universidades. A finales de junio de 2003, se anunció que se estaba recopilando información para eventualmente denunciar a miles de particulares implicados en el intercambio de ficheros[4].

1.2.6 Situación actual de los titulares de derechos

La combinación de potentes computadoras, de capacidad para la conversión de la codificación de los contenidos (*ripping*), de medios de almacenamiento de gran capacidad y de sistemas de intercambio de ficheros, ha contribuido a que se produzca una situación muy complicada para los titulares de derechos. Cualquier contenido es actualmente susceptible de ser copiado y distribuido ilegalmente en Internet, con independencia del tipo de medio de que se trate. Lo que comenzó siendo una vulneración relacionada con los CD de música, se ha extendido a películas, libros y cualquier otro tipo de contenidos que puedan digitalizarse. La situación ha pasado a ser crítica para muchas empresas, que han visto cómo se reducían sustancialmente sus ingresos por la extensión de la piratería a nivel del consumidor.

Por este motivo, la industria de los contenidos está estudiando detenidamente la gestión de derechos digitales. En la sección 4 de este documento se incluye una descripción genérica de dichas tecnologías, junto con información sobre iniciativas específicas apoyadas por la industria de contenidos en relación con la gestión de derechos digitales y aspectos jurídicos y políticos conexos.

---

1 Véase *http://news.bbc.co.uk/1/hi/entertainment/music/2283072.stm*.

2 Véase *http://news.bbc.co.uk/1/hi/entertainment/music/2636235.stm*.

3 Véase *Metro-Goldwyn-Mayer Studios, Inc. contra Grokster, Ltd.*, CV 01-08541-SVW (25 de abril de 2003) (decisión admitiendo la solicitud de los demandados (Grokster y StreamCast) de un juicio sumario y denegando la solicitud de juicio sumario de los demandados), apelación pendiente No. 03-55894 (9th Cir. presentada el 29 de mayo de 2003).

4 Véase *Recording Industry To Begin Collecting Evidence And Preparing Lawsuits Against File 'Sharers' Who Illegally Offer Music Online* (nota de prensa de 25 de junio de 2003), disponible en *http://www.riaa.com/news/newsletter/062503.asp*.

1.2.7 Perspectiva jurídica – Los Tratados de la OMPI sobre Internet y otros aspectos

A lo largo de la década de los 90, los titulares de derechos han analizado las amenazas, pero también las oportunidades, de las tecnologías digitales. El hecho de que los contenidos estén disponibles en Internet y en otros medios de distribución digital, exige fortalecer la seguridad y protección de los contenidos, utilizando para ello las tecnologías DRM. Al mismo tiempo, la extensión cada vez mayor de sistemas de intercambio de ficheros, las posibilidades de la conversión de codificación y la facilidad para copiar y distribuir contenidos en ficheros digitales, preocupa enormemente a los titulares de derechos y les ha hecho adoptar una postura de recelo en relación con la autorización de uso de contenidos digitales. Por este motivo, al tiempo que titulares de derechos y distribuidores analizan posibles enfoques tecnológicos, también analizan con más detenimiento mecanismos jurídicos que puedan utilizarse para salvaguardar los contenidos legítimos de la copia y distribución no autorizadas.

El enfoque jurídico más comúnmente utilizado, y que se refleja en el litigio antes descrito contra Napster, ha sido el basado en los derechos del autor para perseguir a quienes facilitan o contribuyen a dichas prácticas. Los titulares de derechos han optado generalmente por no denunciar directamente a usuarios finales, las personas que participan directamente en las actividades tales como el intercambio de ficheros y que han infringido directamente los derechos de autor. Además, en relación con las personas individuales, la situación jurídica de algunas de las actividades, tales como la conversión de codificación de los CD propios (*ripping*) era ambigua, al menos en los Estados Unidos de América, donde hacer una copia de algo adquirido legítimamente constituye un uso lícito. No obstante, ha sido posible denunciar por realizar acciones que han contribuido a la vulneración de derechos a Napster y a otros servicios dedicados al intercambio de ficheros, en relación con las cuales los titulares de derechos han litigado agresivamente (particularmente las compañías discográficas y la industria cinematográfica) contra un número cada vez mayor de tales proveedores de servicios.

Desde principios de los años 90, los titulares de derechos, particularmente en los Estados Unidos de América, comenzaron a buscar en la tecnología, además de en las leyes, la forma de proteger sus obras. Además de considerar la utilización de la tecnología como una forma para proteger sus contenidos, se llegó a la conclusión de que tal enfoque no sería eficaz salvo que las leyes proporcionaran una protección mejorada para dichos procesos y sistemas. Tal como se ha indicado anteriormente, existían precedentes de protección jurídica de medidas tecnológicas: varios países ya habían otorgado protección jurídica a esquemas de acceso condicional utilizados en servicios por cable y otros servicios de televisión de pago[5]. Además, en los Estados Unidos de América, la Ley de la Grabación de Audio en el Hogar (*Audio Home Recording Act*) de 1992 prohibía la elusión de cualesquiera dispositivo, programa o circuito que implementara algún tipo de medida de carácter tecnológico (el sistema de gestión de copia en serie) utilizado para proteger música en formato digital en dispositivos de grabación digital o con interfaz digital, tales como los grabadores de cinta de audio digital [6].

---

[5] Los Estados Unidos de América prohíben la fabricación y venta de dispositivos utilizados principalmente para la desencriptación no autorizada de la programación emitida por satélite y por cable. 47 U.S.C. § 605(c)(4). En el Acuerdo de Libre Comercio de Norteamérica figuran disposiciones similares ("NAFTA" *North American Free Trade Agreement*), art. 1707(a).

[6] 17 U.S.C. § 1002(c).

En septiembre de 1995, la Oficina de Patentes y de Marcas Comerciales de los Estados Unidos de América publicó el informe *Intellectual Property and the National Information Infrastructure*, en el que trataba estos asuntos con detalle.[7] Redactado por un Grupo de Trabajo sobre Derechos de Propiedad Intelectual, el informe recomendaba que el Congreso elevara a rango de ley una enmienda a la Ley de Derecho de Autor (*Copyright Act*) de 1976, que prohibía la importación, fabricación o distribución de cualquier dispositivo, producto o componente que realizara un servicio cuyo "objetivo o efecto principal fuera . . . eludir, sin la autorización del titular de los derechos de autor o de la ley, cualquier proceso, tratamiento, mecanismo o sistema destinado a impedir la vulneración de un derecho exclusivo del titular del derecho de autor. . . ." [8].

Nótese que este enfoque sólo habría prohibido la provisión de un producto, y no el acto de la elusión. Además, la prohibición sólo se aplicaba a medidas tecnológicas destinadas a impedir la utilización no autorizada de derechos de autor, y no a las medidas de control de acceso.

Además, el Grupo de Trabajo recomendó que se protegiera la "información para la gestión de derechos de autor" y que se prohibiera la eliminación consciente y la distribución de información modificada. Se definió que la "información de derechos de autor" incluye el "nombre y otra información de identificación del autor. . . [y] del titular de los derechos del autor, términos y condiciones de uso..." [9].

Estas disposiciones resultaron ser controvertidas. Aunque se introdujeron en un proyecto de ley, nunca llegaron a formar parte de una ley. Sin embargo, el informe y las propuestas legislativas fueron el punto de partida de la posición negociadora y de la redacción del proyecto de tratado propuesto por los Estados Unidos de América en la ronda inicial de la Conferencia Diplomática sobre Ciertos Derechos de Autor y Cuestiones sobre los Derechos Conexos (Conferencia Diplomática de la OMPI de 1996). Dicha Conferencia diplomática culminó con la adopción del Tratado de la OMPI sobre Derecho de Autor ("WCT", *WIPO Copyright Treaty*) y el Tratado de la OMPI sobre Interpretación o Ejecución de Fonogramas ("WPPT", *WIPO Performances and Phonograms Treaty*) (conjuntamente denominados "los Tratados de la OMPI"), que se firmaron en Ginebra en diciembre de 1996. En la sección 3 de este documento se analizan el WCT y el WPPT, así como sus aplicaciones.

1.3 La DRM como forma de mejorar el acceso a los contenidos en línea

En esta sección se analiza la forma en la que la existencia de una red global modifica las formas tradicionales de acceso a la propiedad intelectual, para lo cual se tienen en cuenta los modelos de negocio de la "industria de los contenidos". A partir de ahí, se deduce la forma en la que la tecnología DRM puede permitir la introducción de nuevos modelos de negocio, mejorando el acceso a la propiedad intelectual de una forma beneficiosa, tanto para los titulares de derechos como para los usuarios.

---

7 Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights* (Oficina de Patentes y Marcas: 1995).

8 *Id.* en Apéndice 1, 6.

9 *Id.* en Apéndices 1, 6-7.

1.3.1 Modelos tradicionales de distribución de contenidos

Las cadenas de valor de la distribución tradicional crean valor allá donde existe escasez. Esto es así para la industria de contenidos y para cualquier otro producto. Los derechos de propiedad intelectual (en adelante: derechos de P.I.) crean dichos puntos de escasez para sus titulares: los creadores de propiedad intelectual (o sus derechohabientes) mantienen dicho derecho durante un tiempo limitado a fin de controlar el acceso a sus contenidos, creando un punto de escasez en la medida en que el contenido no es efectivamente sustituible (por cualquier motivo). El consumidor que desea acceder a una parte específica del contenido sólo lo podrá hacer en la medida en que el titular de los derechos haya autorizado la creación de puntos de acceso.

La vulneración del derecho de autor es algo tan antiguo como la propia legislación al respecto, y la existencia de leyes relativas al derecho de autor no ha sido nunca un obstáculo para quienes desean beneficiarse ilícitamente de la propiedad intelectual ajena. El derecho de autor ha sido, desde hace mucho tiempo, la forma de dar a los titulares de derechos la posibilidad de evitar el uso no autorizado de sus contenidos. Por sí sola, la ley no es suficiente para evitar completamente dichas utilizaciones, con independencia de que éstas se hagan con fines ilícitos o legítimos. Ello incluye los conocimientos técnicos y las inversiones necesarias para crear los medios físicos y acceder a la cadena de suministro (que , por ejemplo, constituye una barrera significativa a la piratería de libros en países con un sector editorial bien establecido).

1.3.2 Nuevos modelos de distribución a través de la red

Tal como se ha señalado anteriormente, el desarrollo de Internet supuso un desafío importante a cualquier modelo de distribución que dependa de la escasez del producto. Aunque las estadísticas pueden interpretarse de formas muy diferentes, a finales de 2002 había alrededor de nueve millones de sitio en la web a nivel mundial. También se estima que cada día se crean cuatro mil nuevos sitios. La comunicación entre particulares (*peer-to-peer*) en la red ha hecho que los contenidos puedan estar disponibles de una forma mucho más directa, incluso para quienes no tienen formación técnica. Es evidente que las barreras de entrada a la publicación (en su sentido más amplio) han caído drásticamente. Sencillamente, las barreras hasta ahora impuestas por cuestiones financieras y por la habilidad o capacidad para hacer que los contenidos pudieran quedar disponibles a nivel global han desaparecido.

Desafortunadamente para los titulares de los derechos, estos mecanismos no solamente hacen que sea más fácil realizar labores editoriales legítimas o ser un usuario igualmente legítimo de los contenidos, sino que también permiten que la gente pueda distribuir los contenidos sin tener autorización expresa para ello, ya sea de forma aislada o sistemática, y sin tener en cuenta que la distribución está legalmente prohibida. En consecuencia, en la medida en que existe un volumen cada vez mayor de contenidos accesibles para los usuarios sin que éstos tengan que pagar ningún canon, frente a tener que realizar pagos legítimos a quienes han producido los contenidos, se derrumban los modelos de negocio construidos en función de la escasez.

Aunque pueda argumentarse sobre el valor que aporta la denominada “economía del efecto red” basada en los beneficios derivados de la ubicuidad frente a la escasez (cuestión que admite pocas dudas desde una perspectiva teórica), es fácil demostrar la dificultad de realizar dicho valor en términos monetarios, es decir, encontrar formas de integrar dicho valor

en la cadena de valor del producto. Si el contenido está ampliamente disponible por nada a cambio, ello puede aumentar el valor potencial asociado al momento de creación, y por tanto, con el creador del contenido, pero ¿cómo puede materializarse dicho valor?.

Para que la aplicación de la tecnología a este problema sea efectiva, debe restablecer en cierta forma un punto de escasez en nombre de los titulares de derechos. Sin embargo, ello plantea una paradoja fundamental, que no ha sido olvidada por quienes han intentado implementar sistemas DRM, y es que el negocio de los editores (término utilizado en el sentido más amplio posible para incluir a todos los negocios que elaboran contenidos de cualquier tipo y en cualquier medio disponible al público) es proporcionar acceso a los contenidos y no impedirlo.

El objetivo fundamental de aplicar "medidas técnicas" para gestionar la distribución de la propiedad intelectual es equilibrar las demandas de los titulares de derechos para controlar y proteger la distribución de los contenidos con los intereses de los consumidores en tener acceso a dichos contenidos. Naturalmente, los consumidores preferirían acceder a los contenidos a cambio de nada; entonces, ¿porqué pagar por algo que puede obtenerse gratuitamente?. Existe asimismo la dificultad evidente de convencer a los consumidores del "valor" objetivo de los bienes intangibles. Sin embargo, salvo que el derecho de autor se abandone como mecanismo para el comercio de la propiedad intelectual, es esencial encontrar una respuesta a esta paradoja.

1. 3.3 Algunos escenarios de utilización de la DRM

Para que los sistemas DRM tengan éxito y sirvan para superar la paradoja de la ubicuidad / escasez, ¿qué tipo de aplicaciones deben utilizarse que sean atractivas para los consumidores?. A continuación se describen algunos escenarios posibles:

– Un consumidor descarga música en casa desde un servicio de red, y recibe el permiso necesario para escuchar la música mediante un dispositivo durante doce meses desde la fecha de la descarga (tantas veces como desee hacerlo); también puede pasar una copia de dicha música a hasta diez amigos sin coste alguno, pero ellos solo puede escucharla una vez si no han obtenido previamente una licencia propia. Sin embargo, el consumidor es recompensado como forma de gratificar su labor de distribuidor de ficheros protegidos, ya sea financieramente o en especies, por el titular del derecho de autor que se beneficia de la distribución a sus amigos.

– Un consumidor descarga una película estrenada recientemente. El permiso que recibe sólo le permite visionar la película tres veces durante un periodo de un mes. Transcurrido ese periodo, el fichero queda inaccesible salvo que se pague una nueva licencia. Sin embargo, los permisos también le permiten registrarse y conseguir una entrada para el cine de su localidad utilizable en cualquier momento del mes siguiente al vencimiento de su permiso.

– Un estudiante "visita" la biblioteca de su Universidad desde su habitación, que se encuentra fuera del campus, encuentra cinco artículos de periódico y varios capítulos de diversos libros que le son de utilidad para redactar un trabajo, los descarga en su computadora personal, quedando sólo disponibles sobre la base de un préstamo a corto plazo, es decir, en cinco días los ficheros descargados quedan inaccesibles. Sin embargo, la biblioteca tiene un acuerdo con un vendedor de libros electrónicos que ofrece descuentos sobre una gama de

libros que son de interés en relación con los artículos del periódico que descargó el estudiante. Esto se consigue mediante una correspondencia compleja entre metadatos utilizando DRM.

1.3.4 El futuro de la DRM – La computación confiable

Actualmente, la DRM sigue siendo una industria en proceso de consolidación. Si bien las tecnologías necesarias para proporcionar la funcionalidad de protección de derechos y contenidos en forma digital son cada vez más sofisticadas (tal como se expone más adelante en este documento), su aplicación no es aún generalizada, tanto por una cuestión de confianza de los titulares de derechos como por la resistencia del consumidor. Asimismo, a ello contribuye la existencia en internet de una gran cantidad de contenidos libres, pero ilícitos.

Aunque este problema se viene atacando mediante una combinación de demandas judiciales y desarrollando servicios de contenido de valor añadido, como los arriba señalados, en el futuro será necesario utilizar un enfoque más radical, empleando algunas de las tecnologías ya desarrolladas. Esta es una de las razones que apoyan lo que genéricamente denomina "computación confiable" ("*trusted computing*") o el desarrollo de "ingeniería segura".

Esencialmente, la computación confiable consiste en el desarrollo de dispositivos basados en microprocesadores (computadoras personales, PDA, teléfonos móviles televisiones, sistemas de alta fidelidad y cualquier otro dispositivo para reproducir contenidos que sea controlado mediante un microprocesador), incluyendo tanto programas como equipos para la protección de contenidos. En este caso, se entiende por contenido cualquier tipo de información entregada al dispositivo, incluyendo material protegido o no por derechos de P.I., pero cuyo titular desea que su acceso y utilización solamente se haga en condiciones predeterminadas.

Actualmente se están desarrollando varias iniciativas, algunas de ellas para fomentar la normalización (por ejemplo, la Alianza para una Plataforma de Computación Confiable, *Trusted Computing Platform Alliance*) y otras de carácter propietario (por ejemplo, la *Next-Generation Secure Computing Base* de Microsoft). Todas ellas pretenden crear un entorno de red que ofrezca confianza en base a la identificación segura de los usuarios, dispositivos y módulos de software, y la seguridad de que el contenido sólo puede explotarse utilizando reglas establecidas por los propietarios del bien. Aunque estas iniciativas suscitan muchas cuestiones, incluyendo aspectos relativos a la intimidad del usuario, existe el sentimiento común de que la combinación de seguridad basada en hardware y software ofrece un entorno seguro y de confianza. En dicho entorno, desaparece la distinción entre métodos para contenidos con DERECHOS DE P.I. y para contenidos sujetos a otras formas de protección jurídica (tales como la legislación sobre el secreto comercial o la protección de datos). Sin embargo, esta tecnología dista aún de estar asentada (incluso algunas opiniones auguran que nunca tendrá éxito) y por el momento, es necesario centrarse en tecnologías específicas diseñadas únicamente para la protección de los derechos de propiedad intelectual.

2. DESCRIPCIÓN DE LAS TECNOLOGÍAS DRM ACTUALES

2.1 Introducción

En esta sección se describen genéricamente tecnologías que pueden combinarse para proporcionar las funcionalidades requeridas para la DRM. Aunque todas las tecnologías descritas tienen implementaciones propietarias, el análisis realizado en este informe parte de la base de que todas las tecnologías propietarias son, en realidad, una respuesta a los requisitos que debe satisfacer una tecnología, requisitos que pueden expresarse en términos funcionales. Por lo tanto, es algo similar a un análisis de requisitos, pero sabiendo que existen comercialmente tecnologías que los satisfacen.

2.2 La DRM como conjunto de herramientas y componentes

Frecuentemente se asume que la tecnología DRM es un elemento monolítico de software que se instala y sirve para proteger los contenidos en línea. En la práctica, la DRM incluye una amplia variedad de tecnologías y servicios, algunos de los cuales pueden residir en un dispositivo de usuario, otros en el servidor de red de un comerciante y otros que, en general, pueden residir en la propia red.

En general, estas tecnologías pueden identificarse genéricamente como:

- Tecnologías para la identificación;
- Tecnologías de metadatos;
- Tecnologías de la lingüística de derechos;
- Tecnologías de encriptación;
- Tecnologías de asociación persistente o continuada;
- Tecnologías relativas a la privacidad;
- Tecnologías de pago.

Se han realizado numerosos estudios y desarrollos en los últimos años para determinar cómo pueden combinarse dichas componentes a fin de desarrollar un entorno seguro para contenidos con derechos de P.I. Dicha actividad ha sido realizada por empresas de *software* mediante actividades de normalización y de la comunidad académica. El consenso general es que el futuro de la DRM reside en una forma híbrida de servicios comerciales, software y componentes normalizados. El objetivo es generar un mercado competitivo en tecnologías, asegurando que el consumidor tenga la capacidad de acceder a los contenidos mediante sistemas DRM sin experimentar problemas debidos a barreras tecnológicas, tales como la incompatibilidad entre sistemas. Aunque las soluciones están aún en una fase inicial y la interoperabilidad sigue sometida a un intenso debate (véase más adelante), el camino a seguir está cada vez más claro.

2.3 Gestión de derechos digitales

La componente de infraestructuras de un sistema integrado para gestionar el acceso a la propiedad intelectual en un entorno de red, requiere el desarrollo de normas de infraestructura estrechamente interrelacionadas para la identificación y descripción inequívoca de la propiedad intelectual, incluyendo los derechos y permisos asociados a ésta.

Probablemente, el estudio más amplio publicado sobre los requisitos de la identificación y descripción del comercio de propiedad intelectual en la red ha sido el realizado en el seno del proyecto <indecs>.[10] Este proyecto ha desarrollado un modelo genérico muy sencillo de comercio, subrayando la necesidad absoluta de identificar cada uno de los elementos claves del modelo – el propio "contenido", las "transacciones" relativas al contenido y las partes de dichos acuerdos (ya sean individuos u organizaciones).

<indecs> consideró en su estudio que es irrealizable tratar de conseguir un sistema monolítico para la descripción e identificación global de todos los aspectos de la propiedad intelectual, y que, en lugar de ello, deben desarrollarse mecanismos que faciliten la interoperabilidad entre enfoques locales o sectoriales. La solución para una interoperabilidad efectiva reside en el diseño de los sistemas de identificación y descripción, que deben cumplir determinados principios lógicos para poder formar parte de una solución global destinada a la gestión de la propiedad intelectual.

2.3.1 Principios básicos de la identificación

Se entiende por "identificación" la adscripción de una etiqueta a algo de forma que pueda ser inequívocamente identificado por un tercero. La identificación inequívoca es esencial en cualquier proceso automatizado de negocio; ello es particularmente obvio en un proceso que requiera la comunicación más allá de los límites de la propia organización, en la que es improbable que los identificadores "locales" sean reconocibles por los partícipes en la cadena de suministro.

En ausencia de un marco de identificación monolítico, dichos identificadores sólo serán fidedignamente singulares cuando exista una autoridad de asignación de nombres, a la que generalmente se hace referencia como "espacio de nombres".

En general, aunque no siempre, los identificadores singulares son números. Un ejemplo fácilmente reconocible entre las industrias de contenidos es el siguiente:

ISBN 0 85021 294 4.

En este caso, las letras "ISBN" identifican el espacio de nombre – este identificador corresponde a la autoridad del Número Internacional Normalizado del Libro (*International Standard Book Number*); si el espacio de nombres se gestiona correctamente (como es el caso del ISBN), la combinación de espacio de nombre e identificador será inequívoco (en el caso del ISBN se identifica un producto que desea vender un editor).

Un sistema bien organizado para el comercio de propiedad intelectual requiere algo más que identificadores de productos (a veces conocidos como identificador de "unidad de producto comercializable"). Los sistemas de identificación son necesarios para permitir el reconocimiento inequívoco de otros aspectos de la propiedad intelectual. Esto puede entenderse más fácilmente describiendo la cada vez más numerosa "familia" de identificadores normalizados desarrollados para la gestión de la música.

---

[10] Véase *www.indecs.org*. Los participantes en el proyecto, financiado por la Comisión Europea dentro del programa Info2000, representan un amplio espectro de organizaciones relacionadas con la gestión de los derechos de propiedad intelectual.

En el cuadro siguiente se enumeran normas de identificación que han sido implementadas (o que están en proceso de serlo). A este respecto, la industria de la música está sensiblemente mejor desarrollada que otros sectores de medios; puede afirmarse que la gestión colectiva de derechos y la necesidad de comunicación entre sociedades de recaudación en distintos ámbitos territoriales ha sido la causa del nivel de desarrollo alcanzado.

Nombre y abreviatura del identificador	**Estado del identificador**	**¿Qué identifica?**
Código internacional normalizado de obras musicales (ISWC, *International Standard Musical Work Code*)	Norma internacional ISO 15707	El ISWC identifica obras musicales, es decir, la "abstracción" subyacente de una pieza musical. Tómese, por ejemplo, la "quinta Sinfonía de Beethoven" – un concepto que existe y que debe ser identificado independientemente de cualquier interpretación, grabación o partitura (pero que agrupa todos esos aspectos). El ISWC juega un papel central en la gestión de derechos de música.
Código internacional normalizado de grabaciones (ISRC, *International Standard Recording Code*)	Norma internacional ISO 3901	El ISRC identifica una grabación específica de una obra musical, independientemente del formato de la grabación (por ejemplo, un CD o un fichero en línea). Identifica una "interpretación" grabada de una obra musical. No identifica el medio de fijación específico.
Código internacional normalizado de música (ISMN, *International Standard Music Code*)	Norma internacional ISO 10957	Identificador (estrechamente relacionado con el ISBN, pero gestionado de forma independiente) utilizado para identificar elementos de música impresa (partituras) en la cadena de suministro.
Código de producto europeo/ Código de producto universal (EAN/UPC)	Norma de facto utilizada a nivel mundial	Estos identificadores son los más habitualmente utilizados para identificar "unidades de productos comercializables" (CD de audio, cintas de audio) en la distribución física. Frecuentemente, auque no necesariamente, se representan mediante un código de barras en el producto.
Identificador mundial de versión (GRID, *Global Release Identifier*)	Norma de comercio en desarrollo	Este identificador ha sido desarrollado por la industria de grabación para identificar "versiones electrónicas de música"; se ha descrito como el equivalente digital de un código de barras EAN (identificador de unidades de productos digitales comercializables).

Nombre y abreviatura del identificador	Estado del identificador	¿Qué identifica?
Número de parte interesada (IPN, *Interested Party Number*)	Norma de comercio implementada colectivamente por sociedades de gestión de derechos de autor musicales	Este identificador es el sucesor recientemente implementado del número de Compositor, autor y editor ("CAE", *Compositeur, Auteur, Editeur*). Ambos esquemas de numeración han sido desarrollados y son utilizados exclusivamente por las sociedades de gestión de derechos musicales de autor para la gestión colectiva de los derechos de sus miembros.
Número internacional de la base de datos de ejecutantes (IPDN, *International Performers Database Number*)	Norma de comercio implementada por sociedades de gestión de derechos de ejecutantes	Este identificador, que ha sido desarrollado independientemente del sistema de número de parte interesada por un consorcio de sociedades de derechos de ejecutantes, se utiliza para la administración colectiva de los derechos de los ejecutantes.

Identificadores de la industria de la música

Se ha elegido la música como ejemplo porque ilustra bien la complejidad de la tarea de identificación en una arquitectura de identificación relativamente madura. En el contexto de otros medios se reconoce actualmente la necesidad de requisitos similares. Por ejemplo, la industria del libro ha trabajado recientemente en el desarrollo de una norma para la identificación de obras textuales, en concreto el Código Internacional Normalizado de Obra Textual (ISTC, *International Standard Textual Work Code*) que debe convertirse en una norma de rango internacional durante 2003.

Lo que puede resultar más sorprendente del sistema de identificación de música es el requisito de acuse de recibo para la identificación de la parte. La identificación inequívoca de los titulares de derechos es esencial para la distribución exacta y efectiva de los fondos recaudados en su nombre. Sin embargo, dichos identificadores solamente se han aplicado hasta la fecha en partes aisladas de la industria musical, no siendo habitual que las etiquetas de registro identifiquen los artistas de forma consistente con los sistemas internos. La mayoría de los restantes sectores de la industria de contenidos no disponen de mecanismo efectivos para la identificación inequívoca de la parte[11].

El requisito de identificar a los titulares de derechos es simétrico de la necesidad de identificar a los usuarios de los derechos. Este aspecto pasa a ser especialmente sensible cuando se trata de la identificación de consumidores individuales. Existen sistemas de

[11] En este contexto, merece la pena señalar la utilización de "autoridades de nombres" por parte de bibliotecas. El proyecto InterParty (véase *www.interparty.org*) está actualmente explorando mecanismos para facilitar la interoperabilidad de "identificadores de personas" entre distintos sectores.

representación (*proxies*) útiles para la identificación individual que conllevan un riego contra la privacidad. Este asunto se trata más adelante en este documento en la sección sobre aspectos ligados a la privacidad (5.2.1).

2.3.2 Identificadores en la red

La mayoría de los identificadores analizados son anteriores al desarrollo de internet y puede parecer que tienen poca relevancia en el mundo actual de comunicaciones en red. El localizador universal de recurso (URL, *Universal Resource Locator*) tiene la ventaja sustancial de ser "activable" en un entorno de red: la acción de hacer "click" sobre un URL tiene el efecto de una actuación predecible, es decir, que su navegador apunte a un recurso específico en la Web (www).

Una acción predecible, pero no un resultado predecible, pues el resultado de "resolver" un URL en su dirección conlleva a menudo un resultado insatisfactorio (puede que no haya nada en el mismo o que lo que allí había haya cambiado). Al fin y al cabo, el URL es lo que pretende ser, es decir, el identificador de una ubicación pero no el identificador de lo que puede encontrarse en dicha ubicación. A este respecto, es como un marcador en una estantería de una biblioteca, le lleva a un lugar específico, donde puede encontrar o no lo que busca.

La comunidad de la red, representada por sus dos organizaciones de normalización, el Consorcio World Wide Web (W3C), y el Grupo de Trabajo de Ingeniería en Internet (IETF, *Internet Engineering Task Force*), han estado estudiando este asunto durante una década. Durante años se ha estudiado el marco conceptual para la identificación permanente en la red, es decir, el nombre universal de recurso (URN, *Universal Resource Name*). Sin embargo, la activación de los URN (y por tanto, su aplicación práctica) ha resultado ser bastante difícil.

La industria editora, liderada principalmente por editores de publicaciones científicas que rápidamente pusieron sus productos en línea, y que había identificado la necesidad de identificadores accionables permanentes de contenidos en la red, estableció en 1998 la Fundación Internacional para Identificador del Objeto Digital (DOI, *Digital Object Identifier*), un identificador de red accionable que utiliza la tecnología de "resolución" de asa (*Handle*) desarrollada por la *Corporation for National Research Initiatives* (CNRI). La CNRI afirmó que se trataba de la primera aplicación del URN.

Una ventaja potencial del DOI sobre otras soluciones reside en la capacidad de "resolución múltiple" del sistema de asa; en otras palabras, la actuación de un DOI es diferente en función del contexto en el que se utiliza. Sin embargo, sólo ahora se han entendido y demostrado las verdaderas implicaciones de la misma. Mientras tanto, se han propuesto implementaciones más genéricas de URN, y se han concedido nombres de domino URN de "alto nivel" a muchos de los sistemas de identificación existentes, habiéndose propuesto que un identificador como "URN: ISBN: 0850212944" sea accionable en la red.

Sin embargo, aún no existe dicha funcionalidad de red "nativa".

2.3.3 Identificadores y su gestión

El auténtico desafío de los sistemas de identificación radica en su gestión. Tim Berners-Lee, el "padre de la World Wide Web," ha afirmado que el problema de la utilización de los URL como identificador permanente es de naturaleza social más que técnica. Incluso los identificadores bien establecidos, como el ISBN, han tenido que hacer frente en su aplicación al reto que supone que algunos usuarios lo utilicen para identificar elementos "fuera de su ámbito" (el caso más conocido es el de la aplicación del ISBN a los juguetes basados en *software* (*soft toys*) que se distribuían a través de la misma cadena de suministro que los libros).

Aunque es esencial la claridad de las directrices de uso, poco puede hacerse para garantizar que los usuarios apliquen los identificadores de la forma en que éstos han sido concebidos. Un enfoque cada vez más utilizado es asegurar que los identificadores solo puedan aplicarse a cosas que pueden ser descritas con estructuras de metadatos mínimas asociadas al identificador.

En última instancia, la gestión de los identificadores es una cuestión de consenso, es decir, los usuarios tienen que encontrar ventajoso "respetar las reglas". Este no es un gran problema si se utilizan identificadores cuyo coste de la aplicación sea relativamente bajo. Sin embargo, el reto es mucho mayor cuando el coste de unificación del sistema de identificación sea relativamente elevado (como ocurre por ejemplo, con el identificador de objeto digital, DOI). En estos casos, las organizaciones pueden recelar de sistemas de gestión sobre los que les resulte difícil ejercer una influencia directa.

2.3.4 Identificación– Resumen de los aspectos más relevantes

La implementación de una infraestructura de identificación inequívoca para la gestión de derechos digitales será compleja y difícil. No todas las industrias de contenidos están igualmente convencidas de su necesidad. Sin embargo, en el sector en el que la infraestructura de gestión de derechos está más desarrollada (la música) se reconoce la importancia del reto planteado.

Sin embargo, los identificadores tienen en sí mismos poco valor, pues solo permiten establecer una vinculación sencilla entre sistemas que aseguran que ambas partes están hablando de "lo mismo". Lo que da valor al identificador es la capacidad de utilizarlo para vincular información sobre "lo mismo" en diferentes sistemas de computadoras.

2.3.5 Metadatos

"Metadatos" es un término utilizado de formas muy diferentes. Es un claro ejemplo del problema de la ambigüedad semántica que se analiza con detalle en esta sección. Por lo tanto, es importante definir cuál es la utilización particular de término adoptado en este informe: "metadatos" significa información que describe el "contenido" (formado por los "datos"). Esta definición, algo extravagante, responde a la interpretación que normalmente se hace en la industria de los contenidos.

La idea de "descripción" es ciertamente muy amplia. El proyecto <indecs> definió los metadatos en términos de expresión de relación, lo cual es una forma útil de tener en cuenta la amplitud de miras con las que algo (o alguien) puede ser descrito.

El objetivo principal de este documento se centra en los metadatos explícitamente asociados con identificadores, puesto que éstos son los metadatos de aplicación más directa a la "gestión de derechos digitales". La normalización de los metadatos está, en muchos aspectos, menos madura que las normas sobre identificadores, ya que es sólo ahora que se comienza a entender el significado de la interoperabilidad de los metadatos.

En este contexto, merece la pena señalar que en la cadena de suministro de información se ha venido compilando, y recompilando, una enorme cantidad de metadatos. En efecto, "la misma" información ha sido grabada por mucha gente, y el despilfarro que suponen dichas prácticas de recopilación y mantenimiento de datos, en términos de coste y calidad, ha incentivado el desarrollo de normas para compartir datos (y esfuerzos).

2.3.6 Identificadores y metadatos mínimos

La importancia de la relación entre sistemas de identificación y metadatos es algo cada vez más evidente para quienes trabajan en la normalización de identificadores. El Comité de la ISO denominado ISO TC46/SC 9, responsable de las normas para Información y Documentación / Descripción (responsable de las normas de identificadores ISO mencionadas en este documento) ha decidido que no elaborará ninguna norma sobre identificadores que no incluya una mínima especificación de metadatos.

Por ejemplo, la actual revisión de la norma ISBN incluye un conjunto mínimo de metadatos diseñados para ser registrados junto con el ISBN.

El objetivo principal de estos "conjuntos mínimos de metadatos" es la eliminación de la ambigüedad , es decir, debe de haber datos suficientes para diferenciar claramente dos cosas superficialmente similares pero diferentes (en otras palabras, para distinguir entidades que comparten algunos, pero no todos, sus atributos).

En lo que se refiere al sector de la edición de libros, se ha tenido cuidado en asegurar que las normas ISO de identificadores de metadatos se diseñan de forma que cumplan la norma de comercio ONIX. Ello garantiza una perfecta interoperabilidad entre diferentes conjuntos de metadatos en el mismo sector.

2.3.7 Interoperabilidad de los metadatos

Incluso si un determinado sector, como el de la edición de libros, tiene éxito en la definición de normas de comercialización, que sean ampliamente aplicadas por todo el sector, es poco probable que dichas normas resulten aceptables a través de las fronteras culturales, territoriales y lingüísticas.

En un mercado cada vez más global, y con la inevitable convergencia de medios que se produce desde el momento en que todos los tipos de contenidos se distribuyen a través de un canal de red común, es esencial la interoperabilidad a través de dichas fronteras.

Tal como ya se ha analizado (véase la sección 2.3), el proyecto <indecs> ha definido los requisitos que deben imponerse a los metadatos para que sean interoperables. Un requisito fundamental es que la terminología de los metadatos debe estar *bien conformada*, lo que sobre todo significa que debe estar definida de *forma adecuada e inequívoca*. A pesar de que gran parte de los esfuerzos dedicados a resolver el reto de la interoperabilidad se han centrado tradicionalmente en la *sintaxis*, el verdadero desafío reside en la *semántica*.

2.3.8 Semántica

El requisito de una semántica bien definida incrementa el papel que juegan los diccionarios de datos correctamente estructurados, diccionarios que definen los términos utilizados en un conjunto de metadatos de conformidad con un modelo de datos correctamente estructurado (esencialmente, una "visión" de las relaciones entre las diferentes entidades del conjunto de metadatos). A continuación se presenta información adicional sobre este asunto.

2.3.9 Lenguajes de expresión de derechos y diccionarios

2.3.9.1 Funcionalidad requerida

Una vez que el contenido se ha identificado y ha sido descrito, los titulares de derechos desean crear las reglas bajo las cuales los usuarios puedan acceder al contenido. Dichas reglas permiten a los titulares de derechos crear modelos de negocio, algunos de los cuales, que pueden resultar familiares o nuevos, se describen en la sección 1.3. Las reglas de esta naturaleza deben ser:

– Completamente expresivas – es decir, deben permitir que los titulares de derechos o cualquiera con mandato de éstos, expresen sus derechos e intereses sobre el contenido, así como los acuerdos contractuales relacionados con el mismo, de conformidad con diversos modelos de utilización y de negocio.

– Inequívocas – es decir, deben ser absolutamente precisas, de forma que no puedan interpretarse de forma diferente a lo pretendido por el titular de los derechos.

– Legibles por máquinas – es decir, las licencias deben poder ser leídas por computadoras y otros dispositivos basados en microprocesadores.

– Seguras – deben crearse de forma que se detecte cualquier intento de manipulación.

Esta es solo una lista básica de requisitos para el lenguaje de expresión de derechos, pero que puede considerarse que establece los requisitos mínimos. La utilización de un lenguaje para la expresión de derechos será clave para el futuro de la gestión de derechos digitales , puesto que proporciona la base de los modelos actuales y crea otros nuevos.

2.3.9.2 Descripción de la tecnología del lenguaje de expresión de derechos

Probablemente, la forma más fácil de entender la expresión o manifestación de derechos es explicarla en los términos utilizados para las instrucciones de una computadora. En este

caso, las instrucciones hacen referencia alo que un usuario puede hacer con un cierto contenido. El titular de derechos convierte su permiso en explicar términos humanos (*Usted puede copiar esto en su disco duro y reproducirlo diez veces*) en un lenguaje lógico que pueda interpretar un programa informático. El *software* en cuestión es el sistema de encriptación que protege el contenido al que el usuario desea acceder.

La tecnología del lenguaje de expresión de derechos se desarrolló inicialmente a principios de los años 1990 en el centro de investigación de Xerox en Palo Alto, California (*Xerox Parc Research Center*). Desde entonces, la tecnología ha alcanzado un creciente grado de sofisticación. Esencialmente, se basa en la noción de que se otorga un permiso a un usuario para que éste realice un acto determinado relacionado con un contenido protegido por derechos de propiedad intelectual. Por ejemplo, si un titular de derechos desea otorgar a un usuario el derecho de copiar un determinado contenido para ser reproducido en el disco duro de una computadora, es posible otorgar dicho derecho con determinadas condiciones. El titular de derechos puede desear que se evite que el contenido pase a una tercera parte (es decir, que no sea copiado de nuevo) o que sea modificado de cualquier modo. Se trata de un permiso o autorización sencilla que una expresión de derechos puede formular como expresión de derechos legibles por una máquina.

Un lenguaje de expresión de derechos se escribe en algún tipo de lenguaje de computadora, probablemente XML. Este es un lenguaje de computadora de alto nivel que también puede ser leído (con algunas dificultades) por un ser humano. El lenguaje XML, a veces denominado el lenguaje de la red, es ampliamente utilizado y su valor como lenguaje de expresión de derechos tiene la ventaja de su omnipresencia, lo cual contribuye a la interoperabilidad (véase 2.5.3.2).

2.3.9.3 Descripción de la tecnología de diccionario de datos de derechos

Un lenguaje de expresión de derechos requiere la utilización de términos extremadamente precisos (semántica) a fin de crear expresiones precisas e inequívocas. Sin embargo, desde hace mucho tiempo se reconoce que el lenguaje natural y el lenguaje de las computadoras son dos cosas bien distintas. El lenguaje cotidiano dista de la precisión habitual de una computadora, y la sociedad está construida sobre la base de que es esencial interpretar los matices del lenguaje. Por ejemplo, todo el entramado jurídico parte de la base de que no puede ser tan preciso como para excluir su interpretación.

Por su parte, las computadoras no pueden actuar en un contexto impreciso. Enfrentados con una expresión ambigua, las computadoras no funcionarán correctamente o lo harán de una forma impredecible. Por este motivo, es preciso crear una serie de términos (palabras) para su utilización específica en un lenguaje de expresión de derechos. Estos términos constituyen la base del diccionario de datos de derechos.

Un buen ejemplo de como el lenguaje natural puede ser problemático cuando se aplica al lenguaje de expresión de derechos es el término "*copia/copiar*" (en inglés, "*Copy*"), que se utiliza ampliamente en la legislación sobre derechos de autor (en inglés, "*copyright*"), siendo de hecho el origen en lengua inglesa del término "*copyright*" (derecho de autor), pero que en el ámbito de las computadoras resulta un término desatinado. Si bien copiar significa teóricamente hacer una réplica exacta de algo que es en todos sus términos lo mismo, los seres humanos somos conscientes de que ello requiere una interpretación. Aunque sepamos lo que de hecho significa "copiar", ello carece de sentido para una computadora. ¿Cómo puede ser

una cosa exactamente la misma que otra?, ya que en ese caso serían la misma cosa (la misma materia, en el mismo momento y lugar) y, por lo tanto, teóricamente no habría copia. Por eso, cuando se utilice el verbo *copiar* (*copy*) en un lenguaje de expresión de derechos que deba ser interpretado por computadoras, es esencial que desaparezca la imprecisión del término *copiar/copia* (*copy*). A mayor abundamiento, en caso de que un tribunal de justicia tuviera que interpretar la semántica del término *copiar/copia* (*copy*), no estaría garantiza que se hiciera en términos absolutamente precisos, por lo que resulta peligroso utilizar una expresión de derechos que incluya el término *copiar/copia* (*copy*) (véase 2.5.3.3).

2.3.9.4 Integración de la tecnología con las medidas de protección técnica

Tal como se ha señalado anteriormente, una expresión de derechos (formulada en términos de un diccionario de datos de derechos) es una instrucción que se da a un dispositivo basado en microprocesadores para que se comporte de una forma determinada. La instrucción alimenta un programa, que constituye una de las partes claves de un sistema de gestión de derechos digitales utilizado para proteger contenidos. Tal como se verá más adelante, la instrucción indica al programa los términos y condiciones bajo los cuales el contenido, actualmente inaccesible para el usuario, puede ser consumido. Para que una expresión de derechos tenga valor, debe interactuar sin perturbaciones con el programa de protección, de forma que las instrucciones que incluya puedan ser entendidas con precisión y permitan tomar las acciones pertinentes en base a las mismas.

Este requisito sugiere que un lenguaje de expresión de derechos deba poder trabajar con diferentes programas de DRM. Sin esta capacidad, un lenguaje de expresión de derechos permanecerá vinculado a un único sistema DRM y su uso sería limitado. La capacidad de integrar una expresión de derechos en varios sistemas DRM propietarios diferentes es, por tanto, una de las formas de ofrecer interoperabilidad a los usuarios de sistemas DRM. Si el mismo contenido, gobernado por una única expresión de derechos, puede ser consumido utilizando varios sistemas DRM diferentes, se reduce el trabajo de empaquetamiento de los titulares de derechos (que en otro caso deberían de elaborar diferentes expresiones de derechos en los diferentes lenguajes de los distintos sistemas DRM), así como los inconvenientes para los usuarios, ya que en ese caso una única expresión de derechos puede interactuar con la tecnología del proveedor de DRM elegido.

2.4 Gestión digital de derechos

Hasta ahora, debe haber quedado claro que la gestión de derechos de contenidos digitales requiere la identificación continua, la claridad en la descripción y la utilización de reglas precisas, en base a las cuales se puedan dar instrucciones inequívocas a los programas informáticos utilizados para la protección de contenidos.

En la sección siguiente se describen las tecnologías para proteger los contenidos de un uso no autorizado, a saber, la aplicación del cifrado y de claves digitales.

2.4.1 Funcionalidades de la tecnología de encriptación

Para proteger los contenidos del acceso no autorizado es necesario utilizar algún tipo de encriptación. La encriptación (cifrado), o proceso de hacer que la información no sea

reconocible, se ha desarrollado durante miles de años. Se ha utilizado ampliamente en aplicaciones diplomáticas y militares, particularmente en tiempos de guerra para ocultar información al enemigo, aunque su utilización en el comercio es más reciente. Es ampliamente utilizada en el sector bancario y en otras áreas financieras vulnerables, en las que el intercambio y seguridad de las transacciones de información van siempre unidos.

El proceso de encriptación mediante dispositivos basados en microprocesadores para la gestión de derechos digitales implica la utilización de algoritmos (procedimientos matemáticos) para la aleatorización de la información digital a fin de evitar que sea comprensible. De esta forma se puede proteger efectivamente del acceso no autorizado a la propiedad intelectual de titulares de derechos.

En la DRM se definen varios requisitos esenciales de la encriptación para que un sistema sea robusto con un nivel de seguridad suficiente que garantice que el contenido permanece seguro contra el acceso no autorizado o la manipulación.

– Seguridad suficiente : los sistemas de encriptación deben ser suficientemente seguros para el tipo de contenidos que desean proteger. Por ejemplo, es previsible que la publicación de un libro comercial necesite menos protección que un documento del gobierno que trate de secretos sobre armas nucleares. Debe existir un equilibrio entre el nivel de encriptación y la conveniencia del usuario.

– Conveniencia del usuario: los sistemas de encriptación no deben ser onerosos cuando el usuario deba utilizarlos. Por ejemplo, un sistema de encriptación que requiera que el usuario espere durante un periodo de tiempo que no sea razonable mientras que se ejecuta el proceso de seguridad, no es aceptable.

– Vulnerabilidad: incluso los mejores sistemas de encriptación acaban siendo descifrados. Sin embargo, un sistema de encriptación debe diseñarse en la mayor medida posible de forma que una brecha en su seguridad no ponga en peligro la seguridad de todo el sistema, sino exclusivamente la de un dispositivo o identidad específica.

– Renovabilidad: tras una ruptura integral de la seguridad, debe ser posible restaurar la seguridad de todo el sistema mediante una mejora o elevación del nivel de prestaciones del software [12].

– Revocabilidad : debe ser posible impedir el acceso de un usuario a un sistema seguro. Por ejemplo, si se sabe que la identidad de un usuario ha sido robada, debe poder evitarse que una persona no autorizada utilice dicha identidad para acceder al sistema suprimiendo los privilegios de la identidad robada.

Si bien la utilización principal de la tecnología de encriptación es para que actúe de contenedor o como a menudo se denomina “envoltorio de contenidos” (“*content wrapping*”), también se utiliza para otras aplicaciones. Por ejemplo, la encriptación forma parte de la tecnología de firma digital, mediante la cual puede asegurarse el origen y la integridad del contenido e identidades (para la protección de los derechos morales).

---

[12] Sobre este asunto véase en 3.3.2 el análisis realizado en el contexto del Taller sobre Gestión de Derechos Digitales de la Comisión Europea y la opinión de los titulares de derechos sobre la importancia de la renovabilidad.

2.4.2 Descripción de las tecnologías de encriptación

La encriptación digital se utiliza para proteger con una clave el contenido de forma que éste no sea accesible y, tal como ocurre en el mundo físico, hay candados (cifrado) y llaves (claves). Por lo tanto, uno de los aspectos más importantes de la tecnología de encriptación de DRM es la gestión de las claves que dan acceso al contenido encriptado. Obviamente, la seguridad y conveniencia de los procesos de gestión de claves es lo que marca la diferencia entre sistemas DRM "buenos" y "malos".

La encriptación digital utilizada en la gestión de derechos digitales utiliza dos tipos de procesos de gestión de claves. Uno es conocido como encriptación de clave simple y el otro se conoce como encriptación con claves privada y pública. El primer tipo es bastante sencillo. La Parte A (Ted) asegura el contenido que remite a la parte B (Alice). Para acceder al contenido, Alice debe tener la clave que utilizó Ted para asegurarlo.

La forma más fácil de explicarlo es mediante una analogía. Supóngase que la persona A (Ted) desea enviar una caja cerrada con un candado a la persona B (Alice). Para que Alice abra la caja cerrada por Ted, es necesario que tenga la llave de Ted (o una copia de la misma). Ello significa que Ted ha dado a Alice una copia de la llave o la propia llave. Es necesario que ambos se encuentren para la entrega, o bien, Ted podría enviar la llave a Alice por correo.

Este proceso de entrega de llave parece bastante satisfactorio hasta que se detectan ciertas debilidades. En primer lugar, obviamente Ted no puede enviar la llave en el mismo paquete que la caja (lo cual sería completamente inseguro), por lo que tendrá que pasar ésta a Alice en una transacción independiente. En segundo lugar, ¿qué ocurre si Ted desea dejar la caja para Alice en algún lugar público pero no conoce su dirección para poder enviarle la llave?. En este caso, Alice podría encontrar la caja cerrada pero no dispondría de la llave.

Aunque en primera instancia parezca imposible, suponga que Ted tiene una caja con un tipo de candado especial que él puede cerrar con su llave, pero que no puede abrir, porque sólo Alice tiene una llave que lo pueda abrir. Aunque puede parecer extraño, éste es el principio de la tecnología de encriptación utilizada en los modernos sistemas de encriptación aplicados a la gestión de derechos digitales. El proceso se denomina de encriptación de clave pública / clave privada.

Este sistema de encriptación explota una rama de las matemáticas denominada Aritmética Modular, en la que funciones unidireccionales permiten que un cálculo se realice en un sentido y sea prácticamente imposible deshacerlo en sentido contrario. Esencialmente, el proceso permite la generación de dos claves (digitales), una de las cuales cierra y la otra abre. El proceso de encriptación de clave pública / clave privada funciona porque es posible dar a alguien la clave de cierre (la que encripta), manteniendo la clave de apertura (la que desencripta) en el ámbito privado. De esta forma, solo la persona que posee la clave de apertura (que lógicamente debe mantenerse segura / privada) podrá acceder al contenido una vez que éste haya sido encriptado. Este proceso permite a un comerciante cerrar un contenido y transmitirlo por la Internet pública a un individuo concreto siendo éste el único que puede abrirlo o acceder al contenido.

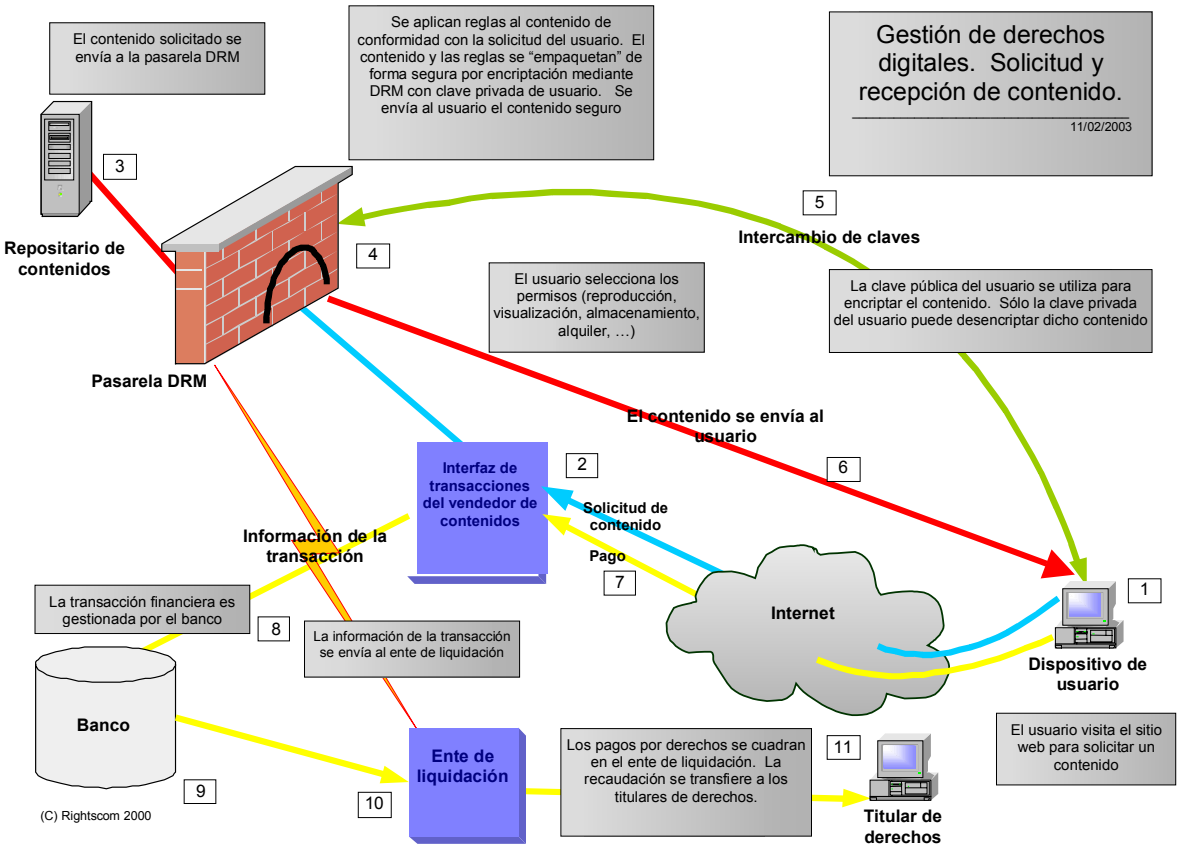
La ventaja singular de la utilización de la tecnología de clave pública / clave privada para DRM es que es posible asegurar que al contenido sólo puede acceder un usuario o dispositivo específico. Teóricamente, impide que un usuario A (Ted) entregue un contenido

al usuario B (Alice) y que éste transfiera su contenido a Mike, ya que al hacerlo Alice estaría dando acceso a su propia clave. Dando un paso más allá, en algunas implementaciones DRM la clave de Alice es inaccesible, de forma que no puede pasársela a nadie más, sino que solamente la puede utilizar localmente en su dispositivo para acceder o desbloquear los contenidos que reciba.

Sin embargo, nada se consigue sin pagar un precio por ello, y el precio de la encriptación mediante clave pública / clave privada es lo que se conoce como tara técnica. En este caso significa que la creación y procesamiento de contenidos seguros con encriptación de clave pública / clave privada requiere una gran cantidad de potencia de cálculo, lo cual ralentiza el proceso de interpretación o acceso al contenido. Para evitar este problema, la encriptación de clave pública / clave privada sólo se utiliza para guardar la denominada clave ordinaria proporcionada por el sistema DRM. Debido a que esta clave ordinaria bloquea y desbloquea el acceso a los contenidos, se mantiene segura mediante la clave privada del receptor, no siendo accesible a usuarios no autorizados. Estas claves ordinarias que se aseguran encriptándola utilizando la clave pública / clave privada sólo son útiles para una porción de contenido y a veces sólo se utilizan una vez, por lo que se denominan “claves de sesión”.

2.4.3 Transacciones DRM seguras

Para entender cómo se realiza una transacción segura entre el titular del contenido y el comprador del mismo, en el diagrama siguiente se muestran los pasos que han de darse. Los números del diagrama hacen referencia al orden de dichos pasos.



Una transacción DRM segura (© Rightscom 2003)

Un usuario (Alice) [1] contacta con un servicio de descarga [2] para conocer el inventario de su oferta. Una vez que hace una selección, el servicio de descarga [2] accede a un repositorio de contenidos [3] en el que el contenido deseado está disponible. La pasarela

DRM asegura el contenido [4] utilizando una clave de sesión a la que se da seguridad mediante la clave pública de Alice [5]. No importa que la pasarela DRM pueda acceder a la clave pública de Alice ya que ésta solo es la clave empleada para encriptar la información. El contenido se manda a Alice [1] asegurado mediante su clave pública. Alice [1] desencripta (accede) el contenido utilizando su clave privada exclusiva. Por supuesto, a cambio del contenido descargado, Alice [1] ha realizado un pago al servicio de descarga [7] que éste pasa al banco. Al mismo tiempo, el servicio DRM puede acceder a un sistema de liquidación [10] donde la descarga se cuadra con el precio o canon establecido por el servidor de descarga, que finalmente se transfiere al titular de los derechos (Ted).

Esta es una visión muy genérica de las actuaciones puestas en juego, pero describe con bastante exactitud los pasos que son necesarios. El modelo de sistemas de servicios entre particulares (*peer-to-peer*) anteriormente descritos en este documento puede explotarse fácilmente utilizando una funcionalidad de esta naturaleza. En ese caso, en lugar de ser Ted quien envía el contenido a Mike, lo envía Alice. Pero debido a que el contenido se asegura y no es accesible sin la clave de Alice (que ella no desea enviar o a la que ella no tiene acceso fuera de su propio dispositivo), Mike debe solicitar a Ted una nueva clave de sesión. Ted encripta una nueva clave de sesión con la clave pública de Mike y se la envía, de forma que éste pueda desencriptar el contenido enviado por Alice. Es previsible que este modelo, en el que un consumidor puede transferir un contenido a otro consumidor, sea en el futuro una forma significativa de distribución segura de contenidos.

2.4.4 Descripción de tecnologías de asociación persistente

En esta sección se presenta una visión general de varias tecnologías que pueden utilizarse para satisfacer requisitos de alto nivel a fin de asociar de forma persistente información con contenido. Estas tecnologías son: la marcación de huella ("*fingerprinting*"), la marca mediante filigrana ("*watermarking*") y la firma digital.

2.4.5 Funcionalidades de las tecnologías de asociación persistente.

Para gestionar y proteger la propiedad intelectual, es esencial identificar y describir adecuadamente el contenido disponible (es decir, los metadatos). Sin embargo, los metadatos deben *asociarse persistentemente* al contenido de forma que diversas aplicaciones, incluyendo los servicios anti-piratería, puedan acceder a los metadatos[13]. En el mundo analógico, dicha asociación entre el contenido y sus metadatos puede conseguirse imprimiendo un identificador en el *medio portador* de los datos (por ejemplo, imprimiendo un código de barras en la cubierta del CD o un código ISBN en una página de un libro). No obstante, este método no es viable en el mundo digital puesto que no existen dichos tipos de medios portadores que transporten los datos. Por tanto, es necesaria una tecnología que permita obtener los metadatos *a través del propio contenido*. Los principales requisitos de dicha tecnología son los siguientes:[14]

---

[13] Un ejemplo de asociación persistente de metadatos y contenido es la "marca de radiodifusión," que se analiza en 3.2.1.3(b).

[14] Nótese que no todos los requisitos se aplican a todos los casos.

– la tecnología debe poder establecer la vinculación entre contenido y metadatos con una elevada precisión;

– la calidad del contenido no debe verse degradada, es decir, no deben existir degradaciones perceptibles;[15]

– supervivencia en caso de alteración del contenido, tanto en el caso de operaciones "normales" (por ejemplo, redimensionar o recortar una imagen) como con intentos "maliciosos" de romper el vínculo entre el contenido y sus metadatos;

– supervivencia en el dominio analógico (es decir, la identificación debe ser aún posible cuando el contenido sea (a) decodificado, (b) reproducido, por ejemplo, en un altavoz analógico, y (c) redigitalizado,

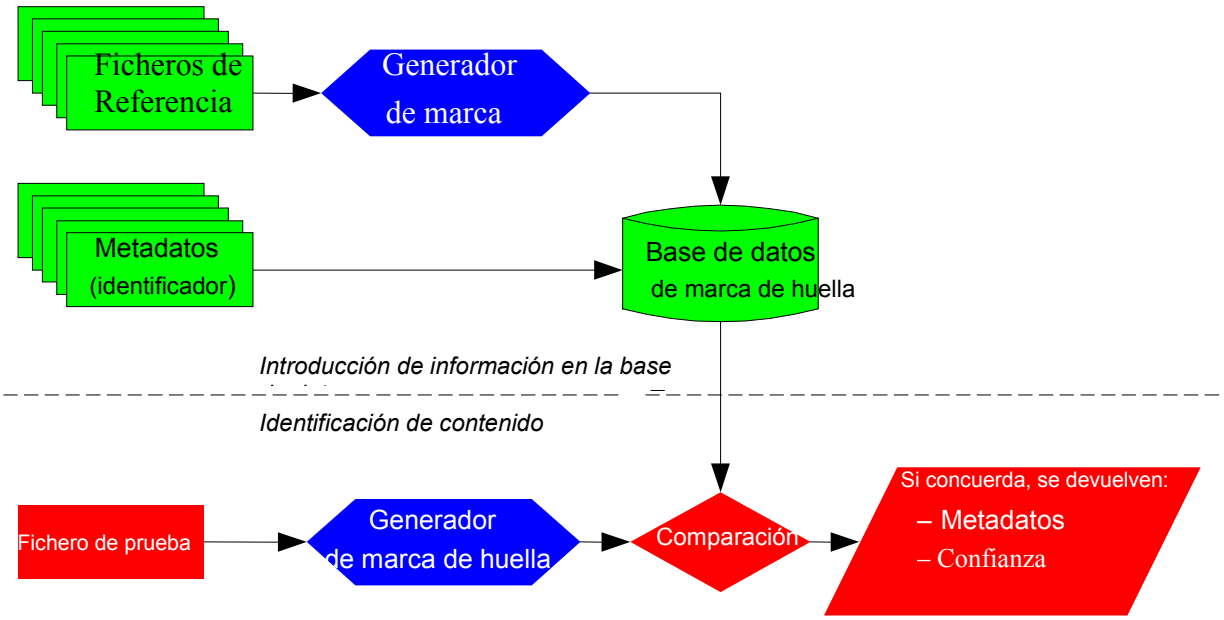
– la detección, respuesta a y procesamiento de los metadatos exige potencia de computación, debiendo minimizarse la sobrecarga de procesamiento de los dispositivos y del *software* en la mayor medida posible; y

– es esencial preservar la retrocompatibilidad de nuevos contenidos con dispositivos previamente existentes, así como la capacidad de que los contenidos anteriores puedan reproducirse en los nuevos dispositivos.

2.4.6 Marcación de huella ("Fingerprinting")

Las tecnologías de marcación de huella, o simplemente marcación, pueden utilizarse para identificar el contenido mediante el proceso que se representa en el diagrama siguiente. La marcación o "tecnologías de identificación basada en el contenido" funcionan extrayendo las características de un fichero y almacenándolas en una base de datos. Cuando esta tecnología se enfrenta a un fichero desconocido, se calculan las características del fichero y se comparan con las que están almacenadas en la base de datos con el objetivo de encontrar concordancias. Si se encuentra una concordancia, el sistema devuelve los metadatos adecuados de la base de datos de marcas (huellas).

[15] Con la excepción de las "filigranas visibles" utilizadas, por ejemplo, por las estaciones de televisión para incluir su logo en sus emisiones de televisión.



Sistema de marcación (de huella) o "fingerprinting"

Para utilizar la tecnología de marcación de huella es necesario realizar tres pasos:

– En primer lugar, debe disponerse de una base de datos con información, es decir, con "marcas (de huella) de referencia" debiendo incorporar a la misma los metadatos adecuados. Este paso, que se representa en el diagrama anterior, debe hacerse antes de intentar identificar un contenido desconocido;

– En segundo lugar, para encontrar información sobre un fichero (denominado "fichero de prueba"), el sistema genera una "marca (de huella) de prueba" a partir del fichero

de prueba. Esta marca de prueba se compara con todas las "marcas de referencia" almacenadas en la base de datos;[16]

– Cuando se encuentra una marca (de huella) concordante, los metadatos asociados con dicho metadato se toman de la base de datos de marcas (de huellas). Dichos metadatos constituyen el resultado del proceso.

Existen disponibles en el mercado programas y servicios que utilizan tecnologías de marcación (de huella) para distintos tipos de medios, tales como audio y video. El mejor de dichos sistemas identificará (para un medio concreto) correctamente más del 95% de los ficheros, incluso en condiciones adversas en que los ficheros hayan sido alterados de forma maliciosa para eludir el sistema de marcación. Algunas tecnologías pueden incluso alcanzar unos niveles elevados de concordancias positivas cuando el fichero de prueba se ha creado con un elevado ruido de fondo, como ocurre en un club (música).

Si bien las marcas (de huella) son muy efectivas para determinados tipos de contenidos, tienen menos capacidad para la identificación inequívoca de otros tipos de contenidos, en función del "detalle" que puedan proporcionar. Así, las marcas (de huella) son adecuadas para contenidos de audio, video y audiovisuales, así como para fotografías, pero lo son menos para gráficos de computadora[17] o texto.

Un campo tradicional para la aplicación de las tecnologías de marcación (de huella) de contenidos es la supervisión de una estación de radio para (a) compilar clips de audio emitidos y, desde la aparición de la MTV, videoclips, y (b) la distribución regalías (royalties) a los titulares de derechos por las sociedades de gestión o recaudación. Los sistemas de marcación (de huella) se utilizan cada vez más para supervisar las posibles vulneraciones del derecho de autor en sistemas de distribución de contenidos entre particulares. El escenario siguiente muestra otro ejemplo de utilización de la técnica de marcación (de huella): un usuario se encuentra en un bar o en un restaurante, y al escuchar una canción que le gusta activa su dispositivo de marcación (por ejemplo, su teléfono móvil), que reconoce la canción y transmite determinada información a un proveedor de servicio. Al llegar a casa, y mediante técnicas de DRM, el usuario encuentra en su buzón de correo electrónico la misma canción en forma de fichero de audio, que ha sido enviado por un sistema automático utilizando la marca (de huella) remitida desde el teléfono móvil para identificar la canción que le había gustado.

2.4.7 Marcación mediante filigrana ("watermarking")

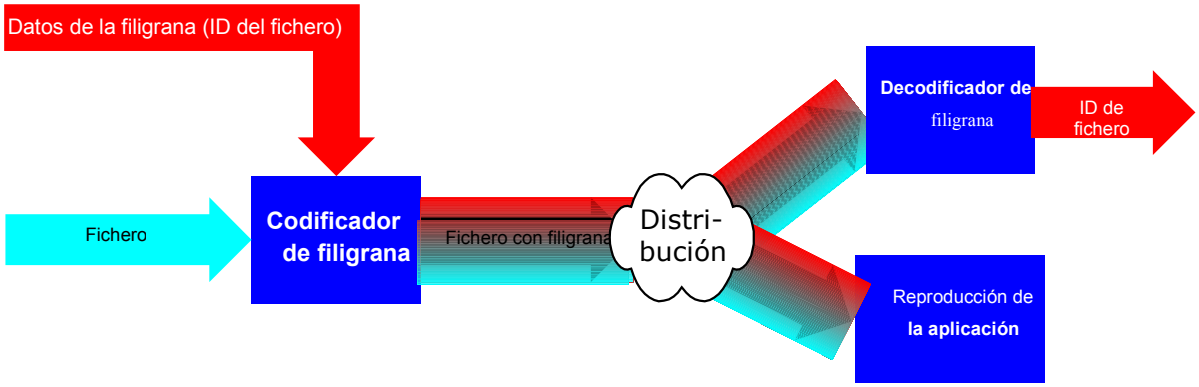
La marcación mediante filigrana (*watermarking)* se menciona a menudo cuando se analizan las tecnologías de protección de derecho de autor. Una marca mediante filigrana es una "información (imperceptiblemente) incrustada". Aunque dicha información

---

16 Nótese que esta comparación puede significar una tarea significativa cuando la base de datos de marcación (de huella) es grande. No obstante, las estrategias de bases de datos inteligentes pueden reducir los recursos necesarios a niveles aceptables.

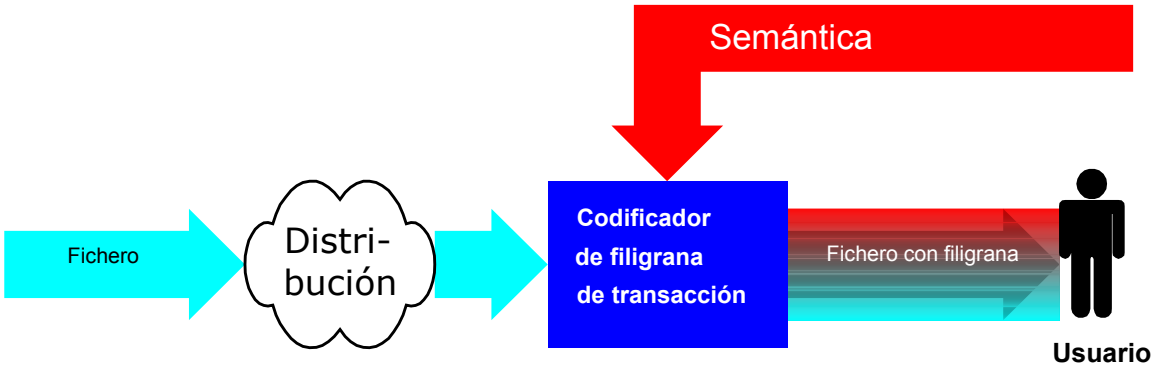
17 Naturalmente, las fotografías con pocos detalles (por ejemplo, una imagen de un cielo azul, despejado) puede ser menos compatible con las tecnologías de marcación (de huella) que un gráfico de computadora con muchos detalles.

(frecuentemente un fichero o un identificador de IP) sea imperceptible para el consumidor[18], puede ser extraída mediante un programa especial. Este "detector de filigrana" puede, cuando se aplica a un contenido sospechoso de haber sido pirateado, verificar si el contenido tiene la filigrana y, en consecuencia, admitir o rechazar la sospecha. Normalmente, en todos los ficheros distribuidos se incluye la filigrana digital antes de incorporarlos en la cadena de suministro. La figura siguiente muestra un diagrama de flujo funcional de este proceso.



Sistema de marcación mediante filigrana

Una segunda forma de utilizar esta misma tecnología es incrustar una "filigrana de la transacción" tal como se muestra en la figura siguiente. Las marcas mediante filigranas de las transacciones permiten establecer un vínculo entre un usuario arbitrario en la cadena de valor de contenidos y el contenido que éste haya "tocado". Cuando es necesario conocer ambos identificadores, de contenido y de usuario, pueden combinarse los dos tipos de marcación con filigrana.



Sistema de marcación mediante filigrana de las transacciones

El tamaño máximo de la "carga útil"[19] de la filigrana (sea una filigrana *a priori* o una filigrana de transacción) varía y depende del tipo de contenido, principalmente debido a la cantidad de datos que una filigrana puede transportar de forma fiable y continuada. En general, cuanto mayor sea el fichero, más datos pueden estar ocultos en el mismo.

---

18 Tal como se ha mencionado antes, no todas las filigranas son necesariamente imperceptibles, véase la nota 15.

19 La carga útil de la filigrana digital son los datos que permanecen "escondidos" (por ejemplo, el identificador utilizado para identificar unívocamente el fichero o la propiedad intelectual contenida en el mismo).

No obstante, la marcación con filigrana tiene algunos inconvenientes. Al igual que ocurre con la marcación de huella, las filigranas no pueden utilizarse con todo tipo de contenidos. Pequeños elementos gráficos, tales como logos o texto no pueden incorporar filigranas debido a la limitación general relativa a la cantidad de datos que pueden incrustarse en el contenido. El tamaño máximo de la carga útil de la filigrana depende de tres factores principales:

- Tipo de contenido (audio, video, imágenes estáticas, gráficos, texto);
- Tamaño del contenido:
  - Vídeo: velocidad de cuadro, tamaño de la imagen, relación de compresión, longitud;
  - Audio: velocidad de muestreo, relación de compresión, duración;
  - Imágenes estáticas: tamaño de la imagen, relación de compresión.
- Robustez:
  - ¿Qué "ataques" debe soportar la filigrana?;
  - ¿Debe la señal admitir un procesado normal, como por ejemplo, recorte, remuestreo o cambio de velocidad?, o bien, ¿podrían realizarse acciones más complejas sobre los datos, tales como girar una imagen algunos grados?

Puede decirse que en función del tamaño de la carga útil que debe incrustarse en un tipo de contenido, varía la robustez de la filigrana. Dado que dichas limitaciones son bastante severas en el caso de los algoritmos actuales de marca con filigrana, es algo generalmente aceptado que las marcas con filigrana sólo deben transportar una pequeña cantidad de información, normalmente un identificador de contenido. Una segunda limitación de las tecnologías de marca con filigrana, es que incrustarla significa modificar el contenido original. Si bien en muchos casos esta alteración no afecta a la calidad desde el punto de vista de la calidad percibida por el ser humano, ello puede hacer que sea difícil incrustar repetidamente filigranas en el mismo contenido sin que éstas se hagan perceptibles. Por tanto, las filigranas no pueden, por ejemplo, estar incrustadas durante el proceso iterativo empleado para el desarrollo de un anuncio.

En tercer lugar, todos los sistemas de marcación con filigrana hasta hoy conocidos, son susceptibles de ser eliminados sin afectar sustancialmente a la calidad del contenido, lo cual puede conducir a una situación en la que cuando se rompe un sistema de marcación con filigrana, el contenido originalmente gestionado se haga incontrolable.

Un inconveniente adicional es que la detección de la marcación mediante filigrana no puede aplicarse a un contenido previamente existente si inicialmente no se insertaron filigranas en el mismo.

La marcación con filigrana se han utilizado principalmente con contenidos de audio y de video para controlar material con derechos de autor. Algunos CD de audio contienen filigranas. Las filigranas, en forma de logos de TV, pueden ser añadidas por las estaciones de televisión a las señales que difunden, de forma claramente visibles y destinadas a evitar la

utilización ilícita del programa por otros radiodifusores. No obstante, no se pretende que dichas filigranas sean robustas frente a su supresión intencionada.

Dado que a menudo se confunden las tecnologías de marcación con filigrana y la marcación de huella, el cuadro siguiente enumera diferencias esenciales entre ambas.

Marcación de huella	Filigrana
Sirve para todos los tipos de medios (aunque es de aplicación limitada en alguno de ellos).	Sólo sirve para algunos tipos de medios.
No es necesaria la modificación de los ficheros. Por tanto, los usuarios sólo utilizarán un fichero "original" o fichero no alterado.	Es necesario incorporar la filigrana en los ficheros antes de que ésta pueda detectarse, lo cual puede, en algunas circunstancias, dificultar la utilización de dichos ficheros.
Susceptible a ataques maliciosos, aunque la tasa de éxito para ciertos sistemas y ciertos tipos de contenidos es superior al 95%.	Susceptible a ataques maliciosos.
Puede identificar contenido "preexistente".	No puede identificar contenido "preexistente"
La marca (de huella) no incluye datos. Sólo proporciona un enlace con una base de datos con una cantidad ilimitada de metadatos.	La cantidad de datos que pueden incluirse en una filigrana es muy reducida. Cuando la filigrana contiene un ID, puede establecerse un enlace con una base de datos que tenga una cantidad ilimitada de metadatos
Necesita una infraestructura con una base de datos que incluya marcas de huella.	La infraestructura sólo es necesaria para un análisis formal ante un tribunal
Necesita una infraestructura con una base de datos que incluya marcas de huella.	La infraestructura sólo es necesaria para un análisis formal ante un tribunal
	La efectividad de los sistemas de filigrana puede disminuir conforme aparezcan tecnologías más eficientes de compresión de contenidos– a pesar de las mejoras en las tecnologías de marcación mediante filigrana.

Marcación mediante filigrana ("watermarking") y marcación de huella ("fingerprinting")

2.4.8 Firma digital

Es importante que exista confianza en la información asociada al contenido (por ejemplo, identificadores y expresiones de derechos). Dicha funcionalidad puede conseguirse cuando la parte que añade los metadatos (a) firma digitalmente los metadatos, y (b) se sabe que está autorizada para añadir los metadatos. Una firma digital, similar a la firma manuscrita o rúbrica,[20] informa del origen de la información y si ésta ha sido alterada. Para asegurar que los metadatos asociados a un fichero no han sido modificados deben darse los pasos siguientes:

– El firmante calcula la función *hash* (o función resumen) del contenido y los metadatos;

El firmante cifra el valor del *hash* con una clave a la que solo él tiene acceso;

– El valor cifrado del *hash* (la "firma") se añade al fichero (que ahora contiene tres elementos: el contenido original, los metadatos y la firma); y

– La persona que desee verificar la firma puede utilizar la misma herramienta con la que el firmante firmó el algoritmo, utilizando la correspondiente clave, que se sabe procede del firmante.

El proceso de cuatro etapas descrito permite al usuario asegurar que el contenido no ha sido alterado, pero quien lo verifica no sabe si el firmante es quien tiene el derecho de añadir la información o empaquetar el contenido. Para confirmarlo, el firmante debe añadir un certificado a su firma. Este certificado, emitido por una agencia de certificación, identifica inequívocamente al firmante y lo hace identificable (y responsable) cuando se encuentren errores en los datos que ha suministrado

2.4.9 Gestión de la privacidad

Uno de los principales retos de la construcción de una infraestructura DRM efectiva reside en el mantenimiento de la privacidad, la confidencialidad y la protección de los datos personales. Existe una preocupación muy real y comprensible sobre el grado en que una infraestructura DRM efectiva para proteger la propiedad intelectual puede implicar, al mismo tiempo, una intrusión inaceptable en la vidas privada y comercial de las personas [21]. En la sección 5.2.1 se analiza este asunto con más detalle.

Los modelos de DRM dependen de que exista una infraestructura de "identidad confiable", que implique la identificación confiable del contenido, de los permisos

---

20 Cada vez más, los países están intentando que las firmas digitales tengan el mismo valor legal que las formas físicas (o rúbricas).

21 Para una visión especialmente siniestra y sombría de la DRM, véase el artículo de Richard Stallman, *The Right to Read*, publicado originalmente en *Communications of the ACM*, *f*ebrero de 1997, 40 No 2; que está disponible con notas del autor actualizadas en 2002, en *http://www.gnu.org/philosophy/right-to-read.html*. Aunque el tono de este artículo ha sido criticado por ser un tanto hiperbólico, debiera ser leído con atención por cualquiera interesado en el desarrollo de la DRM.

relacionados con el contenido y de las partes que gozan de los permisos relacionados con los contenidos. Este aspecto es particularmente sensible cuando las partes son consumidores individuales. Gran parte de la discusión sobre gestión de la privacidad parece estar centrada en el valor comercial que la información personal tiene a los efectos del marketing, junto con la alarma por "robo de identidad" y la utilización indebida de la información de las tarjetas de crédito. A pesar de la importancia de estos asuntos, es posible que los modelos tiendan a trivializar la cuestión subyacente del derecho a la privacidad.

Es previsible que la implementación adecuada de "tecnologías para la mejora de la privacidad" (PET, *Privacy Enhancing Technologies*) en la infraestructura DRM sea esencial para que los consumidores acepten la utilización de la DRM. Ello incluye las tecnologías utilizadas para mantener el anonimato, que permiten que "terceras partes confiables" (una organización confiable para el consumidor y para el distribuidor) autentiquen las identidades sin desvelar la identidad real del consumidor. A pesar de que dichos niveles adicionales de indirección pueden añadir una complejidad aparentemente innecesaria, es previsible que una infraestructura DRM que no tenga debidamente en cuenta las preocupaciones legítimas sobre privacidad y confidencialidad termine por fracasar.

2.4.10 Sistemas de pago

Los sistemas DRM utilizan varios tipos de modelos de pagos.

Una forma típica de pagar por un contenido es introducir el número de una tarjeta de crédito en una página web segura encriptada con el protocolo SSL. La utilización de tarjetas de crédito es la forma más común de comprar contenidos (y artículos) en línea. Estimaciones recientes de la compañía VISA, indican que los clientes europeos gastaron €2,57 miles de millones con tarjetas VISA durante el cuarto trimestre de 2002, lo cual significó un 136% más que lo gastado en el mismo periodo de 2001. Visa también estima que se realizaron 31,1 millones de transacciones en línea durante el cuarto trimestre de 2002, comparado con 14,5 millones durante el cuarto trimestre de 2001. Sin embargo, muchos usuarios aún son reacios a utilizar sus tarjetas de crédito directamente en un sitio web de un comerciante en línea por desconfianza sobre la privacidad y la seguridad, al tiempo que los comerciantes en línea se ven enfrentados a cuestiones relativas a su responsabilidad.

Aunque la mayoría de los pagos en línea se hacen mediante tarjeta de crédito, se han desarrollado o se están en desarrollo formas de pago alternativas. Por ejemplo, el portal de música Popfile.de en Alemania, ha desarrollado un sistema conjuntamente con Deutsche Telekom, que permite que los usuarios acceder a emisiones de datos en tiempo real ("*streaming*") así como descargar canciones con autorización basada en DRM y facturar por el contenido a través de la factura del teléfono fijo. También se han desarrollado varios sistemas de micropagos, que pueden llegar a convertirse en un método común de adquisición de contenidos basados en DRM, no solo en línea, sino también para adquirir contenidos desde móviles.

Varias compañías han desarrollado sistemas que permiten a los usuarios introducir su tarjeta de crédito una sola vez en un servidor central. Una vez que se ha registrado, el consumidor accede a una cartera electrónica, que puede utilizar posteriormente para comprar contenidos en portales en línea que estén asociados al sistema. El sistema asegura que guarda el anonimato y la privacidad, reduciendo el riesgo relacionado con la responsabilidad de los comerciantes. Otras compañías han desarrollado sistema de micropagos generalmente

procesados a través de teléfonos móviles, para transacciones de bajo precio, tal como un obra musical de un catálogo en línea, un libro electrónico o un artículo en la sección de pago del sitio web de un periódico.

2.5 Normalización de la DRM

La normalización o desarrollo de normas comunes constituye un aspecto crítico para el futuro de la gestión de derechos digitales (DRM). Muchas aplicaciones destinadas a la gestión y observancia de la protección de contenidos están basadas en normas, que resultan esenciales para las aplicaciones DRM y que se aplican en diferentes "fases" de la distribución electrónica de los contenidos. La utilización de normas en aplicaciones DRM es importante tanto para permitir el funcionamiento de dispositivos, aplicaciones y servicios de diferentes fabricantes a fin de intercambiar contenidos, como para los proveedores de servicios, que poseen y controlan la infraestructura DRM, los titulares de derechos, que están interesados en la máxima difusión de sus contenidos y los consumidores, que escuchan, visualizan y leen contenidos utilizando dispositivos y aplicaciones "reproductores" ("*players*"). El objetivo principal de utilizar sistemas y elementos normalizados en las aplicaciones DRM es conseguir la interoperabilidad de dispositivos, aplicaciones y servicios, esencial para el éxito de cualquier negocio que utilice DRM.

2.5.1 Normas formales e informales

Las normas pueden ser formales e informales. Las normas formales son las producidas como consecuencia del trabajo de organismos de normalización internacionalmente reconocidos, como por ejemplo la Organización Internacional de Normalización (ISO, *International Organization for Standardization*), y la Unión Internacional de Telecomunicaciones (UIT). Aunque se trata de organizaciones internacionalmente reconocidas, sus procedimientos tienden a ser lentos y hay quien piensa que no están preparadas para seguir el ritmo de cambio de la era de las computadoras. Junto con los organismos formales de normalización, existen otras organizaciones tales como el Grupo de Trabajo de Ingeniería de Internet (IETF, *Internet Engineering Task Force*) y el Consorcio World Wide Web (W3C). Aunque no son organismos formales de normalización, tanto el IETF como el W3C son fuentes fundamentales de normas sobre Internet y sus recomendaciones se adoptan de forma generalizada.

Las normas informales van desde normas apoyadas internacionalmente por todo un sector de la industria, como por ejemplo, el proyecto Difusión de Vídeo Digital (DVB, *Digital Video Broadcasting*) o la Organización para el Progreso de Normas de Información Estructuradas (OASIS, *Organization for the Advancement of Structured Information Standards*). Los miembros de ambas organizaciones proceden de la industria y trabajan en pos de soluciones que permitan a los fabricantes crear productos y servicios que sean utilizados por titulares de derechos y por consumidores. Están internacionalmente reconocidas y las especificaciones que desarrollan se consideran contribuciones muy importantes en el contexto técnico y regulatorio de la gestión de derechos digitales.

2.5.2 Normas relativa a la gestión de derechos digitales

Tal como se ha señalado en 2.3.1, muchos sistemas de identificación han sido normalizados y están gestionados por la ISO. La normalización internacional proporciona una garantía de estabilidad a cualquier sistema de identificación, que debe caracterizarse también por su longevidad, factores ambos esenciales para promover su aplicación generalizada. No obstante, también existen sistemas de identificación que no han sido desarrollados por la ISO, como es el caso de la norma DOI (véase 2.3.2).

La norma, inicialmente desarrollada para "metadatos", fue desarrollada por una comunidad de bibliotecas para poder compartir las tarjetas de catalogación de las mismas. Esta norma, denominada MARC, es aún ampliamente utilizada. Sin embargo, los metadatos para bibliotecas se han diseñado para apoyar sólo una clase de actividad de los usuarios (la "localización") sobre la base de que las bibliotecas disponen de patrones con puntos de acceso a sus archivos de existencias (tal como hacen los sistemas sucesores de éste en la práctica bibliotecaria habitual). ¿Cómo desea realizar sus búsquedas un usuario?: por una parte, a través del nombre del elemento (¿qué ediciones de tal libro hay en la biblioteca?) o por el autor (¿qué libros de tal autor hay en la biblioteca?), o por el asunto (¿qué libros sobre este asunto hay en la biblioteca?).

La tradición de metadatos sobre "localización" en bibliotecas se ha llevado a la práctica en línea mediante la norma "*Dublin Core*"[22], desarrollada principalmente por bibliotecarios y concebida inicialmente como una norma que constituye un "mínimo común denominador" para la localización en diferentes medios y sectores de Internet. Aunque se han hecho intentos para modificar el *Dublin Core* mediante la adición de "calificadores" a los 15 elementos originales, ello sólo ha servido, desafortunadamente, para hacer patente hasta qué punto el *Dublin Core* es conceptualmente inextensible (no dispone de una "visión" subyacente que se exprese a través de un modelo de datos coherente).

Desde hace tiempo se reconoce la necesidad de disponer de "datos de producto", que resultan de gran utilidad para trabajar con los canales de distribución. En particular, en el sector editorial, con su enorme número de líneas de producto y de nuevos lanzamientos de productos, se ha reconocido desde hace muchos años la necesidad de distribuir información sobre "catálogos de libros", inicialmente en forma de volúmenes impresos, pero más recientemente en diversas formas electrónicas que puedan ser cargadas en los sistemas de computadora de quienes los reciben (mayoristas y libreros).

Tradicionalmente, esta información ha sido recopilada por un número reducido de "agencias bibliográficas" en un ámbito geográfico determinado, pero conforme el negocio al por menor del libro avanza cada vez más hacia el ámbito en línea, dichas agencias han mejorado su oferta para incluir información de productos cada vez más sofisticada (por ejemplo, incluyendo imágenes de la portada) que pueden ser necesaria para impulsar la compra de los consumidores dada la imposibilidad de que éstos puedan ojear los libros. Aunque la industria discográfica no tiene un número tan elevado de productos, también ha visto cómo se han desarrollado una serie de agregadores que proporcionan información consolidada de productos a los vendedores al por menor.

---

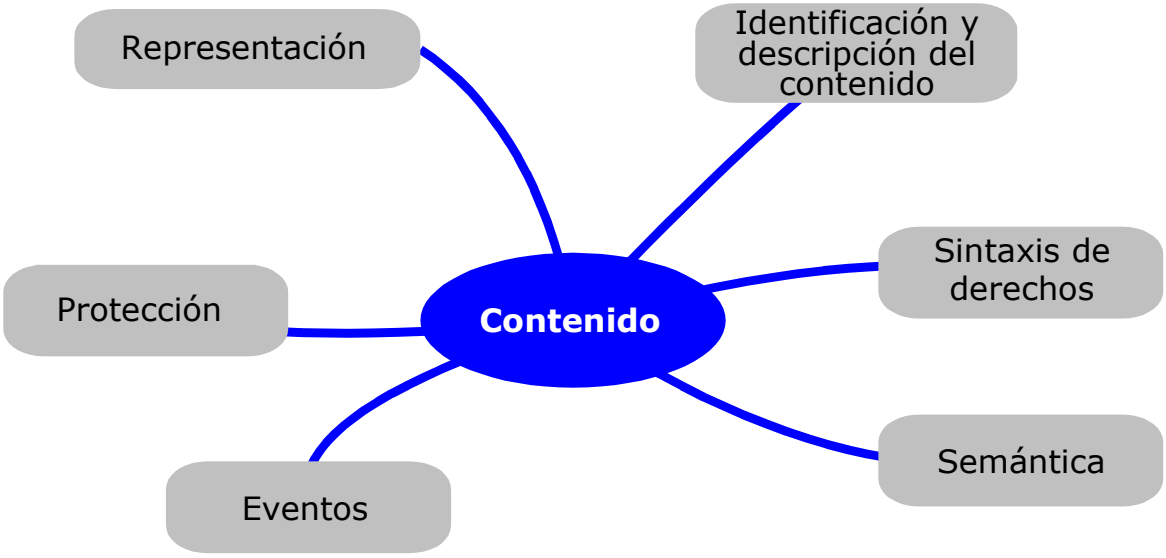
22 Véase *www.dublincore.org*.

La demanda de una capacidad cada vez mayor del sector del libro para comunicar "información valiosa sobre sus productos" es obvia y de ahí el desarrollo de la norma de intercambio de información en línea (ONIX, *online information exchange*). Esta norma, basada en XML, y que está siendo ampliamente implementada en la actualidad, permite la distribución de información completa del producto desde el punto de vista de la creación desde el editor y a través de toda la cadena de suministro (ya sea directamente o a través de intermediarios, que pueden ofrecer control de calidad y mejora de los datos, así como un carácter integral, que puede ser un atributo particularmente importante). Es previsible que se desarrollen normas similares para datos de productos de las industrias musical y audiovisual.

2.5.3 Normas relativas a la gestión digital de derechos

Son necesarios varios elementos para establecer una infraestructura normalizada coherente y funcional para aplicaciones DRM. La figura siguiente muestra los diversos aspectos que sirven para describir elementos del contenido (tales como ficheros de música, videoclips o libros electrónicos) en una aplicación DRM.

En las subsecciones siguientes se presenta un breve panorama general de dichos cualificadores:



Elementos del contenido y cualificadores conexos de DRM

2.5.3.1 Representación del contenido

La representación del contenido sirve para empaquetar contenidos. MP3 y MPEG-4 son normas típicas. En el contexto de la DRM, es importante poder representar asimismo metadatos y la estructura de elementos de contenido complejos. XML y MPEG-21 DID son ejemplos de normas de representación de contenidos típicas que pueden utilizarse en dicho contexto:

– El lenguaje de marcación extensible (XML, *eXtensible Markup Language*) es un lenguaje "Web" común utilizado con muchos fines. XML puede estructurar contenidos en línea, como por ejemplo texto, pero también metadatos asociados con cualquier contenido. Es menos adecuado para representar otros tipos de contenidos tales como ficheros de audio o de video.

– La declaración de elemento digital (DID, *Digital Item Declaration*) MPEG-21 forma parte de la norma marco MPEG-21[23]. Esta norma para la representación de contenidos proporciona la capacidad de declarar la estructura y los metadatos de elementos de contenido complejo. Por ejemplo, una versión de música en formato digital que incluya varias grabaciones sonoras, la portada, incrustaciones con la letra de las canciones, etc., ...

2.5.3.2 Sintaxis de derechos

La sintaxis de derechos, que técnicamente también es parte de la descripción del contenido, es un conjunto de términos para especificar reglas en relación con dicho contenido. Las sintaxis de derechos normalizadas se denominan a menudo lenguajes de expresión de derechos (REL, *rights expression languages*), tal como se describe en la sección 2.3.9. Un ejemplo de ello es el lenguaje de expresión de derechos MPEG-21 ("MPEG-21 REL").

La especificación del REL MPEG-21 describe la sintaxis y la semántica de la expresión de derechos. El lenguaje utiliza un modelo de datos central simple y extensible para sus conceptos y elementos más importantes. El modelo de datos incluye cuatro entidades básicas y las relaciones entre ellas. Las relaciones se definen mediante el elemento asertivo REL "*grant*" (concesión). Una aserción *grant* típica de REL MPEG incluye lo siguiente:

– el principal para quien se genera el *grant*;

– los derechos que especifica el *grant*;

– el recurso al que se aplica el derecho incluido en el *grant*; y

– la condición que debe cumplirse antes de que pueda ejercerse el derecho.

El modelo de datos básico se mejora mediante una serie de las denominadas "extensiones" que añaden funcionalidades. Por ejemplo, una de dichas extensiones puede utilizarse para mejorar el conjunto de condiciones que pueden aplicarse a los *grants*, proporcionando así una funcionalidad adicional. Es previsible que el REL MPEG-21 se convierta en una norma internacional durante el otoño de 2003.

2.5.3.3 Semántica

La sintaxis de derechos solo puede utilizarse cuando sus términos están bien definidos mediante una semántica subyacente. La semántica proporciona el significado exacto de los verbos y términos utilizados en cualquier lenguaje o, de hecho, la sintaxis de los derechos. El objetivo de las normas de semántica en este campo es permitir el intercambio de contenido entre dominios utilizando diferentes normas y sistemas de lenguajes de derechos. Por lo tanto, las normas semánticas pueden convertirse muy pronto en elementos importantes para la interoperabilidad entre aplicaciones DRM. La normalización de la semántica más destacada que actualmente está en desarrollo es el Diccionario de Datos de Derechos (RDD, *Rights Data*

---

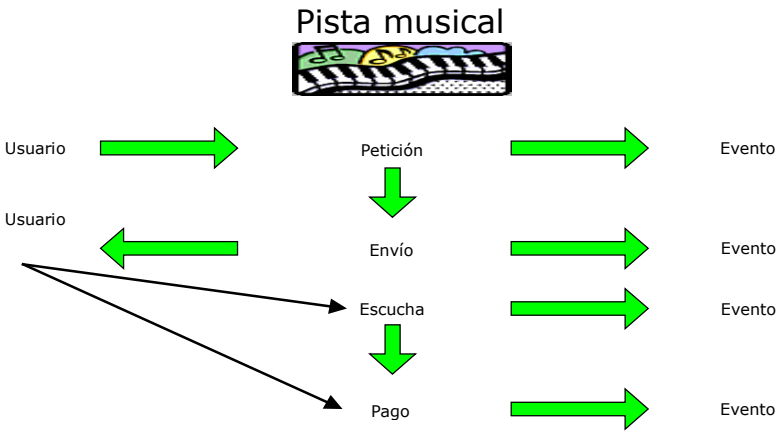
[23] Véase *www.telecomitalialab.com*.

Dictionary) MPEG-21 (véase en 2.3.9.3 un análisis sobre los diccionarios de datos de derechos).

El RDD MPEG-21 tiene por objetivo apoyar la implementación de un lenguaje de derechos para el intercambio seguro de propiedad intelectual en las redes mediante la provisión de un diccionario de datos interoperable relativo a los derechos. Esta iniciativa, basada en el análisis original de <indecs> (véase 2.3), está en marcha desde mediados de 2001.

2.5.3.4 Información de eventos

La provisión de información sobre eventos juega un papel principal en las aplicaciones de comercio electrónico relacionadas con el contenido. En cada paso de una transacción típica de comercio electrónico se genera un evento. Por ejemplo, la compra en línea de una canción, que incluye hacer el pedido, envío, audición y pago, generará los eventos que se reflejan en la figura siguiente:



Información de eventos

Las normas de información de eventos, tales como la información de eventos MPEG-21, puede por tanto, ser una parte importante de una aplicación DRM. Es previsible que la información de eventos MPEG-21 actualmente en desarrollo, incluya una biblioteca de "plantillas" de informe de eventos: el lenguaje de información de eventos MPEG-21 (ERL, *Event Reporting Language*), basado en el REL MPEG-21, mediante el cual un usuario puede solicitar y/o describir un evento, y el diccionario de información de eventos (ERD, *Event Reporting Dictionary)* MPEG-21, basado en el RDD MPEG-21, y que es la semántica que da cabida al ERL MPEG-21.

2.5.3.5 Protección del contenido

La protección del contenido, que impone restricciones a los contenidos digitales e impide el uso no autorizado del contenido, es también un elemento fundamental de un sistema DRM.

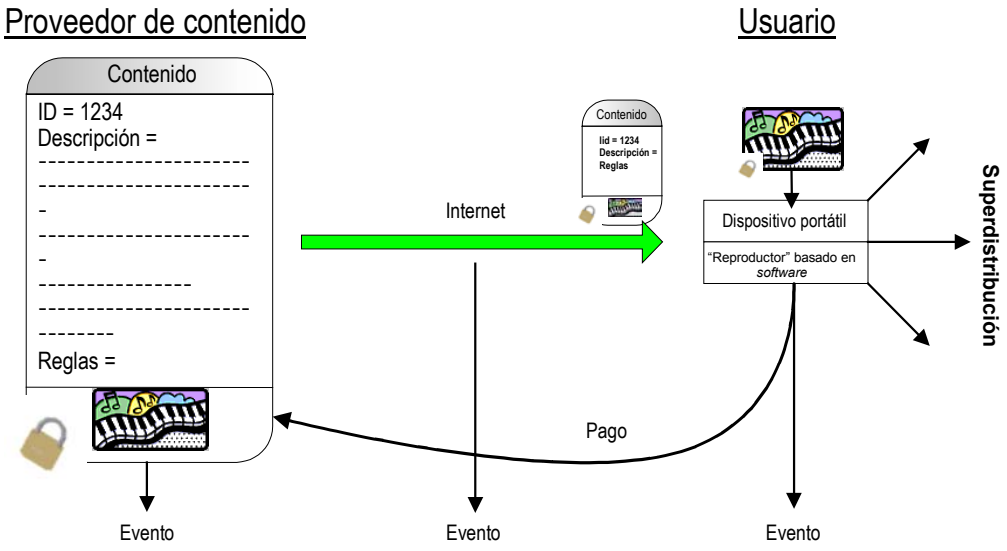
Las normas relativas a la protección de contenidos se ocupan directamente de la protección física del contenido. Incluyen normas de bajo nivel, tales como algoritmos criptográficos, normas de acceso condicional y normas de marca con filigrana, especificaciones de nivel medio, tales como las normas de protección inteligente de medios y especificaciones de alto nivel, tales como la IPMP MPEG-4.

El sistema de aleatorización del contenido (CSS, *Content Scramble System*) es una tecnología de protección de contenidos utilizada para proteger material audiovisual en soporte de videodisco DVD. La CCA DVD concede licencias de CSS a estudios y a fabricantes de dispositivos de reproducción de DVD (incluyendo reproductores externos e internos, y dispositivos integrados, tales como computadoras personales), así como de diversos componentes del sistema CSS. El CSS es una tecnología de protección de contenidos completa. Su protección se complementa con los términos y condiciones obligatorias de la licencia CSS, destinadas a asegurar la máxima protección al contenido del DVD, autorizando sólo determinadas salidas e imponiendo normas de "robustez" a los fabricantes de los productos. Aunque el CSS ha sido pirateado por DeCSS, la tecnología sigue siendo utilizada para proteger contenidos en videodiscos DVD.

MPEG ha impulsado otro enfoque para hacer cumplir las normas, no especificando todo el sistema de seguridad, sino proporcionando un marco para obligar a la protección del contenido. Por lo tanto, la norma admite "incorporar" soluciones propietarias.

2.5.3.6 Imagen completa

Tal como se ha descrito anteriormente, la representación del contenido, su identificación y descripción, la sintaxis de los derechos, la semántica, la información de eventos y la protección de contenidos son cruciales para la construcción de un sistema DRM. Se debe tener en cuenta que cada elemento se basa en otro elemento, tal como se muestra en el diagrama de flujo siguiente:



Flujo operativo de la protección del contenido

El proveedor de contenido "envuelve" al contenido en un contenedor, que incluye el fichero (en este caso la canción). El contenido incluye también un identificador único (por ejemplo, ISRC), un conjunto de descripciones, un conjunto de reglas (con una semántica implícita) y la propia canción (por ejemplo, un fichero MP3).

Una vez envuelto, el contenido está listo para "viajar" a través de internet hasta el usuario. El usuario puede reproducir el contenido en un reproductor basado en *software* o en un dispositivo a medida. Es importante destacar que el ID inicial, la descripción, las reglas y los procedimientos permanecen asociados a los datos. Ello permite que el proveedor de contenidos sea remunerado por el usuario por la reproducción del contenido e informado con exactitud (información de evento), por ejemplo, de la frecuencia de reproducción del contenido. El usuario puede también enviar el contenido (si lo permiten las reglas) a otro usuario (lo que se denomina "superdistribución").

3. MARCO JURÍDICO VIGENTE

3.1 Obligaciones de los tratados internacionales

3.1.1 Tratados de la OMPI sobre Internet

3.1.1.1 Disposiciones contra la elusión

El Tratado de la OMPI sobre Derecho de Autor (WCT, *WIPO Copyright Treaty*) y el Tratado de la OMPI sobre Interpretación o Ejecución de Fonogramas (WPPT, *WIPO Performance and Phonograms Treaty*) han establecido un nuevo marco jurídico internacional para la protección basadas en medidas tecnológicas, tales como las tecnologías DRM, utilizadas para salvaguardar los contenidos del acceso y uso no autorizado. Los Tratados de la OMPI fueron el resultado de una intensa negociación antes y durante la Conferencia Diplomática. Para entender cabalmente las obligaciones impuestas por el tratado que

finalmente fue aprobado, resulta de utilidad comparar la Propuesta Básica[24] que se presentó a los delegados antes de la Conferencia Diplomática con el texto final.

El Artículo 13 de la Propuesta Básica prohibía "menoscabar la protección" –o acción de elusión– de dispositivos y de servicios, a sabiendas de que se utilizarían sin autorización para el "ejercicio de los derechos en el presente Tratado," es decir, los "derechos de autor"[25] El Artículo también hubiera requerido que las Partes Contratantes proporcionaran "recursos adecuados y eficaces" contra los actos ilícitos. Finalmente, la Propuesta Básica no definía las medidas de protección tecnológicas, ya que el proyecto de texto establecía la prohibición de "cualquier dispositivo, producto o componente incorporado en un dispositivo o producto cuyo principal propósito o efecto sea eludir todo procedimiento, tratamiento, mecanismo o sistema que impida o inhiba cualquiera de los actos cubiertos por los derechos establecidos en virtud del presente Tratado.".

La Propuesta Básica se hubiera aplicado solamente a medidas de control del derecho de autor (no para el control de acceso), y sólo a dispositivos y servicios, no al acto de elusión. El texto se modificó durante la Conferencia Diplomática. El Artículo 11 del WCT, titulado "Obligaciones relativas a las medidas tecnológicas," señala lo siguiente:

> *"Las Partes contratantes proporcionarán protección jurídica adecuada y recursos jurídicos efectivos contra la acción de eludir las medidas tecnológicas efectivas que sean 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 las autores concernidos o permitidos de la ley."*[26]

El Artículo 18 del WPPT adopta fundamentalmente el mismo lenguaje.

---

[24] Véase la Propuesta básica de las disposiciones sustantivas del tratado sobre ciertas cuestiones relativas a la protección de las obras literarias y artísticas para consideración por la conferencia diplomática, preparado por el Presidente de los Comités de Expertos sobre un posible Instrumento para la protección de los derechos de los artistas intérpretes o ejecutantes y los productores de fonogramas (documento CRNR/DC/4 de la OMPI, de 30 de agosto de 1996), disponible en: http://www.wipo.int/spa/diplconf/index.htm ["Propuesta Básica"].

[25] "Artículo 13. Obligaciones relativas a las medidas tecnológicas

1) Las Partes Contratantes declararán ilícita la importación, manufactura o distribución de dispositivos que menoscaben la protección, o la oferta o prestación de cualquier servicio con el mismo efecto, por cualquier persona que sepa o tenga bases razonables para saber que el dispositivo o servicio será utilizado para el ejercicio de los derechos previstos en el presente Tratado, o en el transcurso de dicho ejercicio, que no esté autorizado por el titular del derecho o por la ley.

2) Las Partes Contratantes establecerán los recursos adecuados y eficaces contra los actos ilícitos mencionados en el párrafo 1).

3) Para los fines del presente Artículo, se entenderá por "dispositivo que menoscabe la protección" cualquier dispositivo, producto o componente incorporado en un dispositivo o producto cuyo principal propósito o efecto sea eludir todo procedimiento, tratamiento, mecanismo o sistema que impida o inhiba cualquiera de los actos cubiertos por los derechos establecidos en virtud del presente Tratado."

[26] Artículo 11 del Tratado de la OMPI sobre Derecho de Autor (aprobado el 20 de diciembre de 1996).

Ambos artículos dan un margen de flexibilidad sustancial a las Partes Contratantes para determinar cómo implementar estas obligaciones. En tanto que la protección jurídica sea "adecuada" y los recursos jurídicos "efectivos," se cumple con la obligación. No tienen porqué ser a toda prueba y prevenir cada posible tipo de acto de elusión. En particular, los textos no impiden que las Partes Contratantes puedan establecer excepciones y limitaciones adecuadas a las protecciones y recursos jurídicos, en tanto que éstas no menoscaben las protecciones previstas por las Partes Contratantes como "medidas tecnológicas efectivas".

Por lo tanto, ¿qué requiere el Artículo 11?. En primer lugar, ¿requiere la prohibición de cualquier acto de elusión y la comercialización de dispositivos y servicio para la elusión?. Aunque el lenguaje es ambiguo, tiende a una interpretación más próxima a centrase en el acto de la elusión que en los dispositivos, como hacía la Propuesta Básica. No obstante, prohibir solamente las tecnologías puede ser admisible porque sería una forma (o una forma adicional) para evitar efectivamente dichos actos de elusión.

En segundo lugar, el Artículo 11 solo prohíbe la elusión de medidas tecnológicas "efectivas". Sin embargo, no es necesario que una medida tecnológica sea completamente "efectiva" para que disfrute de las protecciones a las que obliga el Artículo 11; si fueran completamente efectivas, obviamente no sería necesaria una prohibición legal contra los actos de elusión de la misma, ya que en ese caso, la tecnología sería, por definición, inmune a la elusión.

En tercer lugar, el Artículo 11 trata de las medidas utilizadas en relación con el ejercicio por parte del autor de sus derechos de propiedad intelectual al amparo del Convenio de Berna y del WCT. En la medida en que un autor utiliza una medida tecnológica para ejercitar derechos que están más allá de los que garantiza el Convenio de Berna (por ejemplo, cuando los usos corresponden a las limitaciones o excepciones a los derechos de autor, tal como es el caso de uso lícito), podría decirse que el Artículo 11 no requiere que una Parte Contratante prohíba las acciones de elusión en relación con dicho uso.

En cuarto lugar, ¿existen medidas tecnológicas que sólo realicen "control de acceso," pero no el control del derecho de autor, sujetas a la protección que otorga el Artículo 11, dado que en el Convenio de Berna no existe expresamente el "derecho de acceso"?. También se ha señalado que puesto que los autores pueden autorizar, y de hecho autorizan, el acceso a sus obras, y dado que una medida de control de acceso puede efectivamente "restringir" cualquier acceso no autorizado, la última cláusula del Artículo 11 abarca medidas tecnológicas (además de medidas que aplican el control del derecho de autor).

En cualquier caso, tal como se ha sugerido anteriormente, el Artículo 11 no prohíbe a las partes Contratantes aplicar protecciones de medidas tecnológicas que excedan los requisitos de los Tratados de la OMPI. Además, los tratados de la OMPI permiten a las Partes Contratantes utilizar los recursos jurídicos existentes contra la elusión de medidas tecnológicas, incluyendo las DRM. A este respecto, el Artículo 11 del WCT y el Artículo 18 del WPPT no requieren una nueva legislación específica contra la elusión y, ciertamente, algunos países han establecido desde entonces que sus regímenes jurídicos son adecuados y efectivos para cumplir sus obligaciones recogidas en los Tratados de la OMPI.

3.1.1.2 Información sobre la gestión de derechos

Los Tratados de la OMPI también establecen referencias comparativas en relación con la protección de la información sobre gestión de derechos. La información sobre gestión de derechos se define como información que identifica a la obra, al autor o al titular de cualquier derecho sobre la obra, o información sobre términos y condiciones de utilización de las obras, así como cualquier número o código que represente dicha información.

El Artículo 12 del WCT y el Artículo 19 del WPPT requieren que las Partes Contratantes proporcionen "recursos jurídicos efectivos y adecuados" contra dos tipos de actos. Las personas que con conocimiento de causa, realicen actos sabiendo que inducen, permiten, facilitan u ocultan una infracción (o tiene motivos para conocer que sus actos tendrán ese efecto) no pueden:

– suprimir o alterar sin autorización cualquier información electrónica sobre la gestión de derechos; o

– distribuir, importar para su distribución, emitir, o comunicar al público, sin autorización, ejemplares de obras sabiendo que la información electrónica sobre la gestión de derechos ha sido suprimida o alterada sin autorización.

3.1.1.3 El entorno digital

El WCT también estableció algunos derechos amparados por derechos de autor, incluyendo el derecho de distribución del autor y el derecho de comunicación al público, "comprendida la puesta a disposición del público de sus obras, de tal forma que los miembros del público puedan acceder a estas obras desde el lugar y en el momento que cada uno de ellos elija"[27]. Los titulares de derechos consideran que disponer de estos derechos es crítico para hacer un mejor uso de las oportunidades en un entorno digital. Dichos derechos son especialmente importantes para la distribución de contenidos en Internet y a través de otros medios digitales, incluyendo la televisión, ya sea radiodifundida o por cable. Sin embargo, en relación con las preocupaciones de algunas naciones y comunidades de usuarios, el Artículo 10 establece expresamente que las Partes Contratantes podrán prever "limitaciones o excepciones impuestas a los derechos concedidos a los autores" en la medida que dichos casos especiales "no atenten a la explotación normal de la obra ni causen un perjuicio injustificado a los intereses legítimos del autor" [28]. Igualmente importante, la Declaración Concertada que acompaña al Artículo 10 deja claro que los estados Miembros pueden "ampliar debidamente las limitaciones y excepciones al entorno digital, en sus legislaciones nacionales" y "establecer nuevas excepciones y limitaciones" adecuadas al entorno digital [29]. El grado en el que las DRM y la legislación nacional destinada a aplicar las disposiciones contra la elusión de los Tratados de la OMPI, incluya, como asunto de carácter práctico y técnico, las políticas reflejadas en el Artículo 10 y en la Declaración Concertada que la acompaña, se analiza más adelante en esta sección 3 y en 5.1.2.

---

27 WCT, Art. 6 (derecho de distribución) y Art. 8 (derecho de comunicación al publico).

28 *Id*. en el Artículo 10.

29 *Id.* en la Declaración Concertada relativa al Artículo 10.

3.1.2 Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (el Acuerdo sobre los ADPIC)

3.1.2.1 Alcance del Acuerdo sobre los ADPIC

El Acuerdo sobre los ADPIC de la Organización Mundial del Comercio (OMC) es otro tratado internacional de importancia fundamental para los titulares de derechos que distribuyen sus contenidos a través de los medios que ofrece el comercio electrónico, incluyendo sistemas de DRM. El Acuerdo sobre los ADPIC se firmó en 1995 como parte integral del conjunto de negociaciones más amplio realizado durante la Ronda de Uruguay del Acuerdo General sobre Aranceles Aduaneros y Comercio.[30]

El Acuerdo sobre los ADPIC entró en vigor el 1 de enero de 1995. Proporciona protección y obliga a la observancia de diversos tipos de derechos de propiedad intelectual, incluyendo, entre otros, derecho de autor, patentes, marcas de fábrica o de comercio y secretos comerciales. En concreto, la Parte II del Acuerdo sobre los ADPIC establece normas mínimas en áreas relevantes de la propiedad intelectual que deben cumplir los miembros. La Parte III establece normas mínimas en relación con la observancia a nivel nacional en los países miembros de los derechos de propiedad intelectual. La Parte V se ocupa de la prevención y solución de diferencias y la Parte VI establece disposiciones transitorias[31]. El Acuerdo sobre los ADPIC también requiere en general un trato nacional (por parte de los Estados Miembros en relación con el trato que den a nacionales de otros Estados) y el trato de nación más favorecida (prohibiendo la discriminación de nacionales de otros Estados Miembros).

En relación con la Parte II, el Acuerdo sobre los ADPIC incorpora mediante referencias y, hasta cierto punto, se extiende en relación con las protecciones sustantivas que exige el convenio de Berna en materia de derechos de autor y el Convenio de París sobre la Protección de la Propiedad Intelectual y otros. Se trata de un conjunto de normas mínimas, por lo que los Miembros son libres de proporcionar una mayor protección a la propiedad intelectual. En lo que se refiere a la Parte III, el Acuerdo sobre los ADPIC exige que los estados miembros apliquen y cumplan los procedimientos para la observancia de derechos de propiedad intelectual, incluyendo procedimientos y recursos civiles y administrativos, el derecho de los titulares de derechos a la aplicación de medidas provisionales contra los presuntos infractores y prescripciones especiales relacionadas con medidas aplicables en las fronteras y los procedimientos penales.

Aunque el Acuerdo sobre los ADPIC establece un importante marco jurídico internacional común y básico para la protección del derecho de autor y demás propiedad intelectual, y para su observancia a nivel nacional, el acuerdo fue intensamente negociado durante diciembre de 1991 y entró en vigor antes que los Tratados de la OMPI. En este

---

30 *Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio*, disponible en *http://www.wto.org/spanish/docs_s/legal_s/27-trips.doc*.

31 Entre las disposiciones transitorias se encuentran calendarios para el cumplimiento total del Acuerdo sobre los ADPIC. Se exigió que los países desarrollados cumplieran íntegramente el Acuerdo sobre los ADPIC el 1 de enero de 1996. Los países en desarrollo tenían cinco años, hasta el 1 de enero de 2000. A los países menos adelantados se les concedió diez años, hasta el 1 de enero de 2005.

sentido, algunos analistas han hecho notar que el Acuerdo sobre los ADPIC no tiene debidamente en cuenta los aspectos de propiedad intelectual implicados en la distribución digital de contenidos, incluido Internet, y que las protecciones para las DRM que ofrecen los Tratados de la OMPI no están cubiertos por el Acuerdo[32]. Sin embargo, gran parte del debate sobre la distribución electrónica ha pasado de tratar los aspectos fundamentales relacionados con las normas básicas de protección de derecho de autor, que proporciona el Acuerdo sobre los ADPIC, a tratar los retos que trae consigo el entorno digital y a aspectos más novedosos de la protección de las salvaguardas técnicas a la elusión, asuntos incluidos en los Acuerdos de la OMPI. En consecuencia, se ha señalado que los Acuerdos de la OMPI fueron impulsados, en parte, por la necesidad de llenar las "lagunas" existentes en el Acuerdo sobre los ADPIC y en los Convenios de Berna y de Roma[33].

3.1.2.2 Programa de Trabajo de la Organización Mundial del Comercio (OMC) sobre Comercio Electrónico

No obstante lo anterior, en la OMC se ha considerado, por ejemplo, si incluir en el Acuerdo sobre los ADPIC, y cómo hacerlo, prohibiciones a la elusión de las DRM y de otras medidas tecnológicas. Estas discusiones han tenido lugar en el contexto del Programa de Trabajo más amplio dedicado por la OMC al Comercio Electrónico ("Programa de Trabajo"), que comenzó con una declaración durante la Conferencia Ministerial en mayo de 1998, por la que el Consejo General estableció un amplio programa de trabajo para analizar "todas las cuestiones relacionadas con el comercio electrónico mundial que afectan al comercio"[34]. El Programa de Trabajo se adoptó el 25 de septiembre de 1998 a los efectos de los órganos relevantes de la OMC, incluyendo el Consejo de la OMC sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (Consejo de los ADPIC). Los asuntos que se pretendía que examinara el Consejo de los ADPIC incluían la protección y observancia de los derechos de autor y derechos conexos, las nuevas tecnologías y el acceso a la tecnología[35].

Tal como indicó expresamente la Secretaría del Consejo de los ADPIC en un Documento de Antecedentes del 10 de febrero de 1999, la cuestión es si, en un entorno de red digital, la normas del Acuerdo sobre los ADPIC proporcionan "protección efectiva y adecuada de los derechos de propiedad intelectual"[36]. El Documento de Antecedentes identificaba y examinaba específicamente asuntos incluidos en los Tratados de la OMPI, tales como la definición de "publicación" y el alcance de los derechos de reproducción y comunicación al público en el entorno de las comunicaciones en línea. De forma

---

32 Véase S. Baker, P. Lichtenbaum, M. Shenk y M. Yeo, *E-Products and the WTO*, 35 *The International Lawyer* 5, 20 (2001).

33 Véase la contribución de Australia, *Programa de Trabajo del Comercio Electrónico,* documento de la OMC IP/C/W/233, párrafo 28 (7 de diciembre de 2000). Véase también *Programa de Trabajo del Comercio Electrónico: Background Note de la Secretaría*, documento de la OMC IP/C/W/128, párrafo 75 (10 de febrero de 1999) (en las negociaciones del ADPIC no se plantearon medidas tecnológicas, y el Acuerdo sobre los ADPIC no contiene medidas específicas concernientes a dichas medidas) ["Documento de Antecedentes"].

34 *Declaración sobre Comercio Electrónico Mundial*, documento de la OMC WT/MIN(98)/DEC/2 (25 de mayo de 1998).

35 *Programa de Trabajo sobre comercio Electrónico*, WT/L/274, párrafo 4.1 (30 de septiembre de 1998).

36 Documento de Antecedentes, párrafo 14.

significativa, el Documento de Antecedentes señalaba la importancia de las medidas tecnológicas de protección contra la copia, la encriptación y la marca mediante filigrana, así como la utilidad de la información sobre la gestión de derechos electrónicos, que dependen de las protecciones jurídicas incluidas en los Tratados de la OMPI[37]. El Documento de Antecedentes analiza ampliamente las actividades realizadas por la OMPI, incluyendo los dos tratados dela OMPI y las implicaciones del comercio electrónico sobre la propiedad intelectual[38].

En el Documento de Antecedentes se vertían consideraciones adicionales sobre estos asuntos por parte del Consejo de los ADPIC, incluyendo contribuciones de los miembros de la OMC y una presentación de un representante de la OMPI sobre las actividades que estaban en marcha en dicha organización. Los miembros de la OMC remitieron contribuciones al Consejo, proponiendo la realización de trabajos adicionales. Una de las propuestas era a cerca de si el propio Acuerdo sobre los ADPIC debería ser adaptado o clarificado para reflejar nuevos desarrollos tecnológicos, tales como la utilización de DRM. Sin embargo, otras contribuciones reflejaban la postura de que la OMC no debía duplicar los trabajos que ya estaban en curso en la OMPI. En los Informes de situación de julio de 1999 y de diciembre de 2000, el Consejo de los ADPIC llegó a un consenso entre sus miembros: el Consejo seguía reconociendo la complejidad de este asunto y señalaba la necesidad de estudios adicionales en determinadas áreas fundamentales, siendo de la opinión de que la OMC debía continuar considerando estos desarrollos, incluyendo los trabajos en curso de la OMPI[39]. A partir de entonces, en la *Declaración Ministerial* de Doha, de la OMC, de noviembre de 2001 se tomó nota de los trabajos en curso sobre comercio electrónico y se solicitó al Consejo General que informara sobre las disposiciones institucionales adecuadas para continuar dichos trabajos durante la Quinta Sesión de la Conferencia Ministerial[40] programada para septiembre de 2003.

3.2 Estados Unidos de América

3.2.1 Marco jurídico

En octubre de 1998, Estados Unidos de América aplicó las disposiciones contra la elusión de los Tratados de la OMPI mediante el Título I de la Ley de Derecho de Autor para el Milenio Digital (DMCA, *Digital Millennium Copyright Act*)[41]. También existen otras leyes federales y estatales para la protección de las tecnologías contra la elusión ilícita y para la protección de los titulares de derechos a cuyas obras se accede sin su autorización.

---

37 Documento de Antecedentes, párrafos 75-76.

38 *Id*. párrafos 80-92.

39 *Programa de Trabajo sobre Comercio Electrónico: Informe de situación para el Consejo General*, documento de la OMC IP/C/18 (30 de julio de 1999); *Programa de Trabajo sobre Comercio Electrónico: Informe de situación del Presidente para el Consejo General*, documento de la OMC IP/C/20 (4 de diciembre de 2000).

40 *Declaración Ministerial*, documento de la OMC WT/MIN(01)/DEC/1, párrafo 34 (20 de noviembre de 2001).

41 Acta de 1998 sobre la Aplicación de los Tratados de la OMPI de Derecho de Autor y de Interpretación o Ejecución y Fonogramas, Título I de la Digital Millennium Copyright Act (codificado en 17 U.S.C. Capítulo 12).

En los Estados Unidos de América, la protección jurídica de las tecnologías DRM surge como consecuencia de una delicada interacción entre los acuerdos alcanzados por el sector privado (utilizados para conceder licencias de tecnologías de protección de contenidos) y las iniciativas gubernamentales, incluyendo leyes estatales y federales y reglamentos federales. El punto de vista más extendido en los Estados Unidos de América desde mediados de los 90 se inclina por que el sector privado llegue a soluciones pactadas, siempre que ello sea posible, en base a negociaciones entre las industrias afectadas. Esta soluciones permiten a los titulares de derechos aplicar protecciones contractuales y resoluciones en relación con productos que no sean conformes con las normas acordadas para la protección de contenidos. Esta interacción y las disposiciones contractuales se analizan con detalle en un documento elaborado para la OMPI por Dean S. Marks y Bruce H. Turnbull: "Las medidas tecnológicas de protección: el punto de encuentro de la tecnología, el derecho y las licencias comerciales."[42]

Para resumir las conclusiones de dicho documento, éste recopila un conjunto prolijo de acuerdos del sector privado sobre licencias de tecnologías para la protección de contenidos que incluyen requisitos específicos destinados a proteger los contenidos, tales como películas y música, una vez que han entrado al entorno del hogar y a redes personales. Tal como se describe en el documento, dichos acuerdos contienen:

– Reglas de codificación – relativas a cuándo pueden los titulares de derechos "codificar" el contenido para restringir la copia o la redistribución;

– Reglas de conformidad – que determinan las salidas a las que los contenidos protegidos puede redirigirse; y

– Reglas de robustez – que establecen cómo deben elaborarse los productos para resistir los intentos de elusión de sus elementos de protección contra la copia.

Aunque este documento no pretende hacer un análisis exhaustivo de dichos acuerdos, éstos incluyen: la Protección de Contenido para Transmisión Digital (DTCP, *Digital Transmission Content Protection*), cuya licencia otorga el Administrador de Licencia para Transmisión Digital LLC (DTLA, *Digital Transmission Licensing Administrator LLC*); la Protección de Contenido Digital de Banda Ancha (HDCP, *High-bandwidth Digital Content Protection*), cuya licencia otorga la Protección de Contenido Digital LLC; la Protección de Contenidos para Medios Pregrabados (CPPM, *Content Protection For Prerecorded Media*) y la Protección de Contenidos para Medios Grabables (CPRM, *Content Protection for Recordable Media*), reciben ambos su licencia de la Entidad 4C LLC; y el Sistema de Aleatorización de Contenidos (CSS, *Content Scramble System*), cuya licencia la otorga la Asociación para el Control del Copiado de DVD (DVD CCA, *DVD Copy Control Association, Inc*.).[43]

Cuando las iniciativas del sector privado no han sido suficientes para abarcar todos los aspectos de la protección de contenidos, los grupos industriales de los Estados Unidos de América han conseguido que el gobierno tome medidas al respecto. Cuando es necesario

---

42 Doc OMPI No. WCT-WPPT/IMP/3 (3 de diciembre de 1999) ["Marks/Turnbull"], disponible en *http://www.wipo.int/spa/meetings/1999/wct_wppt/pdf/imp99_3.pdf*. Se hizo una reimpresión del documento en 22 E.I.P.R. 198 (2000).

43 *Id*.

exigir un cumplimiento generalizado, son necesarias medidas ejecutivas gubernamentales concretas. Además, en muchas situaciones específicas, puede no ser factible ni efectivo un enfoque basado en relaciones contractuales, por ejemplo, cuando las medidas DRM pueden ser eludidas por individuos o por productos fabricados por entidades que están fuera del ámbito del contrato. Para dichos casos, solo resulta adecuado recurrir a los ámbitos civil y penal[44].

3.2.1. DMCA

3.2.1.1.a) Antecedentes

El tratamiento legislativo y la promulgación del proyecto de ley que ulteriormente se convirtió en la DMCA se caracterizó por generar el debate más intenso tanto en el Congreso como en otros medios públicos sobre la legislación de propiedad intelectual desde la promulgación de la Ley de Derecho de Autor (*Copyright Act*) de los Estados Unidos de América en 1976. En un lado del debate (favorables a una aplicación robusta y de amplia base de los Tratados de la OMPI) se situaban los intereses de los titulares de derechos de autor, principalmente las industrias del cine, discográficas y editoriales. Por otro lado, reclamando prudencia, equilibrio y excepciones de carácter más amplio estaban las industrias tecnológicas, tales como las compañías electrónicas de computadoras y de otros productos de consumo, así como los intereses de los usuarios, incluyendo bibliotecas, instituciones educativas y consumidores. La DMCA ha estado, y sigue estando, sujeta a críticas muy importantes por parte de estos grupos.

En las deliberaciones legislativas, participaron varios Comités del Congreso, cada uno con su perspectiva propia. Entre los aspectos más significativos de los muchos que tuvo en cuenta el Congreso estaban los siguientes:

– Si la DMCA debía prohibir las herramientas utilizadas para la elusión (incluyendo servicios),[45] o solamente los actos de elusión;

– Si se debería permitir la elusión de una medida tecnológica en virtud de un acto que no supusiera infringir la ley, como por ejemplo un uso lícito;

– Si se debían prohibir actividades legítimas, tales como la ingeniería inversa y la prueba de sistemas de encriptación;

– Si se debían prohibir herramientas lícitas al amparo del marco jurídico existente sobre la vulneración de derechos de autor por autoría indirecta, por el hecho de estar diseñadas para eludir medidas tecnológicas;

---

44 *Id*. Este aspecto se considera con más detalle en la sección 5.2.3, donde se analiza el papel de los gobiernos en el establecimiento de normas DRM.

45 En última instancia, el concepto de herramientas de elusión se incluyó en la frase de la DMCA "tecnología, producto, servicio, dispositivo, componente o parte." 17 U.S.C. §§ 1201.a).2), 1201.b).1).

– Si la DMCA debía prohibir solamente "cajas negras" diseñadas para la elusión, y no las computadoras personales normales, productos electrónicos de consumo o productos de telecomunicaciones;

– Si la DMCA debía definir las "medidas tecnológicas" para las que la elusión está prohibida; y

– En qué medida la DMCA representa la transición hacia una sociedad que utilice ampliamente el "pago por uso", limitando el acceso sólo a obras encriptadas.

3.2.1.1.b) Disposiciones contra la elusión

A alto nivel, las disposiciones de la DCMA contra la elusión, que son una aplicación del Artículo 11 del WCT y del Artículo 18 del WPPT, reflejan la siguiente matriz de prohibiciones:

	Acto de elusión	**Herramientas de elusión**
Medida tecnológica de control de acceso	Prohibida (§ 1201.a)1))	Prohibida (§ 1201.a)2))
Medida tecnológica de control de derechos de autor	No prohibida (por DMCA)	Prohibida (§ 1201.b))

Tal como se ha indicado, podría decirse que los Tratados de la OMPI sólo requieren una protección adecuada y efectiva contra los *actos* de elusión y solo con respecto a medidas utilizadas para proteger el ejercicio de *los derechos de autor* de conformidad con el Convenio de Berna, el WCT y el WPPT. Sin embargo, la DMCA va más allá de los mínimos establecidos en los Tratados de la OMPI prohibiendo tanto los actos de elusión como los productos de elusión, con respecto a las medidas tecnológicas de "control de acceso" y "control del derecho de autor" utilizadas para proteger una obra con derechos de autor.

Artículo 1201.a): en virtud de este artículo se prohíben actos y productos que eludan las medidas tecnológicas de control de acceso. La definición de "elusión" es expansiva, incluyendo la desaleatorización, el desencriptado, o "cualquier forma de evitar, neutralizar, desactivar u obstaculizar una medida tecnológica sin la autorización del titular de derechos de autor."[46]

La DMCA no define el término "medida tecnológica". Sin embargo, define si una medida tecnológica "controla efectivamente el acceso a una obra", señalando que controla el acceso "si en el curso normal de su funcionamiento, la medida requiere la aplicación de información, o un proceso o tratamiento realizado con la autorización del titular del derecho de autor para acceder a la obra"[47]. Los antecedentes de la DMCA sugieren que el Congreso consideraba que las medidas tecnológicas tales como la encriptación y la autenticación eran

[46] 17 U.S.C. § 1201.a)3)A).
[47] § 1201.a)3)B).

los tipos de medidas tecnológicas que darían acceso a la obra, sin embargo, la definición se dejó intencionadamente abierta para poder incluir futuros desarrollos.

Entre las diversas medidas tecnológicas establecidas por los tribunales y por el Bibliotecario del Congreso (el "Bibliotecario") para controlar el acceso a una obra, se encuentran la secuencia de autenticación para asegurar que el contenido se ha transmitido exclusivamente al reproductor autorizado; el CSS utilizado para proteger los discos de video DVD del acceso no autorizado; el sistema de codificación por región de los discos de video DVD, que sólo permite su reproducción en regiones geográficas determinadas; y los códigos de región utilizados en videojuegos.

Artículo 1201.a)1): en virtud de este artículo se prohíbe a una persona eludir una medida tecnológica que "controle efectivamente el acceso a una obra". La prohibición proscribe rotundamente el acto de la elusión, aunque éste se realice con propósitos plenamente lícitos y autorizados por la Ley de Derecho de Autor (*Copyright Act*). Durante los debates de la DMCA, una de las controversias más intensas surgió en torno a si debería haber una excepción expresa por "uso lícito" (u otro similar) a esta prohibición. Finalmente, el Congreso concluyó que no debía incluirse una excepción de ese tipo y que la elusión, incluso para un uso lícito, es ilegítima.

Sin embargo, debido a las preocupaciones surgidas por los posibles efectos de la prohibición se llegó a un compromiso. En primer lugar, la ley retrasó la fecha de efectividad de esta sección dos años, hasta el 28 de octubre de 2000. El propósito de este retraso era permitir al Bibliotecario, realizar a petición del Registro de Derechos de Autor (*Register of Copyrights*) un estudio para examinar si los usuarios de obras con derecho de autor se verían "negativamente afectados" por la prohibición de hacer un uso que no infringiera la ley de determinadas clases de obras. En segundo lugar, la DCMA requiere que el Bibliotecario realice el mismo estudio cada tres años. En la sección 3.2.1.3.a) se describe este proceso reglamentario, las conclusiones del Bibliotecario correspondientes al año 2000 y el estudio en curso (que debe terminarse a finales de 2003).

Además, se ha señalado que prohibiendo la elusión de medidas tecnológicas que controlan el acceso a una obra, la DCMA ha creado indirectamente un nuevo "derecho de acceso" a las obras de los titulares de derechos; sin embargo, para estar seguro, la disponibilidad del nuevo derecho queda expresamente supeditado a la utilización de una medida tecnológica. Dicho derecho de acceso no se había incluido previamente ni en el Convenio de Berna ni en el WCT.

Los bibliotecarios y otros usuarios han argumentado que este nuevo derecho (en ausencia de un derecho de elusión para facilitar un uso lícito) conduce inexorablemente al establecimiento de una nueva sociedad de "pago por uso". Advirtieron que el futuro sería sensiblemente diferente del mundo tradicional de las copias tangibles, en el que un usuario que compra un libro o un disco lo puede utilizar una y otra vez sin tener que pagar por cada uso. Desde este punto de vista, el equilibrio de intereses entre titulares de derechos y usuarios de la Ley de Derecho de Autor de los Estados Unidos de América, se ve o se verá amenazada.

Los titulares de derechos han respondido a esta preocupación señalando que el control de acceso permite utilizar diversos modelos de negocio que podrían ser de interés para una gama más amplia de preferencias de los consumidores. Han indicado que los usuarios pueden estar más interesados en pagar por un único uso que en comprar los derechos de uso de una

obra para múltiples ocasiones, comprando una copia que tendría un precio superior. Han destacado además, que si existiera mercado para un tipo de uso específico, propondrían un producto en la forma más adecuada para atender dicha demanda.

Artículo 1201.a)2): en virtud de este artículo se prohíbe la fabricación, venta, oferta al público o provisión (es decir, "circulación") de cualquier tecnología, producto, servicio, dispositivo, componente o parte (es decir, de cualquier "herramienta") que eluda una medida de protección tecnológica. Obsérvese que aunque una tecnología no infrinja en su conjunto la prescripción legal, puede prohibirse un componente de la misma, o incluso una parte de un componente. Sin embargo, para que dicha herramienta pueda prohibirse, debe satisfacer al menos una de las tres condiciones siguientes:

– Haber sido "diseñada o producida principalmente para la elusión de la medida tecnológica que controla efectivamente el acceso a una obra"[48],

– Tener "solamente una utilización u objetivo comercial relevante limitado para todo lo que no sea eludir una medida tecnológica que controla efectivamente el acceso a una obra"[49], o

– Ser "comercializado por una persona o por alguien que actúe de acuerdo con dicha persona con el conocimiento de ésta con el fin de eludir una medida tecnológica que controla efectivamente el acceso a una obra"[50].

Existió una gran controversia en relación con estas tres pruebas cuando se aprobó la DMCA, controversia que aún sigue existiendo. En particular, la prueba de ser "diseñado o producido principalmente para la elusión" se aparta significativamente de la prueba establecida por el Tribunal Supremo de los Estados Unidos de América en 1984, en un caso sobre la licitud del grabador de video Betamax de Sony. El Tribunal Supremo decidió que Sony no era culpable de las prácticas de copia casera de los usuarios de Betamax debido a que el grabador, como cualquier otro producto básico del comercio, era objeto de un interés comercial significativo para un uso que no infringía la ley[51]. Sin embargo, la DMCA prohíbe tajantemente herramientas (en la medida que sirven para eludir medidas tecnológicas) en base a sus diseño o producción principal, sin considerar si pueden ser o serán utilizadas para usos que no supongan infringir la ley.

Para responder a este cambio sustancial de la ley en relación con la responsabilidad potencial de los fabricantes por sus productos, el Congreso adoptó el Artículo 1201.c)3), que se analiza más adelante en 3.2.1.1.c).

Otra área de incertidumbre es la que existe en torno al significado de la expresión "diseñado o producido principalmente". En este sentido, la historia legislativa de la DMCA no está clara. Sin embargo, parece evidente que la utilización del término "principalmente" sólo hace referencia al "propósito" más significativo; probablemente sólo puede haber un único propósito principal. Una herramienta que permita la elusión, pero que tenga múltiples usos, todos ellos de un interés similar, no puede por tanto haber sido "diseñada o producida principalmente" con el propósito de la elusión.

---

48 § 1201.a)2)A).
49 § 1201.a)2)B).
50 § 1201.a)2)C).
51 *Sony Corp. contra Universal City Studios, Inc.*, 464 U.S. 417 (1984).

Artículo 1201.b): en virtud de este artículo sólo se prohíbe el tráfico de herramientas que permitan eludir las tecnologías que protejan el derecho de un titular del derecho de autor de una obra o de parte de la misma. Para quedar fuera de la ley, la herramienta de elusión debe cumplir una tres pruebas que, en esencia, son similares a las arriba descritas[52]. Este artículo define la elusión en los mismos términos que el Artículo 1201.a). Tampoco aquí se define una medida tecnológica, pero dicha medida "protege efectivamente el derecho de un titular de derechos de autor" si ésta "en el curso normal de su funcionamiento, impide, restringe o limita el ejercicio de un derecho [derecho de autor] de un titular de derechos de autor." En otras palabras, si se utiliza una medida tecnológica para impedir la reproducción, distribución, representación o visualización pública no autorizada (es decir, un "uso" de derecho de autor no autorizado), se prohíbe cualquier herramienta de elusión de la misma (suponiendo que satisface una de las tres pruebas, como el de ser "diseñada o producida principalmente para dicho fin").

Es de destacar que la DMCA no prohíbe el acto de elusión de una medida tecnológica que proteja el derecho exclusivo de un titular de derecho de autor de autorizar el uso de una obra. El Congreso estableció que no es preciso que la DMCA prohíba el acto de elusión, por ejemplo, para hacer una copia de una obra, porque en muchos casos el eventual acto (de copia no autorizada) infringiría el derecho de autor. En consecuencia, un titular de derechos podría recurrir a la ley de derecho de autor y el demandado podría recurrir a cualquiera de las defensas o limitaciones incluidas en dicha ley.

3.2.1.1.c) Limitaciones y excepciones

La DMCA incluye numerosas limitaciones y excepciones que reflejan la gran intensidad de los debates en el Congreso y el interés de determinados grupos. A continuación se analizan algunas de las más significativas.

Relación con la vulneración de los derechos de autor, incluido el uso lícito: la DMCA establece que el Artículo 1201 no afecta a los "derechos, recursos, limitaciones o defensas a la vulneración de derecho de autor, incluido el uso lícito"[53]. Aunque en una lectura superficial puede interpretarse que esta disposición protege las actividades de uso lícito, al interpretar esta disposición los tribunales han determinado, que cualesquier derechos y defensas al amparo de la ley de derecho de autor son diferentes de, y no se ven afectados por los nuevos derechos, recursos y excepciones de las disposiciones contra la elusión, es decir, ante una reclamación realizada al amparo del Artículo 1201.a)1) de la DCMA no es una defensa válida argumentar que la elusión se realizó en aras de una actividad plenamente legítima y para un uso lícito[54].

Relación con la vulneración del derecho de autor por colaboración o autoría indirecta: la DMCA señala que nada de lo incluido en el Artículo 1201 "aumentará o disminuirá" la responsabilidad "por colaboración o autoría indirecta" en la vulneración de derechos de autor mediante una tecnología[55]. Sin embargo, la redacción utilizada adolece en buena medida de

---

52 17 U.S.C. § 1201.b)1)A)-C).
53 § 1201.c)1).
54 Véase 3.2.2 (análisis del caso *Universal City Studios, Inc. contra Corley*).
55 17 U.S.C. § 1201.c)2).

un sentido claro, ya que, tal como se ha señalado anteriormente, si un producto viola lo dispuesto por el Artículo 1201.a)2) o 1201.b), dicha violación puede ser objeto de demanda judicial (a tenor de lo dispuesto en el Artículo 1201), independientemente de que el producto ayude o contribuya a la vulneración del derecho de autor.

Disposición de "no-obligatoriedad " para productos ordinarios: en respuesta a las preocupaciones de los fabricantes de computadoras, de electrónica de consumo y de productos de telecomunicaciones en el sentido de que podría considerarse que sus productos violasen el Artículo 1201, la DMCA señala que la disposición no requiere que sus productos legítimos sean diseñados, o que partes y componentes de los mismos sean diseñados o seleccionados para "dar respuesta a cualquier medida tecnológica"[56]. Esta cláusula se denomina generalmente como disposición "de no-obligatoriedad", porque significa que dichos productos no tendrán que responder afirmativamente a cualquier medida tecnológica a fin de evitar una acusación de elusión; en otras palabras, solo los actos afirmativos de elusión (y no la mera no respuesta a una medida tecnológica) supondrá una violación del Artículo 1201.

Los fabricantes podrán beneficiarse de esta disposición sólo "en la medida en que" el producto, parte o componente "no satisfaga ninguna de las prohibiciones" establecidas en la sección. Aunque el significado cabal de esta disposición no está claro en su conjunto, de la propia historia legislativa se desprende que un producto debe ser analizado íntegramente para determinar porqué no respondió satisfactoriamente, ya sea por algún motivo de diseño legítimo o por algún propósito ilícito de elusión. La redacción sugiere que un fabricante no puede beneficiarse de esta disposición cuando alguna funcionalidad del producto sea positivamente utilizada para impedir, evitar o eludir en cualquier forma una medida tecnológica.

Además de estas limitaciones, el Artículo 1201 contiene otras excepciones específicas. Los Tratados de la OMPI no prohíben que las Partes Contratantes puedan adoptar excepciones a la prescripción general contra la elusión. Sin embargo, el requisito de que los recursos jurídicos deben ser "adecuados" y "eficaces" implica que cuando un país aplique las medidas, puede decidir sopesar las ventajas e inconvenientes para los usuarios y titulares de derechos de la prohibición de la elusión. Esto es precisamente lo que hizo el Congreso al adoptar siete excepciones que, sin embargo, se reconoce que son muy limitadas y aplicables a casos muy concretos. En la mayoría de las situaciones, las excepciones serían, en términos estrictos, inaplicables. Todas las excepciones son aplicables al acto de elusión de controles de acceso, pero sólo cinco de ellas se aplica a las disposiciones que prohíben el tráfico de tecnologías de elusión.

Las siete excepciones son las siguientes:

---

[56] § 1201.c)3). Otra sección importante de la DMCA proporciona expresamente una respuesta afirmativa para un caso en particular: esencialmente todos los grabadores de videocasetes analógicos deben ser diseñados de forma que cumplan ciertas tecnologías de protección de copiado analógica cuya licencia concede Macrovision Corp. § 1201.k). Como parte del compromiso entre los fabricantes de dichos dispositivos y los titulares de derechos, la provisión incluye específicamente reglas de codificación que impiden que dichas tecnologías anticopia se utilicen gratuitamente en la radiodifusión de televisión; sin embargo, pueden utilizarse para restringir la copia (1) de una obra de un programa contratado por suscripción; (2) de un programa de pago por visión o de video bajo demanda, o de medios empaquetados, o (3) de copias realizadas a partir de dichos programas o medios.

– Bibliotecas, Archivos e Instituciones Educativas sin ánimo de lucro:[57] cuando estas instituciones no restrinjan el acceso al público o personas no afiliadas a la biblioteca, podrán eludir su obligación con el único propósito de tener acceso a una obra y tomar un decisión sobre su posible interés en adquirirla. Una institución cualificada sólo tendrá acceso durante el tiempo necesario para determinar si desea disponer de una copia lícita. Queda prohibida cualquier elusión para conseguir una ventaja económica o financiera.

– Agencias para la observancia de la Ley, para actividades de Inteligencia y otras Agencias Gubernamentales[58]: las actividades de seguridad nacional y de observancia de la ley, incluyendo las actividades de seguridad de la información, legalmente autorizadas, no estarán sujetas a las prohibiciones relativas a los actos de elusión y al tráfico de tecnologías establecidas en los Artículos 1201.a) y 1201.b). Tampoco están sujetas a las disposiciones del Artículo 1202, que se describe más abajo en 3.2.1.1.d).[59]

– Ingeniería inversa de programas informáticos[60]: se permite la ingeniería inversa de un programa informático (y sólo de un programa informático) por parte de quien disponga de una copia lícita del mismo (a pesar de los controles de acceso), pero sujeto a una serie de condiciones. En primer lugar, el"único propósito" de la elusión debe ser identificar y analizar elementos del programa "necesarios para conseguir la interoperabilidad" con un "programa informático creado de forma independiente". Segundo, dichos elementos de programa no han debido haber estado previamente "disponibles" para la persona que realiza la elusión. Tercero, las actividades no deben en sí mismas constituir un acto de elusión (en circunstancias normales, y con la jurisprudencia existente en los Estados Unidos de América, se considera que hacer una reproducción relacionada con la ingeniería inversa legal, se considera un uso lícito[61]). Además, una persona puede "desarrollar y utilizar" herramientas de elusión para el propósito permitido y poner a disposición de terceros la información que consigue mediante ingeniería inversa, pero exclusivamente para permitir a interoperabilidad.

– Investigación criptográfica[62]: la investigación criptográfica realizada con "buena fe" de una medida tecnológica de control de acceso se permite sujeta a cuatro condiciones: 1) la persona que realiza la investigación ha obtenido la copia lícitamente; 2) el acto es necesario para realizar la investigación; 3) la persona ha hecho un "esfuerzo de buena fe" para conseguir la autorización; y 4) el acto no supone la violación de otra ley. La investigación criptográfica se define como las "actividades necesarias para identificar y analizar fallos y vulnerabilidades de las tecnologías de encriptación. . . para avanzar en el estado del conocimiento. . . o para ayudar en el desarrollo de productos criptográficos". Para determinar la viabilidad de la excepción, un tribunal debe considerar si la información obtenida de la investigación criptográfica ha sido diseminada y cómo, si la persona participa legítimamente en la investigación criptográfica y si los resultados y documentación de la investigación se facilitan al titular del derecho de autor del trabajo protegido por la medida tecnológica.

---

57 § 1201.d).
58 § 1201.e).
59 § 1202.d).
60 § 1201.f).
61 Véase *Sega Enterprises Ltd. contra Accolade, Inc.*, 977 F.2d 1510, 1527-28 (9º Circuito, 1992).
62 17 U.S.C. § 1201.g).

En el momento de su promulgación, se pensó que las limitaciones y condiciones de esta excepción restringirían gravemente su aplicabilidad y que, por tanto, la investigación criptográfica legítima se vería afectadas negativamente por la DMCA. A tal fin, la DMCA exigía que al cabo de una año se preparase un informe en relación con la influencia de la DMCA sobre la investigación criptográfica, la adecuación y efectividad de las medidas tecnológicas y la protección de los titulares de derecho de autor contra el acceso no autorizado a obras encriptadas[63]. El informe, publicado en julio de 1999 por el Registro de Derechos de Autor y el Subsecretario para Comunicaciones e Información, concluía que no se habían identificado un "impacto discernible" en relación con estos asuntos, que cualquier daño al respecto se produciría, en su caso, ulteriormente, y que dicho resultado era previsible puesto que el Artículo 1201.a)1) sobre prohibición de actos de elusión aún no había entrado en vigor[64].

– Protección de menores[65]: esta excepción establece que cuando un tribunal aplique a un componente o una parte las disposiciones contra el tráfico del Artículo 1201.a), puede considerar si la excepción a la prohibición de elusión es necesaria para una tecnología que "tiene el único propósito de impedir el acceso de menores a material en Internet."

– Protección de información para la identificación personal[66]: esta excepción, destinada a las *cookies*, permite la elusión cuando la medida tecnológica (o la obra que protege) recopila o disemina información de datos personales en el transcurso de actividades en línea; cuando dicha recopilación o diseminación se hace sin "aviso manifiesto", tenga el "único efecto" de identificar e inhabilitar dicha capacidad de recopilación o diseminación y se realice exclusivamente para impedir dichas actividades y no viole ninguna otra ley.

– Pruebas de seguridad[67]: esta excepción permite que una persona participe en la realización de buena fe de pruebas sobre la seguridad de una computadora, sistema de computadoras o red de computadoras, con la autorización del titular. Permite la elusión y que la persona desarrolle, distribuya y utilice medios tecnológicos con el único propósito de realizar pruebas de seguridad, y no para ningún otro propósito. Los actos sólo se permiten si no vulneran o violan otra ley. Si un demandado invocase esta excepción ante un tribunal, éste deberá considerar si la información se utilizó "exclusivamente para promover la seguridad del propietario" de la computadora, o si había sido compartida con éste; y si la información fue "utilizada o mantenida" de forma que no facilitara el cumplimiento o vulneración de cualquier otra ley.

3.2.1.1.d) Información para la gestión del derecho de autor

En su Artículo 1202, la DMCA proporciona específicamente protección de la "información para la gestión del derecho de autor" (CMI, *copyright management*

---

63 § 1202.g)5).

64 Véase Register of Copyrights and Assistant Secretary for Communications and Information, *Report to Congress: Joint Study of Section 1201(g) of The Digital Millennium Copyright Act,* Part III (1999), disponible en: *http://www.copyright.gov/ reports/studies/dmca_report.html*.

65 17 U.S.C. § 1201.h).

66 § 1201.i).

67 § 1201.j).

information). La CMI es fundamental para un sistema DRM eficaz, ya que dicha información describe la obra y cómo puede utilizarse.

La DMCA define la CMI de una forma bastante amplia e incluye cualquier información contenida en una obra que la describa, incluyendo título, autor, información de aviso de derecho de autor, nombre de los ejecutantes (en determinadas circunstancias, sin incluir las representaciones públicas de una obra por una estación de radiodifusión de radio o televisión ni las de una obra audiovisual), nombre de los escritores, directores y ejecutantes (de una obra audiovisual, excepto cuando se emite en radiodifusión), términos y condiciones de utilización, números o símbolos de identificación y otra información prescrita por el Registrador de Derechos de Autor[68].

El Artículo 1202 tiene dos disposiciones operativas. La primera prohíbe la inclusión de información CMI falsa, o la distribución e importación de CMI falsa, cuando la persona lo hace a sabiendas y la intención es "inducir, permitir, facilitar o encubrir la vulneración"[69].

La segunda prohíbe a una persona no autorizada eliminar o modificar intencionadamente la CMI, así como la distribución o importación de CMI a sabiendas que ésta ha sido eliminada o modificada sin autorización y la distribución, importación o ejecución pública de la copia de una obra o de una obra a sabiendas de que la CMI ha sido eliminada o alterada sin la autorización del titular del derecho de autor. Los actos mencionados quedan prohibidos cuando la persona conoce o existen fundamentos razonables para que conozca que dicha actividad puede inducir, permitir, facilitar o encubrir una vulneración[70].

3.2.1.1.e) Vías de recurso

La DMCA incluye sanciones civiles y penales[71]. Los recursos civiles incluyen medidas cautelares y embargos así como el reconocimiento de daños y perjuicios. Los perjuicios reconocidos pueden oscilar, a discreción del tribunal, entre 200 dólares y 2.500 dólares para cada acto de elusión o producto elusivo (para violaciones del Artículo 1201) y desde 2.500 dólares a 25.000 dólares (para el Artículo 1202). Las multas pueden elevarse en caso de vulneración repetitiva y reducirse en caso de vulneración inocente. Las bibliotecas, archivos e instituciones educativas sin ánimo de lucro pueden no ser responsables de daños causados no siendo conscientes de que sus actividades violaban la ley, sin que se les pueda imponer sanciones penales.

3.2.1.2 Otras leyes / leyes estatales

Existe una amplia variedad de leyes estatales y federales que dan cierta protección contra la elusión de las medidas tecnológicas utilizadas en sistemas DRM. Éstas se describen brevemente a continuación:

---

68 § 1202.c).
69 § 1202.a).
70 § 1202.b).
71 § 1204.

– Ley de Derecho de Autor (*Copyright Act*): cuando un producto permite la vulneración de un derecho de autor, incluida la elusión de la DRM para permitir una copia no autorizada, pueden tomarse acciones por la vulneración del derecho de autor contra el fabricante o proveedor del dispositivo. Además, para ser procesado al amparo del Artículo 1201.b) de la DMCA, debe determinarse su responsabilidad en la vulneración del derecho de autor por autoría indirecta si el dispositivo permite a un usuario vulnerar directamente el derecho de autor o si existe algún tipo de estímulo para la vulneración. Sin embargo, el fabricante de un "producto básico de comercio" (definido por el Tribunal Supremo como un producto que permite "usos comerciales significativamente no vulneradores") no podrá ser declarado responsable de la vulneración del derecho de autor por autoría indirecta[72].

– Ley TEACH (*TEACH Act*): a finales de 2002, el Congreso promulgó la Ley de Tecnología, Educación y Armonización de Derechos de Autor (*Technology, Education and Copyright Harmonization Act*), que modificaba la Ley de Derecho de Autor (*Copyright Act*) para permitir sistemas de educación a distancia distribuidos por medios digitales. La Ley TEACH amplió el ámbito de las excepciones tradicionales de los derechos exclusivos de los titulares de derecho de autor en relación con su utilización en las aulas y mediante radiodifusión a fin de autorizar su la utilización pública de las obras[73]. Dichas excepciones se habían vinculado a la tecnología y con la aparición de Internet habían quedado obsoletas.

La Ley TEACH permite la transmisión asociada a la educación en línea, sujeta a condiciones específicas. Una de éstas es que deben utilizarse las medidas de protección tecnológica tales como la protección mediante contraseña para permitir el acceso a sitios Web. Cuando se utilice la transmisión digital para distribuir el material, la institución de enseñanza debe utilizar tecnologías DRM que "impidan razonablemente" que los estudiantes mantengan en su poder las obras durante un tiempo superior al período de clases, así como una ulterior distribución de las obras[74].

La Ley TEACH requiere asimismo que el Subsecretario de Comercio para la Propiedad Intelectual remita al Congreso, después de haber consultado al Registro de Derechos de Autor, un informe sobre medidas de protección tecnológicas para proteger las obras con derechos de autor que hayan sido digitalizadas y para impedir la vulneración de dichos derechos. El Informe, que constituye una visión general útil y de alto nivel sobre este asunto, fue remitido en diciembre de 2002[75]. El Informe identificaba varias "tecnologías básicas" para la protección de contenidos, incluyendo la encriptación, la filigrana digital, la autenticación y los sistemas DRM. En el campo de la DRM, el Informe analiza los conceptos de "computación confiable" y "modelos de derechos y lenguajes de expresión de derechos", y analiza distintos tipos de arquitectura y sistemas DRM. Finalmente el Informe enumera y describe brevemente una amplia gama de compañías; privadas, iniciativas voluntarias de la industria, instituciones de normalización y organizaciones conexas así como asociaciones comerciales implicadas en el desarrollo, promoción y normalización de DRM y otras medidas de protección tecnológicas.

---

72 *Sony Corp. contra Universal City Studios, Inc.,* 464 U.S. 417, 442-43 (1984).

73 17 U.S.C. § 110.2).

74 § 110.2)d)ii).

75 Véase *Technological Protection Systems for Digitized Copyrighted Works: A Report to Congress* (Diciembre de 2002), disponible en *http://www.uspto.gov/web/offices/dcom/olia/teachreport.pdf*.

– Salvaguardas para los proveedores de servicios en línea: en 1998 se promulgó la Ley de Limitación de la Responsabilidad por la Vulneración de Derechos de Autor en Línea (*Online Copyright Infringement Liability Limitation Act*) como parte de la DMCA. Dicha ley proporciona "salvaguardas" a la responsabilidad por derecho de autor de varios tipos de actividades, incluyendo la transmisión, utilización de sistemas caché, almacenamiento de material de terceras partes y provisión de herramientas de localización de información[76]. Estas salvaguardas sólo se aplican si el proveedor de servicio cumple algunas condiciones generales. Una de ellas es que el proveedor de servicio "incluya y no interfiera con medidas técnicas normalizadas"[77]. Un proveedor de servicio que no las implemente o que diseñe su sistema sin incluir dichas medidas, no será específicamente penalizado pero no podrá acogerse a dicha salvaguarda.

Por este motivo, no es sorprendente que la definición de "medidas técnicas normalizadas" incluya conceptos sobre los que existe un amplio acuerdo en la industria y cuya implementación es ya posible. La definición establece específicamente que dichas medidas (tal como son utilizadas por los titulares de derechos de autor para identificar y proteger obras con derecho de autor) deben haber sido desarrolladas "en virtud de un amplio consenso entre los titulares de derecho de autor y los proveedores de servicio de una forma abierta, honesta, voluntaria y en el contexto de un proceso de normalización compartido por las diversas industrias; que estén disponibles en una forma razonable y no discriminatoria; y que no impongan un coste sustancial a los proveedores de servicio o un impedimento sustancial a sus sistemas o redes"[78]. Por el contrario, el Artículo 1201 de la DMCA no contiene definición alguna de "medida tecnológica". En contraste con los principios incluidos en la definición de "medida técnica normalizada", el Artículo 1201 protege los sistemas DRM propietarios desarrollados o adoptados unilateralmente cuyo precio es elevado o cuyo cumplimiento implique problemas de naturaleza técnica (excepto en la medida en que la disposición de "no-obligatoriedad" permita que los productos no respondan a dichas medidas).

– Ley de Grabación de Audio en el Hogar (*Audio Home Recording Act*): promulgada en 1992, establece la obligatoriedad de incluir un "sistema de gestión de copia en serie" (SCMS, *serial copy management system*) o un sistema funcionalmente equivalente en todos los "dispositivos de digitales grabación de audio" fabricados, importados o distribuidos en los Estados Unidos de América[79]. El objetivo de la ley era limitar la copia en serie incontrolada de música. Puede hacerse un número ilimitado de copias digitales partiendo del original, pero queda proscrita la realización de copias digitales adicionales a partir de dichas copias. La Ley también prohíbe el tráfico o comercialización de dispositivos o bien la prohibición de servicios "cuyo objetivo principal o cuyo efecto" sea la elusión de cualquier programa o circuito que implemente el SCMS (o un sistema con las mismas características funcionales que el SCMS)[80]; el acto de elusión en sí mismo no está prohibido.

La Ley también protege la información codificada en una grabación musical digital sonora. Queda prohibida la codificación de información inexacta en relación con el código de categoría (que está relacionado con el tipo de dispositivo que implementa el sistema), el

---

76 17 U.S.C. § 512.
77 § 512.i)1)B).
78 § 512.i)2).
79 17 U.S.C. § 1002.
80 § 1002.c).

estado relativo al derecho de autor (que puede ser reivindicado) o el estado de generación (original o copia) del material fuente utilizado para una grabación[81].

La Ley también impone un canon a los dispositivos de grabación de audio digital y a los medios de grabación de audio digital[82]. Finalmente, establece vías de recurso civiles, incluyendo medidas cautelares e indemnizaciones por daños directos y perjuicios[83].

– Ley del Fraude y Abuso por Computadora (*Computer Fraud and Abuse Act*): esta ley fue promulgada en 1986 por el Congreso y es relevante cuando la elusión de un sistema DRM se produce accediendo a una computadora, ya sea un servidor o una computadora personal, sin la debida autorización. La ley proporciona vías de recurso civiles y penales contra el "acceso intencionado a una computadora sin autorización o excediendo el acceso autorizado, y por lo tanto, por la obtención de … información de una computadora protegido si dicha conducta implica una comunicación interestatal o con el extranjero"[84]. También prohíbe el "acceso intencionado a una computadora protegido sin autorización, cuando el resultado de dicha conducta sea causar un daño"[85]. En general, el acto del acceso no autorizado debe haber causado un perjuicio de, al menos, 5.000 dólares para ser susceptible de reclamación judicial.

– Ley de Comunicaciones (*Communications Act*): esta ley prohíbe explícitamente tres casos de venta y distribución de "cajas negras" que desencripten señales encriptadas. Primero, protege las tecnologías de acceso condicional utilizadas para encriptar la programación por cable y satélite o los servicios por satélite directos al hogar prohibiendo la fabricación, ensamblaje, modificación y tráfico de cualquier dispositivo que una persona sepa (o tenga razones para saber) que sea "principalmente para la desencriptación no autorizada" de dichos programas[86]. Pueden imponerse indemnizaciones por daños y perjuicios, así como sanciones penales con multas de hasta 500.000 dólares y condenas de cárcel de hasta cinco años.

En segundo lugar, la Ley de Comunicaciones prohibió desde su promulgación, la interceptación no autorizada de cualquier comunicación de radio, así como la recepción no autorizada (o la ayuda para la recepción) de una comunicación de radio para el beneficio de una persona o de cualquier otra sin autorización de acceso a dicha comunicación[87]. Se establecen indemnizaciones por daños civiles y la vulneración intencionada puede sancionarse con una multa de hasta 2.000 dólares y una condena de cárcel de hasta seis meses. Si el acto se realizase para conseguir un beneficio comercial directo o indirecto, o un beneficio financiero privado, las sanciones incluyen multas de hasta 50.000 dólares y condenas de cárcel de dos años en caso de primera condena.

En tercer lugar, queda prohibida la interceptación o recepción no autorizada de cualquier servicio de comunicación por cable[88]. Los actos prohibidos incluyen la fabricación

---

81 § 1002.d).
82 § 1003.
83 § 1009.
84 18 U.S.C. § 1030.a)2)C).
85 § 1030.a)5)A)iii).
86 47 U.S.C. § 605.e)4).
87 § 605.a).
88 § 553.

o distribución de dispositivos destinados a dicha recepción no autorizada. Se establecen indemnizaciones por daños civiles y la vulneración de esta disposición está sancionada con multas de hasta 1.000 dólares y condenas de cárcel de hasta seis meses, con sanciones más elevadas si los actos se realizaran para conseguir un beneficio comercial o un beneficio financiero privado (hasta 50.000 dólares de multa y dos años de prisión en caso de primera condena).

– Leyes Estatales sobre la Seguridad de las Comunicaciones: desde hace tiempo muchos Estados han promulgado leyes que prohíben el robo de servicios de telecomunicaciones y por cable, la piratería de vídeos y los delitos por computadora. Desde el año 2002 se ha realizado un esfuerzo sustancial para modernizar dichas leyes y adaptarlas al entorno digital. Una coalición formada por la industria cinematográfica y los proveedores de servicios de comunicaciones, tales como operadores de cable y productores de programas, han instado a que los Estados faciliten el comercio electrónico mediante la protección de los contenidos digitales emitidos en tiempo real (*streaming*) o descargados de Internet mediante servicios de banda ancha.

Este grupo está promoviendo una "legislación para un modelo de seguridad en las comunicaciones" que proporcione una protección jurídica más amplia para todos los servicios de banda ancha y servicios por Internet en caso de acceso, recepción, transmisión y desencriptación no autorizada. Además, las medidas tecnológicas utilizadas para proteger el contenido de la programación quedarían protegidas legalmente de la elusión al dejar fuera de la ley los dispositivos que facilitaran el acceso ilegítimo. La legislación para un modelo de seguridad de las comunicaciones es percibida por sus críticos como la contrapartida a la DMCA a nivel estatal. En el momento de elaborar este informe, el modelo legislativo o algunas variantes al mismo han sido adoptados por varios Estados y está siendo considerado por otros.

De forma resumida, el modelo de ley, tal como está evolucionando durante los debates con compañías tecnológicas y con otros interesados, prohibiría entre otros actos los siguientes:

– el conocimiento con la intención de defraudar a un proveedor de servicios de comunicaciones y la posesión, utilización, fabricación, desarrollo, promoción y tráfico de cualquier "dispositivo de comunicación" para el hurto de un "servicio de comunicación" o para la recepción, interceptación, desencriptación o adquisición de un servicio de comunicación sin consentimiento explícito por contrato;

– la modificación, alteración o reprogramación de un dispositivo de comunicaciones con tales propósitos;

– la posesión, utilización, fabricación, desarrollo, promoción y tráfico de cualquier "dispositivo de acceso ilegítimo"; o

– la posesión, utilización o tráfico de 1) planes o instrucciones para realizar o ensamblar cualquier "dispositivo de comunicación" o "dispositivo de acceso ilegítimo" para cualquiera de dichos propósitos prohibidos, o 2) material, incluyendo *hardware*, datos, programas informáticos o cualquier otra información, a sabiendas de que el comprador o una tercera persona utilizará dicho material para la fabricación, ensamblado o desarrollo de un dispositivo de acceso ilegítimo o de un dispositivo de comunicaciones para un propósito prohibido.

La vulneración de estas disposiciones daría lugar a sanciones civiles y penales.

La legislación para un modelo de seguridad en las comunicaciones contiene un conjunto completo de definiciones que se resumen a continuación:

– "Dispositivo de comunicación" que incluye tanto un equipo capaz de interceptar, transmitir, adquirir, desencriptar o recibir cualquier servicio de comunicación, como cualquier componente del mismo, incluyendo cualquier número, circuito, conmutador, tarjeta, programa o chip que "permita facilitar" la interceptación, transmisión, desencriptación, adquisición o recepción de cualquier servicio de comunicaciones.

– "Servicio de comunicación", se define ampliamente e incluye esencialmente cualquier servicio que pueda concebirse para que, a cambio de un precio, se proporcionen contenidos sobre cualquier medio de comunicación, incluido Internet.

– Finalmente, se define ampliamente el concepto de "dispositivo de acceso ilegítimo" para incluir cualquier dispositivo, tecnología o programa informático que esté "principalmente diseñado, desarrollado, ensamblado y fabricado", o con el cual se trafique, "para burlar o eludir cualquier tecnología, dispositivo o programa eficaz, o cualquier componente o parte del mismo", utilizado para proteger una comunicación, datos o servicio de la adquisición, interceptación, acceso, desencriptación o revelación no autorizada.

La legislación para un modelo de seguridad en las comunicaciones se considera un modelo más amplio que la propia DMCA y, por este motivo, ha sido muy controvertida en diversos ámbitos. Prohíbe tanto el acto de elusión como las herramientas que permiten dicha elusión. El modelo legislativo hasta ahora utilizado no incorpora excepciones ni limitaciones (tales como las relacionadas con la ingeniería inversa y la investigación criptográfica) como las incluidas en la DMCA. Sin embargo, revisiones recientes de la misma han incluido una "cláusula de no-obligatoriedad", que pretende excluir productos legítimos del ámbito de las prohibiciones.

3.2.1.3 Actividades reglamentarias

3.2.1.3.a) Elaboración de disposiciones reglamentarias por la Oficina de Derechos de Autor

Tal como se ha descrito anteriormente, el Congreso estaba preocupado de que el Artículo 1201.a)1) de la DMCA afectara a los usos lícitos tradicionales de material con derecho de autor debido a que la ley prohíbe la elusión de las tecnologías de control de acceso incluso para dichos usos. Sin embargo, en el transcurso de las deliberaciones legislativas, el Congreso decidió no modificar el proyecto de ley para autorizar la elusión del control de acceso en relación con actividades que no constituyeran una vulneración. En lugar de ello, estableció un proceso mediante el cual el Bibliotecario del Congreso debería definir "la clase o clases específicas de obras" para las cuales estuviera permitida la elusión de medidas tecnológicas por parte de determinadas personas[89]. El Bibliotecario debe determinar cada tres años (tras un período inicial de dos años) si en relación con dichas clases, existen personas cuya capacidad para hacer un uso no vulnerador de dichas clases de obras se vea o pueda verse "negativamente afectada" en virtud del Artículo 1201.a)1).

[89] 17 U.S.C. § 1201.a)1)C).

Se ordena al Bibliotecario que examine diversos factores a fin de tomar una decisión, incluyendo la posible utilización de obras (particularmente para usos relacionados con el archivo, preservación y educación sin ánimo de lucro); el impacto del Artículo 1201.a)1) sobre usos lícitos tradicionales; y el impacto de la elusión en el mercado de obras protegidas.

El 28 de octubre de 2000, en la primera de dichas decisiones, el Bibliotecario estableció que sólo existían dos clases limitadas de obras que se podían beneficiar de una excepción en relación con las prohibiciones durante los tres próximos años: las compilaciones de sitios Web cuyo acceso está bloqueado por aplicaciones *software* de filtrado y las obras literarias cuyo acceso no puede hacerse debido a mal funcionamiento, daño u obsolescencia[90]. Actualmente, la Oficina de Derechos de Autor de la Biblioteca del Congreso, que debe realizar sus recomendaciones al Bibliotecario, está inmersa en el segundo de dichos procedimientos de elaboración de normas que debe estar terminado el 28 de octubre de 2003[91].

Las dificultades de quienes intentan que se reconozca una excepción están resultando ser bastante importantes. En primer lugar, deben demostrar que las disposiciones contra la elusión "afectan negativamente" a su utilización actual o futura de obras protegidas, lo cual resulta difícil de probar debido a que las tecnologías de control de acceso no están siendo aún ampliamente utilizadas.

En segundo lugar, deben demostrar que se ven perjudicados en relación con una "clase de obras" cuya definición está resultando ser ciertamente difícil para la Oficina de Derechos de Autor. Aunque las partes desean una excepción para "un uso lícito de las obras" la Oficina de Derechos de Autor ha denegado dicha petición debido a que no puede establecerse una "clase de obras" en función de cómo pueden usarse dichas obras. La Oficina ha concluido que el lenguaje de las disposiciones jurídicas y la historia legislativa impiden otorgar concesiones genéricas para un uso lícito.

Algunos defensores del uso lícito y otros que se han opuesto tanto a la DMCA en general como a lo limitado de sus excepciones, esperaban que estos procesos hubieran dado lugar a un mayor perfeccionamiento de la DMCA de lo que fue posible conseguir durante el debate en el Congreso. En el proceso actual por ejemplo, han solicitado que la Oficina de Derechos de Autor permita la elusión con fines específicos tales como evitar las limitaciones de la codificación regional de los DVD o la publicidad obligada en el DVD, el acceso a películas de dominio público en DVD y para objetivos de propósito general tales como participar en la investigación sobre tecnologías de control de acceso y conseguir el acceso a obras protegidas mediante mecanismos de control de acceso que exigen utilizar un sistema DRM especificado por el titular de derechos. A la vista de las normas establecidas en la decisión de octubre de 2000 del Bibliotecario, del lenguaje utilizado en la DMCA y de las dificultades asociadas a la carga de la prueba, es poco probable que la excepción de la prohibición del Artículo 1201.a)1) se extienda a una amplia variedad de "clases de obras". En este sentido, el Registro de Derechos de Autor ha sugerido que deberían presentarse ante el Congreso cualesquiera argumentos relativos a la posible ampliación de las categorías de obras

---

90 "Exemptions to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies", 65 Fed. Reg. 64556 (27 de octubre de 2000); 37 C.F.R. § 201.

91 "Exemptions to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies", 67 Fed. Reg. 63578 (15 de octubre de 2002).

elegibles para una excepción, así como las justificaciones de la excesiva dificultad que actualmente existe para conseguir una excepción[92].

Finalmente, debe señalarse que aunque se defina una excepción para un tipo particular de obra, solamente se permitiría el acto de elusión. Las herramientas que permiten la elusión continuarían estando prohibidas[93]. Por tanto, tener el derecho de eludir una medida de control de acceso sin poder disponer de herramientas que permitan la elusión a los usuarios normales resulta de poca utilidad. En todo caso, el Artículo 1201.a)2) seguiría prohibiendo el tráfico de herramientas de elusión a pesar de la existencia de excepciones; podría decirse que dichas herramientas no conseguirían pasar las pruebas incluidas en dicha Sección si estuvieran diseñadas o producidas principalmente para la elusión en aquellas circunstancias para las que el Bibliotecario las hubiera autorizado (y hubiera limitado otras utilizaciones).

3.2.1.3.b) Comisión Federal de Comunicaciones: proceso de elaboración de disposiciones reglamentarias basadas en la marca de radiodifusión

Los titulares de derechos han argumentado durante varios años que uno de los elementos más críticos no contemplados en la protección de los contenidos en la era digital es la radiodifusión de contenidos mediante televisión digital en abierto (transmitida sin ningún tipo de encriptación). Los sistemas de acceso condicional protegen el contenido hasta que éste alcanza el hogar. Tal como se señala en la sección 3.2.1, existen nuevas tecnologías (DTCP, HDCP y CPRM) para proteger los contenidos audiovisuales y de audio de una distribución no autorizada en las redes en el hogar, o desde el hogar a Internet, así como para la grabación de contenidos de forma segura. Sin embargo, para que los contenidos estén protegidos por dichas tecnologías, deben ser distribuidos de forma protegida, como por ejemplo, mediante un sistema de acceso condicional o algún otro mecanismo que indique que el contenido debe estar protegido en el hogar.

Los titulares de derechos están muy preocupados por la posibilidad de que los contenidos de televisión digital radiodifundidos que no estén protegidos cuando entren en el hogar puedan ser copiados, enviados a Internet o ser objeto de una distribución no autorizada. Como consecuencia de ello, pueden estar poco predispuestos a producir programas de televisión digital de alta calidad destinados a ser difundidos en formato digital.

En respuesta a dichas preocupaciones, diversos grupos privados iniciaron la evaluación de nuevas posibilidades en el seno del Foro denominado Grupo de Trabajo Técnico de Protección del Copiado (CPTWG, *Copy Protection Technical Working Group*), que en noviembre de 2001 creó un Grupo de análisis para la protección de la radiodifusión (desde 1996 el CPTWG se ha reunido mensualmente en Los Ángeles, California, para evaluar soluciones técnicas relacionadas con la protección del copiado). En junio de 2002, los copresidentes de dicho grupo publicaron un informe que reflejaba el amplio consenso alcanzado entre las diversas industrias involucradas en relación con un enfoque razonable sobre este problema. El informe recomienda que se utilice el desencriptador del control de redistribución incluido en la Norma ATSC A/65/A (la denominada "marca (o bandera) de radiodifusión") para señalizar que un contenido de televisión digital radiodifundido está protegido.

---

92 65 Fed. Reg. at 64562.

93 17 U.S.C. § 1201.a)1)E).

Entre los aspectos fundamentales reconocidos por todas las partes se encuentra la cuestión de la observancia: cualquier consenso del sector privado sobre la conveniencia de utilizar la marca de radiodifusión carecería de valor si no existiera un mecanismo para asegurar que los dispositivos detectaran y respondieran ante la presencia de dicha marca de radiodifusión. En particular, ha habido un amplio acuerdo (aunque no unánime), sobre la necesidad de algún tipo de mandato gubernamental para garantizar que todos los productos diseñados para recibir contenidos de radiodifusión digital se comporten adecuadamente.

Un conjunto adicional de aspectos hace referencia a las reglas aplicables a dispositivos de recepción de contenidos radiodifundidos, ya sea antes de la detección de la marca de radiodifusión o una vez detectada su presencia. Éstos incluyen: 1) el grado de protección del contenido de radiodifusión, y 2) los medios analógicos y digitales protegidos a los que un producto regido por dichas reglas puede enviar contenidos que incluyan la marca de radiodifusión. Otro asunto adicional es la elusión y, en concreto, cuál debe ser el grado de "robustez" del diseño y fabricación de dispositivos que implementen dichos requisitos a fin de evitar que se soslaye o evite la marca de radiodifusión.

Para responder a esta y otras cuestiones, la Comisión Federal de Comunicaciones (FCC, *Federal Communications Commission*) inició un proceso de elaboración de disposiciones reglamentarias (*rulemaking*) en agosto de 2002[94]. La FCC está evaluando si debe establecer la obligatoriedad de que los dispositivos reconozcan y actúen en función de la bandera ATSC o de cualquier otra señal, e igualmente si debe hacerse obligatorio que los receptores protejan los contenidos de la radiodifusión digital y cómo, y qué criterios deben utilizarse a fin de determinar las tecnologías de protección autorizadas para recibir contenidos que incluyan la marca de radiodifusión.

La FCC recibió muchos comentarios sobre estas propuestas, tanto de la industria como del público en general. Los principales impulsores de la promulgación de una disposición reglamentaria por parte de la FCC son los titulares de derechos, tales como la industria cinematográfica, los radiodifusores de televisión y algunas otras grandes compañías tecnológicas. Sin embargo, hubo muchos puntos de vista discrepantes, particularmente por parte de algunas compañías tecnológicas (principalmente con respecto a si la FCC debería regular los dispositivos), así como de numerosos grupos de consumidores y de interés público. Entre los aspectos que han dado lugar a más opiniones enfrentadas se encuentra la determinación de si un requisito reglamentario que obligara a que los contenidos de radiodifusión digital con marca de radiodifusión se grabaran de forma segura, restringiría las legítimas prácticas de grabación y reproducción personales en el hogar, o perjudicaría la capacidad de enviar contenidos sobre una red digital del hogar. Otro aspecto objeto de análisis ha sido si debería prohibirse utilizar la marca de radiodifusión para ciertos tipos de contenidos cuya distribución puede estar permitida o ser conveniente, como por ejemplo, los programas de emergencia.

Finalmente, en relación a la protección del contenido de la radiodifusión digital, existe un amplio consenso entre los titulares de derechos y algunas de las principales compañías tecnológicas de que debería adoptarse un enfoque de alcance internacional. Aunque la adopción por parte de la FCC de la marca de radiodifusión puede limitar significativamente la transferencia a Internet de contenidos digitales marcados en los Estados Unidos de América,

---

94 Véase "*In the Matter of Digital Broadcast Copy Protection*, Notice of Proposed Rulemaking, MB Docket No. 02-230, 67 Fed. Reg. 53903" (20 de agosto de 2002).

los programas de televisión radiodifundidos en los Estados Unidos de América se reciben en los países vecinos, desde donde podrían ser redistribuidos. Igualmente, cuando dichos programas se emiten en forma digital sin encriptar fuera de los Estados Unidos de América, pueden ser captados por receptores y ser encaminados hacia Internet. En consecuencia, se considera que si la FCC adopta finalmente el requisito de la marca de radiodifusión, se debería intentar conseguir la aplicación de disposiciones semejantes por mandato gubernamental en otras jurisdicciones.

3.2.1.3.c) Comisión Federal de Comunicaciones: Reglas de Compatibilidad de los Servicios por Cable y la Electrónica de Consumo

Otra área de la gestión de derechos en la que la FCC ha estado involucrada es consecuencia de los esfuerzos destinados a garantizar la compatibilidad entre los servicios por cable y los dispositivos electrónicos del consumidor, tales como los receptores de televisión de alta definición (HDTV, *High Definition Televisión*). En diciembre de 2002 y después de una larga e intensa negociación, un importante grupo de fabricantes de electrónica de consumo y los principales operadores de cable llegaron a un amplio acuerdo para asegurar la compatibilidad en modo "enchufar y funcionar" ("*plug and play*") entre los servicios de cable unidireccionales y la siguiente generación de receptores de televisión digital sin la necesidad de utilizar unidades de adaptación multimedia ("*set-top converter box*") para permitir que los consumidores reciban y graben señales HDTV y para permitir la conexión de nuevos dispositivos a los receptores de HDTV.

Una vez finalizadas las negociaciones del sector privado se presentaron sus acuerdos a la FCC, recomendado conjuntamente a ésta que determinara que los requisitos acordados fueran aplicables a todos los tipos de proveedores de programación de televisión de pago, por cable y por satélite, así como a los fabricantes de equipos. Los promotores del acuerdo consideran esencial la existencia de un mandato gubernamental que asegure un "campo de juego común" para toda la industria. Todos ellos apoyan con firmeza que tanto el Congreso como la FCC manifiesten que ésta última debe poner en marcha requisitos de compatibilidad de carácter universal que afecten a sistemas por satélite y a sistemas por cable.

Es igualmente importante que a lo largo de todo el proceso la FCC ha expresado su más firme apoyo a dichas negociaciones entre miembros del sector privado. En efecto, la propia FCC sugirió que se hiciera una propuesta común en el convencimiento de que la existencia de disputas no resueltas sobre la protección de contenidos de programas de televisión era un impedimento significativo que afectaría negativamente a la transición hacia la televisión digital en los Estados Unidos de América.

En relación con los aspectos relativos a la DRM, las partes han solicitado a la FCC que adopte disposiciones para la protección frente a la copia de los programas de televisión de pago, incluyendo reglas de codificación que sean obligatorias a nivel federal. En caso de que la FCC adoptara dichas reglas, éstas determinarían la forma en la que los consumidores podrían grabar ciertos tipos de programas recibidos por satélite o por cable (pero no los servicios distribuidos mediante cable módem o Internet). Desde el punto de vista de los fabricantes de productos electrónicos de consumo y del interés de los consumidores, estas reglas son parte integral y necesaria del acuerdo.

En general, las reglas de codificación específicas acordadas por las partes y que la FCC está considerando se basan en las establecidas en la tecnología DTCP y en el Artículo 1201.k)

de la DMCA[95]. Estas reglas permitirían a los titulares de derechos de programas de televisión marcar sus contenidos de forma que 1) sólo se pudiera hacer una generación de copias de un programa que hubiera sido distribuido mediante un servicio de suscripción mensual; 2) que puedan restringirse los programas vendidos en pago por visión, vídeo bajo demanda y suscripción de vídeo bajo demanda de forma que no se permita hacer copias, sino mantenerlos almacenados durante 90 minutos (o más en caso de acuerdo) en un grabador de vídeo personal; y 3) los contenidos radiodifundidos en abierto podrían ser copiados libremente. Las reglas propuestas también tratan sobre si se debería permitir, y cómo, la codificación de contenidos distribuidos a través de modelos de negocio nuevos y aún no definidos (es decir, distintos de los tipos de servicios antes descritos) y para la actualización de dichas reglas de codificación; la propuesta recoge que los operadores podrían aplicar distintas reglas de codificación para nuevos modelos de negocio, pero que cualquiera de dichas reglas esté sujeta a una posible reclamación ante la FCC (y a la pertinente resolución de ésta).

Inmediatamente después de que se remitiera el acuerdo a la FCC, ésta lanzó un proceso de consulta pública recogiendo las reglas que habían sido propuestas[96]. Naturalmente, las reglas de codificación (y otros elementos del acuerdo) son apoyadas por quienes han participado en los acuerdos y por otras entidades con intereses similares. Los operadores por satélite objetan verse afectados por dichas reglas.

Adicionalmente, algunos grupos de consumidores han expresado una fuerte oposición, particularmente contra la existencia de reglas de codificación obligatorias, puesto que temen que dichas reglas eliminen efectivamente algunos usos lícitos de grabación de ciertos tipos de programas para los que la grabación en el hogar está actualmente permitida. Muchos titulares de derechos, si bien han expresado un apoyo limitado al acuerdo, son también bastante críticos, particularmente en lo que se refiere a la inclusión de reglas de codificación que, creen, limitarían su capacidad para elegir el modelo de negocio a utilizar para distribuir contenidos mediante sistemas de acceso condicional. Por su parte, otros participantes en el proceso han expresado sus reservas en el sentido de que al amparo del acuerdo, las reglas de codificación podrían ser modificadas con demasiada facilidad o acabar haciéndolas inaplicables para los operadores.

---

95 Véase la Nota 56, en la que se describe el Artículo 1201.k).

96 Véase "*In the Matter of Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices*, CS Docket No. 97-80, *Compatibility Between Cable Systems and Consumer Electronics Equipment*, PP Docket No. 00-67, Further Notice of Proposed Rulemaking, 68 Fed. Reg. 2278 (16 de enero de 2003)".

3.2.1.4 Propuestas legislativas

Después de la promulgación de la DMCA, han tenido entrada en el Congreso muchas otras propuestas legislativas sobre numerosos aspectos, desde la modificación de la propia DMCA, a un papel más activo del Gobierno en el establecimiento de sistemas DRM para permitir que los titulares de derechos puedan aplicar soluciones denominadas de "autoayuda" para luchar contra la distribución no autorizada de contenidos. Ninguno de los proyectos de ley presentados ante el 107º Congreso (que finalizó en 2002) ha sido promulgado como ley, como tampoco ha sido aún promulgado ninguno de los proyectos de ley presentados ante el actual Congreso (el 108º). Sin embargo, dichas propuestas son ilustrativas para clarificar algunos de los aspectos pendientes y sobre los que siguen existiendo discrepancias aún después de la aplicación de los tratados de la OMPI en los Estados Unidos de América. Estas propuestas se resumen a continuación:

– Modificación de la DMCA: Autorización de elusión para usos lícitos. En octubre de 2002 se presentaron dos proyectos de ley para modificar la DMCA a fin de permitir la elusión en determinadas circunstancias. En primer lugar, la H.R. 5544, la Ley de Derechos de los Consumidores de Medios Digitales (*Digital Media Consumers' Rights Act*) supondría la creación de una excepción para actividades "exclusivamente orientadas a la investigación científica de medidas de protección tecnológica"[97]. El proyecto de ley también permitiría la elusión de una medida tecnológica "si dicha elusión no da lugar a una vulneración" (es decir, permitir la elusión en aras de un uso lícito[98]). Finalmente, el proyecto de ley autorizaría la fabricación, distribución o el uso no fraudulento de un "producto que permite un uso significativo no fraudulento de una obra con derechos de autor" (esencialmente para restaurar la responsabilidad por autoría indirecta expresada por el Tribunal Supremo)[99]. El principal promotor del proyecto de ley, el Congresista Richard Boucher, del Partido Republicano, declaró que su proyecto de ley trataba sobre la amenaza que las medidas tecnológicas de protección de la DMCA suponían para el uso lícito. En enero de 2003, el Congresista Boucher volvió a presentar la Ley de Derechos del Consumidor de Medios Digitales como H.R. 107[100].

En segundo lugar, se presentó la H.R. 5522, la Ley de Libertad y Elección Digital (*Digital Choice and Freedom Act*), que trata de la amenaza que supone la DCMA para los legítimos derechos y expectativas de los consumidores[101]. El proyecto de ley supone modificar la Ley de Derecho de Autor y la DMCA de varias formas. Se añadiría una nueva limitación a los derechos exclusivos de los titulares de derechos de autor: las personas que hubiera adquirido legítimamente una copia de una obra digital, o que hubieran recibido legítimamente la transmisión de una obra, tendrían la autorización necesaria para "reproducir, almacenar, adaptar o acceder a la obra" con fines de archivo o para ejecutar o visualizar la obra con fines no comerciales[102], presumiblemente sin tener en cuenta la aplicación de medida tecnológica alguna. Además, el proyecto de ley supondría modificar la DMCA para establecer expresamente que una persona podría eludir cualquier medida tecnológica si dicha medida impidiera un uso no fraudulento y el titular del derecho de autor no pusiera a

---

97 H.R. 5544, 107º Cong., 2ª sesión. § 5(a) (2002).
98 *Id*. § 5(b).
99 *Id*.
100 H.R. 107, 108º Cong., 2ª sesión (2003).
101 H.R. 5522, 107º Cong., 2ª sesión (2002).
102 *Id*. § 3 (propuesta de adición de un nuevo § 123 a la Ley de Derecho de Autor).

disposición del usuario los medios necesarios para hacer dicha utilización[103]. Finalmente, el proyecto de ley supondría una excepción de las provisiones contra la elusión orientadas a los dispositivos de la DMCA para aquellos productos diseñados, producidos o comercializados con el objeto de eludir una medida si dicha medida impidiera la utilización no fraudulenta y el titular de los derechos no pusiera a disposición del usuario los medios necesarios para hacer dicha utilización[104].

Un amplio grupo de titulares de derechos de autor y otras partes interesadas se han opuesto tanto a la H.R. 5544 como a la H.R. 5522 en el Congreso 107, así como a la H.R. 107 en el Congreso actual. Han argumentado que dichos proyectos de ley elevarían los precios y serían un obstáculo a la innovación en DRM y en tecnologías de distribución digital. Además, aunque reconocen que las propuestas permitirían la elusión de tecnologías DRM en aras de una utilización lícita, han enfatizado que los productos que serían permitidos podrían ser también utilizados para eludir sistemas DRM con fines ilegítimos. Además, señalan que debido a que la DMCA es una ley equilibrada que ha sido un modelo en otros países, la adopción de la H.R 107 sería un precedente perjudicial a nivel internacional porque reconocería que en los Estados Unidos de América se considera aceptable un cierto nivel de elusión

– Establecimiento de normas gubernamentales para las tecnologías DRM: probablemente el proyecto de ley con más eco y más controvertido sobre DRM considerado por el Congreso en la etapa de aplicación posterior a la DMCA ha sido la S.2048, Ley del Fomento de la Televisión Digital y la Banda Ancha para el Consumidor (*Consumer Broadband and Digital Television Promotion Act*), que se presentó en marzo de 2002[105]. El proyecto puso de relieve las notables diferencias existentes en la percepción de los papeles más adecuados para el sector privado y el gobierno en la formulación de normas, incluido lo relativo a las DRM. A raíz de las presiones de algunas compañías cinematográficas, el Senador Ernest Hollings introdujo y fue el principal promotor de la S. 2048. El propósito de esta medida legislativa era crear incentivos sustanciales para que el sector privado alcanzara un acuerdo sobre "normas para sistemas de seguridad" para dispositivos digitales y reglas de codificación. En caso de que el sector privado no consiguiera desarrollar dichas normas, el gobierno debería tomar medidas y establecer normas de forma obligatoria. Dichas normas deberían cumplir determinados requisitos señalados en el proyecto de ley y las reglas de codificación deberían permitir la copia personal de la televisión por cable y por satélite tanto en radiodifusión en abierto como en modalidad de pago[106].

Esencialmente, el proyecto de ley daba al sector privado 12 meses para finalizar dichos acuerdos. Si concluido ese período la FCC consideraba que el sector privado lo había conseguido con éxito, se establecía reglamentariamente que la FCC debería exigir el cumplimiento de dichas normas tecnológicas y reglas de codificación[107]. Sin embargo, si la FCC determinara que el sector privado no hubiera tenido éxito, el proyecto de ley habría exigido que la FCC adoptara normas DRM y reglas de codificación desarrolladas por el propio gobierno (cumpliendo los criterios legales) dentro de los 13 meses siguientes a dicha

---

103 *Id*. § 5.
104 *Id*.
105 S. 2048, 107º Congreso, 2ª Sesión (2002).
106 *Id*. § 3(d).
107 *Id*. § 3(b).

determinación[108]. El proyecto de ley habría permitido al sector privado modificar normas acordadas o establecidas por el Gobierno en circunstancias en las que la tecnología se hubiera visto comprometida o a la luz de mejoras tecnológicas[109].

Además, la S. 2048 contenía un conjunto de disposiciones para asegurar que los fabricantes y titulares de derechos cumplieran las normas. La primera habría prohibido la venta de futuros "dispositivos de medios digitales" (definidos como dispositivos de grabación digital, conversión o recuperación o acceso) en caso de que no cumplieran las normas[110]. La segunda habría prohibido la supresión o alteración consciente de una tecnología que cumpliera las normas, o la transmisión consciente de material con derecho de autor cuando la medida de seguridad hubiera sido eliminada o modificada[111]. La tercera habría prohibido la aplicación de una tecnología de seguridad que vulnerara las reglas de codificación[112].

Aparentemente no eran evidentes los problemas específicos o las deficiencias existentes en las tecnologías DRM (o los fallos del sector privado) que la S. 2048 pretendía resolver. El proyecto de ley proponía que el Congreso determinara que los acuerdos existentes no proporcionaban un entorno digital seguro y que los esquemas DRM existentes sólo ofrecían soluciones parciales y propietarias. Las potenciales resoluciones del Congreso habrían sido críticas para el sector privado, al establecer que "los intereses comerciales en competencia han frustrado la consecución de acuerdos para la aplicación de la tecnología existente en dispositivos de medios digitales con el fin de proteger los contenidos digitales en Internet o los de la radiodifusión de televisión digital"[113]. Era bien conocido, y las audiencias del Congreso así lo demostraron, que el Senador Hollings y los que apoyaban la S. 2048 tenían tres preocupaciones fundamentales: 1) el fallo de protección de la radiodifusión de televisión digital y su posible retransmisión a través de Internet; 2) la dificultad de impedir la retransmisión de contenidos convertidos en analógicos a partir de una fuente digital protegida (lo que se denomina problema del "agujero analógico"); y 3) las amenazas que supone el intercambio de ficheros con contenido digital entre particulares sin control ni autorización.

La S. 2048 se encontró con una dura y virtualmente unánime oposición de las compañías de tecnología de la información, compañías de electrónica de consumo, grupos de consumidores y usuarios de contenidos. Existían varios argumentos contra la propuesta. En primer lugar, el hecho de que el sector privado estaba realizando progresos en la resolución de estos asuntos (los estudios sobre la marca de radiodifusión habían finalizado con un informe que había permitido que la FCC lanzara el procedimiento de elaboración de disposiciones reglamentarias antes descrito). En segundo lugar, que sería muy contraproducente y un error involucrar al gobierno en el desarrollo y la imposición obligatoria de normas. En tercer lugar, que el gobierno no debería fijar plazos artificiales a los esfuerzos del sector privado para encontrar soluciones tecnológicas, especialmente para el espinoso problema del intercambio de ficheros. Los principales promotores del proyecto de ley eran los estudios cinematográficos y las empresas de radiodifusión.

---

108 *Id*. § 3(c).
109 *Id*. § 3(h).
110 *Id*. § 5.
111 *Id*. § 6.
112 *Id*.
113 *Id*. § 2.

– Soluciones basadas en iniciativas de ”autoayuda” contra el problema del intercambio de ficheros. Un enfoque completamente diferente en relación con los aspectos de protección de los contenidos sería impulsar el desarrollo y aplicación de iniciativas denominadas de “autoayuda” para impedir el comercio no autorizado de ficheros entre particulares. Los titulares de derechos y el Congreso habían sido incapaces de establecer medidas técnicas que solucionaran dicho problema. Aunque las denuncias interpuestas contra Napster y otros sistemas de intercambio de ficheros por la vulneración de derechos de autor habían sido exitosas desde el puesto de vista de los titulares de derechos, eran procesos que se dilataban mucho en el tiempo y sólo atacaban uno a uno los sistemas problemáticos. Además, cuando los sistemas están completamente distribuidos sin que exista un directorio o un conjunto de servidores centralizados del tipo Napster y servicios similares, la vía del litigio para detener los intercambios de ficheros masivos constituye una labor extremadamente difícil.

Cada vez más, los titulares de derechos empezaron a considerar si podían, y cómo, emplear tecnologías destinadas a interferir el intercambio de ficheros no autorizado, es decir, tecnologías tales como la interdicción, los señuelos, la redirección, el bloqueo de ficheros o el falseamiento de la dirección de origen (*spoof*). Sin embargo, los titulares de derechos de autor se preocuparon por el hecho de que la utilización de estas herramientas podrían justificar la interposición de demandas por parte de beneficiarios del intercambio de ficheros, tales como usuarios y organizaciones de consumidores, que se vieran afectados negativamente por dichas medidas.

Para tratar de solventar estas preocupaciones, el Republicano Howard Berman presentó en julio de 2002 la H.R. 5211, Ley contra la Piratería entre Particulares (*Peer-to-Peer Piracy Prevention Act*) [114]. Cuando presentó el proyecto de ley, comentó que aunque debería impulsarse el desarrollo y aplicación de soluciones DRM, dichos sistemas no trataban en su totalidad el problema del intercambio de ficheros ya que las obras con derecho de autor distribuidas a través de sistemas entre particulares estaban ya “en claro” (sin protección) en Internet.

La H.R. 5211 habría dado a los titulares de derechos de autor una salvaguarda legal indeterminada para poder llevar a cabo iniciativas de autoayuda contra el intercambio de ficheros, siempre que no se produjeran consecuencias colaterales. Un titular de derecho de autor hubiera tenido protección completa ante cualquier tipo de responsabilidad civil y penal, en el contexto de cualquier ley federal o estatal, por la “inhabilitación, interferencia, bloqueo, desvío o cualquier tipo de perjuicio” que afectara a un uso no autorizado de las obras con derecho de autor de dicho titular en una “red de intercambio de ficheros entre particulares accesible públicamente”[115]. Sin embargo, la salvaguarda sólo hubiera sido efectiva con la condición de que los actos del titular de derechos de autor no afectasen a ningún otro fichero o datos de la computadora de quien realizara el intercambio de ficheros. La salvaguarda legal dejaba de existir si se produjera un perjuicio económico a una persona diferente de la que hubiera realizado el intercambio de ficheros o si el daño económico sobre la propiedad de quien realizase el intercambio de ficheros fuera superior a 50 dólares (sin incluir las obras del titular de los derechos de autor)[116].

---

114 H.R. 5211, 107º Congreso, 2ª Sesión (2002).

115 *Id*. § 1(a) (propuesta de añadir un nuevo § 514 a la *Copyright Act*).

116 *Id*.

Una condición adicional para que la salvaguarda fuera efectiva era que el titular del derecho de autor debía advertir al Departamento de Justicia con una antelación de cinco días sobre las tecnologías específicas que pretendía utilizar para perjudicar las actividades de intercambio de ficheros no autorizadas[117]. Los titulares de derechos de autor debían asimismo advertir a quien realizaba el intercambio de ficheros, si éste lo solicitaba, del motivo por el que actuaban contra dicho intercambio, sin embargo, no era necesario que avisaran antes de iniciar la utilización de la herramienta de deterioro. Las actividades del titular de derechos de autor que perjudicaran de forma desproporcionada y produjeran un daño económico real a quien realizara el intercambio de ficheros, permitía a éste reclamar compensaciones. El Departamento de Justicia podía incluso llegar a imponer penas de cárcel a titulares de derechos de autor que hubieran realizado actividades dañinas abusivas sin una base razonable para creer que se hubiera producido un comportamiento ilegítimo[118].

Algunos grupos con intereses se opusieron a la H.R. 5211 debido a que desde su punto de vista el proyecto de ley no se limitaba a que el titular de derechos de autor impidiera el uso no autorizado de su obra. Argumentaban que la H.R. 5211 habría dado inmunidad a cualquier actividad (incluso a aquellas que hubieran producido la destrucción de otros ficheros) por parte del titular de derechos de autor para detener las actividades de quienes infringieran sus derechos mediante el intercambio de ficheros entre particulares. Asimismo, argumentaron que cualquier titular de derechos de autor podría realizar un ataque a la computadora de personas que participaran en este tipo de comercio utilizando cualquier tecnología, con la única condición de que el titular debía notificarlo previamente al Departamento de Justicia. Los ponentes del proyecto de ley señalaron la limitación de la salvaguarda legal y enfatizaron que se prohibía al titular de derechos de autor alterar o suprimir cualquier tipo de ficheros de la computadora de quien participaba en este tipo de comercio, aunque el proyecto de ley permitía bloquear la transmisión de las obras del titular de derechos de autor.

– Prohibición del tráfico de características de autenticación ilícitas. El Congreso también ha analizado el eventual reforzamiento de la ley contra la falsificación para prohibir el tráfico de "características de autenticación ilícitas anexas o integradas" en una copia de un programa informático, película o cualquier otra obra audiovisual o discográfica. En abril de 2002 se presentaron las modificaciones a la Ley contra la Falsificación (*Anticounterfeiting Amendments*), S. 2395, precisamente con dicho propósito[119].

En la S. 2395 se definía una "característica de autenticación" incluyendo filigranas digitales, símbolos, códigos, certificados, hologramas y otros medios utilizados para identificar que una copia o grabación sonora no ha sido falsificada. Se definió como "característica de autenticación ilícita" aquella característica de autenticación genuina en su origen pero que había sido alterada "con el propósito de inducir a que una tercera parte reprodujera o distribuyera" la copia, o bien, que ésta hubiera sido distribuida sin la autorización del titular de derechos de autor y no en relación con una copia realizada legítimamente a la que estuviera destinada la característica de autenticación integrada. En otras palabras, sería legítimo alterar un elemento de un sistema DRM, como por ejemplo una filigrana digital o un código de computadora destinado a verificar la autenticidad de una

---

117 *Id*.

118 *Id*.

119 S. 2395, Modificaciones a la ley contra la falsificación (Anticounterfeiting Amendments) de 2002, 107º Congreso, 2ª Sesión (2002).

copia de una obra, y la posterior distribución de dicho elemento para facilitar la distribución de copias pirateadas. Se implementaban recursos civiles y penales.

Debido a que S. 2395 era básicamente un proyecto de ley contra la falsificación, no tuvo inicialmente demasiada oposición. Algunos grupos de interés se opusieron a la misma cuando interpretaron que la propuesta se podía aplicar potencialmente a tecnologías o actos que podían perturbar las filigranas digitales. En marzo de 2003 se volvió a presentar el proyecto de ley denominada ahora S. 731, Ley de Defensa de la Identificación Mejorada y de las Características de Autenticación Seguras (*Secure Authentication Feature and Enhanced Identification Defense Act*) de 2003, pero con un alcance mucho más reducido y aplicable sólo a la protección de características de autenticación emitidas por el gobierno[120].

– Revelación obligatoria de medidas tecnológicas: una propuesta legislativa que implicara al gobierno en las tecnologías DRM sería, en caso de ser aprobada, menos intrusiva que algunos de los proyectos de ley antes analizados, ya que simplemente requerirían que los consumidores fueran convenientemente informados sobre la utilización de medidas tecnológicas destinadas a restringir su capacidad de utilizar contenidos. La S. 692, Ley del Derecho a la Información del Consumidor Digital (*Digital Consumer Right to Know Act*), se presentó en marzo de 2003 a fin de crear incentivos para que el mercado desarrollara sistemas DRM que atajaran los problemas de la reproducción y distribución no autorizados pero "preservando la máxima flexibilidad posible para los consumidores que utilizaran y manipularan" contenidos de forma legítima[121].

La S. 692 requería que la Comisión Federal de Comercio (*Federal Trade Commission*) elaborara disposiciones reglamentarias que exigieran a los productores o a los distribuidores de contenidos digitales con derechos de autor a desvelar de forma manifiesta cualquier característica tecnológica que limitara la capacidad de los consumidores para reproducir, copiar, transmitir o transferir dichos contenidos entre dispositivos de consumo normalmente utilizados[122]. Los proponentes del proyecto de ley describen dicha información previa como una cuestión de lealtad básica para que los hábitos de los consumidores no se vean truncados de forma inesperada. En concreto, la S. 692 obligaría a desvelar cualquier limitación tecnológica en relación con las prácticas siguientes: la grabación con desplazamiento temporal de la programación radiodifundida o de pago (pero no del pago por visión); el desplazamiento espacial o de la plataforma de contenidos de audio o vídeo (por ejemplo en el hogar y en la oficina o hacía dispositivos portátiles); la realización de copias de respaldo de contenidos adquiridos legalmente; la utilización de determinados pasajes para un uso lícito; y la transferencia o venta de contenidos legalmente adquiridos a otro consumidor (en la que el transferente o vendedor no retiene ningún derecho sobre el contenido)[123].

---

120 S. 731, 108º Congreso, 1ª Sesión (2003).

121 S. 692, 108º Congreso, 1ª Sesión. (2003).

122 *Id*. § 3(a).

123 *Id*. § 3(c). H.R. 107, citado más arriba, también incluye una disposición con un sistema que asume un enfoque destinado a desvelar; encargaría a la *Federal Trade Commission* que garantizara un etiquetado adecuado de los CD que estén protegidos contra la copia.

3.2.2 Jurisprudencia

Hasta la fecha, ha habido varias decisiones judiciales en los Estados Unidos de América que han interpretado las disposiciones contra la elusión de la Sección 1201.

Universal City Studios, Inc. contra Corley:[124] el caso más significativo relacionado con la DMCA es una denuncia interpuesta por ocho importantes estudios contra los demandados, que explotaban una publicación web en la que habían incluido, y animado a otros a copiar y distribuir, un algoritmo de desencriptación conocido como DeCSS. El DeCSS permite a los usuarios romper o eludir una medida tecnológica (CSS) que restringe el acceso no autorizado a discos de video DVD. Los acusados también incluían enlaces con otros sitios web en los que se ofrecía el DeCSS. El principal argumento de la defensa era que las disposiciones contra el tráfico del Artículo 1201.a)2) eran inconstitucionales porque vulneraban el derecho de los acusados establecido en la Primera Enmienda a la libre expresión, mediante el intercambio del código fuente DeCSS.

El juzgado de distrito determinó que el CSS "controla efectivamente el acceso" a películas en formato DVD, puesto que se requieren claves para acceder a las películas y dichas claves no pueden obtenerse sin una licencia CSS del CCA DVD. El juez también rechazó los argumentos de la defensa de que debido a que el CSS era un sistema de desencriptación débil, no era una medida tecnológica "efectiva", señalando que la ley no tendría sentido si solo protegiera medidas que fueran absolutamente efectivas.

El tribunal rechazó todos los argumentos de la defensa, concluyendo de forma categórica que los acusados no cumplían las condiciones para justificar una de las tres excepciones del Artículo 1201, que consideraban aplicables a sus actividades (ingeniería inversa, investigación criptográfica y pruebas de seguridad). También determinó que el uso lícito no era aplicable a un caso interpuesto en relación con el Artículo 1201.

Se ordenó a los acusados que retirasen el DeCSS en su sitio web. El mandato judicial también prohibía que los demandados mantuvieran enlaces con otros sitios que dispusieran del DeCSS. El tribunal señaló que la eliminación de dichos enlaces ayudaría a impedir la difusión del DeCSS, especialmente si dichos enlaces eran con sitios web situados fuera de los Estados Unidos de América.

En noviembre de 2001, el Tribunal de Apelación del Segundo Circuito de los Estados Unidos de América confirmó la decisión del tribunal de distrito en todos sus términos. El tribunal determinó que la medida cautelar era constitucional porque era "de contenido neutral" (estaba destinada exclusivamente a los componentes funcionales, no a la capacidad de expresión asociada al código de desencriptación (y en el caso de los enlaces, sólo a los aspectos funcionales, no de expresión, del hiper-enlace), y que sólo tenía una influencia menor en la "capacidad de expresión" de los acusados.

El tribunal de apelación examinó en concreto la cuestión de si debía permitirse la elusión del CSS cuando se hiciera para permitir un uso lícito de una película en DVD. En una interpretación del Artículo 1201.c)1), el tribunal concluyó que la DMCA tiene por objeto la elusión de protecciones digitales mediante disposiciones contra el tráfico, pero no se ocupa de

---

124 273 F.3d 429 (2ª Cir. 2001), *aff'g Universal City Studios, Inc. contra Reimerdes*, 111 F. Supp. 2d 346 (S.D.N.Y. 2000).

la utilización que pueda hacerse del contenido después de la elusión y rechazó la idea de que el Congreso intentaba permitir la elusión para un "uso lícito". Finalmente, el tribunal discrepaba de la posición de la defensa que argüía que la DMCA era anticonstitucional por eliminar la capacidad de hacer un uso lícito de obras con derecho de autor protegidas mediante control de acceso; el tribunal dictaminó que la doctrina del uso lícito no significaba que cualquiera pudiera tener acceso a material con derechos de autor.

RealNetworks, Inc. contra Streambox, Inc.:[125] una decisión anterior se produjo a raíz de una denuncia interpuesta por RealNetworks al amparo del Artículo 1201.a) y b). RealNetworks había desarrollado un sistema de distribución de contenidos que permitía a los titulares de derechos codificar sus obras de forma digital, y hacerlos llegar a los consumidores mediante un método seguro utilizando la aplicación RealServer. Los consumidores deben utilizar el RealPlayer para acceder a las obras. Conjuntamente RealServer y RealPlayer permiten recibir emisiones de datos en tiempo real (*streaming*), pero no realizar una copia de las obras, utilizando una secuencia de autenticación y un conmutador de copia (que permite que el titular de derechos determine si se autoriza la copia). La empresa Streambox había desarrollado un producto que sustituía al RealPlayer y engaña al RealServer haciéndole creer que se ha producido una autenticación verdadera; el producto no responde al conmutador de copia, por lo que los consumidores pueden grabar el contenido del flujo recibido.

El tribunal dictaminó que la autenticación era una medida tecnológica eficaz para el control de acceso en el sentido expresado por el Artículo 1201.a). El conmutador de copia, utilizado junto con la autenticación, era una medida tecnológica a tenor del Artículo 1201.b) porque permitía que un titular de derecho controlara el proceso de copia del consumidor. En consecuencia, el tribunal dictó medidas cautelares contra la distribución del producto, señalando que estaba principalmente diseñado para eludir las medidas tecnológicas de control de acceso y de control del copiado y que no tenía ningún otro objetivo desde un punto de vista comercial. Las partes llegaron a un acuerdo en septiembre de 2000.

Sony Computer Entertainment America, Inc. contra GameMasters, Inc.:[126] en una decisión tomada muy poco después de la aprobación de la DMCA, se dictaminó que un producto vendido por el demandado vulneraba el Artículo 1201.a)2)A). Las consolas PlayStation de Sony están diseñadas de forma que autentican los videojuegos; cada video juego tiene un código de región que debe concordar con la ubicación geográfica donde ha sido vendida la consola antes de poder utilizarse. El producto del acusado se conectaba a la Consola PlayStation de Sony y permitía al consumidor utilizar videojuegos importados o no territoriales. El tribunal prohibió el producto porque consideró que su función principal era eludir la función de autenticación de la codificación de región.

Estados Unidos de América contra Elcom, Ltd.:[127] Dmitry Sklyarov, un programador ruso, fue acusado de violar las disposiciones contra el tráfico de productos de la DCMA. Como empleado de la compañía rusa Elcom, creó un programa que desencriptaba el *software* de seguridad del eBook de Adobe, que permitía a los usuarios leer los eBook en múltiples formatos y que los copiaran. Elcom reaccionó para que se desestimaran los cargos, poniendo en duda la legalidad de la DCMA en base a varios principios constitucionales, incluyendo que el Artículo 1201.b) era inconstitucionalmente vago, que dicha sección limitaba su capacidad

---

125 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000).
126 87 F. Supp. 2d 976 (N.D. Cal. 1999).
127 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

de expresión así como los derechos de terceros de hacer un uso lícito de material con derechos de autor. En mayo de 2002, el juzgado de distrito rechazó cada una de tales las pretensiones y rechazó el recurso de Elcom. Haciéndose eco de la decisión del caso *Corley*, el tribunal estableció que incluso aunque la DCMA regulara directamente el derecho a la libre expresión constitucionalmente protegido, no afectaba al derecho del público de utilizar obras de dominio público u obras con derechos de autor, porque sólo afectaba a la capacidad de acceder a, y utilizar, copias concretas de dichas obras.

Existen pendientes de decisión judicial varios casos más en relación con la interpretación y aplicación de la DCMA. En uno de dichos casos, un fabricante de *software* desea que el tribunal declare que un *software* que permite copiar video discos DVD no vulnera las disposiciones contra la elusión de la DCMA[128]. Uno de los desarrollos más interesantes que han tenido lugar en los Estados Unidos de América es que la DMCA está siendo actualmente interpretada en un sentido amplio para prohibir la elusión de tecnologías distintas a DRM utilizadas por fabricantes en diversas aplicaciones industriales, con el efecto de que los competidores y sus productos no pueden tener acceso a un código de computadora que un fabricante puede utilizar para autenticar que sus productos sólo son utilizados por un consumidor[129].

3.3 Unión Europea

3.3.1 Marco jurídico

El 22 de mayo de 2001 la Unión Europea aprobó la directiva "relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información" ("Directiva de Derechos de Autor ")[130]. La Directiva de Derechos de Autor aplicó las diversas disposiciones de los tratados de la OMPI, incluyendo las disposiciones relativas a los derechos de autor sobre los derechos de reproducción, comunicación al público y distribución, así como las disposiciones que prohibían la elusión de medidas técnicas y de información para la gestión de derechos. Antes de la aprobación de la Directiva de Derechos de Autor en el ámbito de la Unión Europea, la elusión de medidas tecnológicas se trataba en otras tres directivas relativas a la protección jurídica de los programas informáticos, al acceso condicional y al comercio electrónico que se analizan más adelante.

Estas directivas tienen por objetivo armonizar la legislación de los Estados Miembros. Los principios de las directivas han sido o deben ser traspuestos por los Estados Miembros en sus respectivas leyes nacionales. En este sentido, la Directiva de Derechos de Autor es algo menos detallada, particularmente en lo relativo a las excepciones, que la DMCA (la

---

128 *321 Studios contra Metro-Goldwyn-Mayer Studios, Inc.*, No. C-02-1955 (N.D. Cal., presentado el 23 de abril de 2002).

129 Véase, por ejemplo, *Lexmark International, Inc. contra Static Control, Components, Inc.*, 253 F. Supp. 2d 943 (E.D. Ky. 2003) (decisión ordenando medidas cautelares preliminares) (el acceso al programa del motor de la impresora implica una secuencia de autenticación entre la impresora y el cartucho de tinta).

130 Directiva 2001/29/EC del Parlamento Europeo y del Consejo de 22 de mayo de 2001 relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, Diario Oficial L167/10, 22/06/2001.

caracterización precisa de dichas excepciones basadas en la Directiva se hará en la legislación nacional de cada Estado Miembro). El plazo para la trasposición de la Directiva de Derechos de Autor venció el 22 de diciembre de 2002.

3.3.1.1 Directiva de Derechos de Autor

3.3.1.1.a) Antecedentes

La Directiva de Derechos de Autor fue inicialmente propuesta en 1997 y, desde entonces hasta la fecha de su aprobación, fue objeto de un intenso debate a nivel comunitario en el que participaron los principales interesados (titulares de derechos, fabricantes de equipos de tecnología de la información y de electrónica de consumo y organizaciones de consumidores). El primer borrador de lo que llegó a ser la Directiva de Derechos de Autor prohibía " cualquier actividad " de elusión, principalmente dejando al margen de la ley el tráfico de herramientas de elusión, no los actos de elusión en sí mismos. A lo largo del tiempo, se prepararon y analizaron múltiples versiones de la directiva. Entre los aspectos más significativos discutidos durante este período, destacan la fundamental distinción entre, por un lado, la prohibición del acto de elusión y, por otro, el tráfico de herramientas de elusión, así como el alcance de las excepciones. Además, el alcance de la directiva se amplió desde prohibir las herramientas utilizadas para la elusión de las medidas de control de los derechos de autor hasta las que también eludían los controles de acceso.

3.3.1.1.b) Disposiciones contra la elusión

El Artículo 6 de la Directiva de Derechos de Autor aplica los Artículos 11 del WCT y el Artículo 18 del WPPT. Al igual que la DMCA, el Artículo 6 se aplica tanto a los actos de elusión como a las herramientas de elusión y, de una manera amplia, se aplica a las medidas tecnológicas que controlan el acceso así como el derecho de autor.

El Artículo 6.1) prohíbe los actos de elusión: los Estados Miembros establecerán "una protección jurídica adecuada contra la elusión de cualquier medida tecnológica efectiva". Sólo se prohíben los actos realizados "a sabiendas" o teniendo motivos razonables para saber que se persigue el objetivo de la elusión.

El Artículo 6.2) se dedica a las herramientas de elusión (incluyendo los servicios): los Estados Miembros establecerán "una protección jurídica adecuada" contra el tráfico (así como contra la posesión con propósito comercial) de herramientas que cumplan una de las tres condiciones siguientes:

– que sean objeto de una promoción, de una publicidad o de una comercialización con la finalidad de eludir la protección, o

– que sólo tenga una finalidad o uso comercial limitado al margen de la elusión de la protección, o

– que esté principalmente concebida, producida, adaptada o realizada con la finalidad de permitir o facilitar la elusión de la protección de cualquier medida tecnológica eficaz. Estas tres pruebas son bastante similares a las de la DMCA y, como tales, contienen incertidumbres semejantes (el significado de "principalmente"). Sin embargo, debe señalarse que una de los

considerandos de la Directiva de Derechos de Autor sugiere que las leyes nacionales pueden ir más allá del Artículo 6.2) y prohibir la "posesión privada" de productos para la elusión[131].

La Directiva de Derechos de Autor se basa en el enfoque de la DMCA para definir "medidas tecnológicas eficaces". Sin embargo, a diferencia de la DMCA, es en esta definición (y no en otras disposiciones diferentes, tal como se hace en el Artículo 1201.a) y e)) donde se establece el amplio alcance de las disposiciones contra la elusión aplicables tanto a las medidas de acceso como a las medidas de control de derechos de autor.

En el Artículo 6.3) se definen las medidas tecnológicas incluyendo cualquier tecnología que "en su funcionamiento normal, esté destinado a impedir o restringir actos referidos a obras o prestaciones protegidas que no cuenten con la autorización del titular de los derechos de autor o de los derechos afines a los derechos de autor establecidos por ley o el derecho *sui generis* previsto en el Capítulo III de la Directiva 96/9/CE [aplicable a las bases de datos]". En consecuencia, cuando se utilice una medida tecnológica para asegurar que se dispone de la autorización del titular de derechos antes de acceder o utilizar una obra, queda prohibida la elusión de la medida (por acto o producto). En este sentido, el concepto de "medidas tecnológicas" es más amplio que el incluido en la DMCA.

El Artículo 6.3) también define cuándo una medida tecnológica es "eficaz". Una medida tecnológica es "eficaz" cuando el uso de la obra o prestación protegidas esté controlado por los titulares de los derechos mediante "la aplicación de un control de acceso o de un procedimiento de protección, por ejemplo codificación, aleatorización u otra transformación de la obra o prestación o un mecanismo de control del copiado, que logre este objetivo de protección". Al definir que las medidas que deben protegerse contra la elusión sólo son aquellas que "logran este objetivo de protección", puede interpretarse que el artículo establece que solamente las medidas que de hecho sean "eficaces" serán consideradas como tales a los efectos de la Directiva de Derechos de Autor y de la aplicación de la ley. Además no está claro si un control de acceso o un proceso de protección "eficaz" sólo puede utilizar "la codificación, aleatorización u otra transformación de la obra" y si puede utilizarse cualquier tipo de "mecanismo" de "control del copiado". Además, el artículo utiliza el término "control del copiado" en lugar de "control del derecho de autor"; al hacerlo, se plantea si las medidas tecnológicas que controlan los usos no destinados al copiado de material con derechos de autor, tales como la ejecución en público o la distribución, caen realmente dentro del ámbito del Artículo 6.

La Directiva de Derechos de Autor es más amplia que la DMCA debido a que también prohíbe actos de elusión de medidas de control de derechos de autor y otros actos no autorizados por el titular de derechos. Por ejemplo, asume que una medida tecnológica se utiliza para condicionar el acceso y para utilizar contenido con derecho de autor, y que el acceso se concede al usuario sobre la base de un acuerdo que controla el uso ulterior que haga dicha persona. Si una persona vulnera dichas condiciones de utilización, eso constituiría un "acto no autorizado por el titular del derecho". Dicho acto quedaría prohibido por las disposiciones contra la elusión de la Directiva de Derechos de Autor (por el contrario, en los Estados Unidos de América el incumplimiento de este tipo de acuerdo puede suponer que se infringe el derecho de autor, pero no que sea un acto de elusión que la DMCA considere fuera de la ley). La matriz de prohibiciones de la Directiva de Derechos de Autor es la siguiente:

---

131 Considerando 49, Directiva de Derechos de Autor.

	Acto de elusión	**Herramientas de elusión**
Medida tecnológica de control de acceso	Prohibida (Art. 6.1))	Prohibida (Art. 6.2))
Medida tecnológica de control de derechos de autor	Prohibida (Art. 6.1))	Prohibida (Art. 6.2))

3.3.1.1.c) Limitaciones y excepciones

Al igual que la DMCA, la Directiva de Derechos de Autor contiene excepciones y limitaciones pero de una manera bastante diferente de la que presenta la ley de los Estados Unidos de América. El Artículo 6.4) no proporciona excepciones terminantes a las disposiciones contra la elusión en el mismo sentido que las establecidas en el Artículo 1201 de la DMCA. En lugar de ello, se inclina claramente por los acuerdos que puedan alcanzarse en el sector privado. El Artículo 6.4) se basa esencialmente en la voluntad de los titulares de derechos para que éstos concedan el acceso y permitan la utilización de obras protegidas por medidas tecnológicas en determinadas circunstancias. Solamente si los titulares de derechos no lo hacen, la Directiva de Derechos de Autor establece que los Estados Miembros "tomarán las medidas pertinentes para que los titulares de los derechos" faciliten a los beneficiarios las excepciones o limitaciones establecidas en el Artículo 5. La Directiva de Derechos de Autor no establece cuándo ni cómo debe actuar un Estado Miembro cuando no existan acuerdos voluntarios con los titulares de derechos que contemplen las excepciones y limitaciones.

La Directiva de Derechos de Autor utiliza, por tanto, un enfoque basado en varias etapas para que pueda establecerse una excepción o una limitación. En primer lugar, se establece que los Estados Miembros sólo actuarán "en caso de que los titulares de los derechos no adopten medidas voluntarias, incluidos los acuerdos" con otros interesados. Dichos "otros interesados" pueden incluir fabricantes de electrónica de consumo y de productos de tecnología de la información, consumidores y vendedores de medidas tecnológicas. En relación con los beneficiarios de las excepciones que sean usuarios finales, no queda en todos los casos suficientemente claro quiénes son las otras partes de un diálogo o eventual acuerdo. La Directiva de Derechos de Autor exige que se deje un "período de tiempo razonable" para que los titulares de derechos lleguen a acuerdos antes de la intervención de los Estados Miembros[132].

En segundo lugar, las medidas que deben tomar los Estados Miembros no exigen que las excepciones estén explícitamente incluidas en la legislación nacional. En lugar de ello, ésta puede ordenar que los titulares de derechos (y previsiblemente las medidas tecnológicas que utilicen) dispongan de salvaguardas para tener en cuenta actos específicamente identificados por parte de los usuarios finales. Debe tenerse en cuenta que no existe la certidumbre de que los Estados Miembros aplicarán estas excepciones de una forma armonizada. Además, tampoco se especifica la forma en la que deben intervenir los Estados Miembros cuando no existan medidas voluntarias y, en consecuencia, pueden existir actuaciones diferentes en los Estados Miembros.

[132] Considerando 51.

Tercero, las excepciones que los titulares de derechos conceden a los beneficiarios sólo deben otorgarse "en la medida necesaria". Cuarto, las personas que tengan "legalmente acceso" a la obra deben disfrutar del beneficio de una excepción. Quinto, y tal como se describe más abajo, debe aplicarse un régimen especial en relación con las excepciones o limitaciones a la elusión con fines privados.

Sin embargo, todo este régimen de excepciones tiene un aspecto crítico adicional que, en algunos sentidos, puede tener consecuencias significativas. El Artículo 6.4)4), establece que lo dispuesto en relación con los acuerdos voluntarios y los requisitos de los Estados Miembros no será de aplicación a las obras "que se hayan puesto a disposición del público con arreglo a lo convenido por contrato, de tal forma que miembros concretos del público puedan acceder a ellas desde un lugar y en un momento que ella misma haya elegido". Esta disposición tiene por objetivo permitir que puedan utilizarse diversos modelos de negocio y está principalmente destinada a obras que se ponen a disposición de los usuarios de forma interactiva y bajo demanda[133]. Ello incluye servicios de pago por visión/escucha/descarga o vídeo bajo demanda (que pueden considerarse distintos de un servicio por suscripción o de la "difusión" en línea). En dichas circunstancias, la Directiva de Derechos de Autor establece que, como consecuencia del contrato directo realizado con el usuario final en relación con la utilización de una obra determinada, los titulares de derechos no necesitan proporcionar excepciones o limitaciones a las medidas de acceso o de control del copiado.

En el Artículo 5 se establecen excepciones y limitaciones a los derechos de autor que los Estados Miembros pueden (pero no necesariamente deben) proporcionar en relación con la utilización de material con derecho de autor (así por ejemplo, varios Estados Miembros no han establecido excepciones genéricas para la copia privada). En consecuencia, los Artículos 5 y 6 establecen conjuntamente que la elusión de medidas tecnológicas se permite cuando dicho acto (o el tráfico de productos para la elusión) se realiza para beneficiarse de las excepciones o limitaciones en el ámbito de las leyes nacionales. Por lo tanto, a diferencia de la DMCA, en la que las excepciones del Artículo 1201 son esencialmente defensas frente a la acción de elusión, el enfoque de la Directiva de Derechos de Autor consiste en sugerir que los que un Estado Miembro puede, o no, permitir determinados actos subyacentes que supuestamente están contemplados por las medidas tecnológicas (sobre una base voluntaria o de otra forma). Los actos que pueden permitirse son los que se señalan a continuación.

Reproducciones permitidas: el Artículo 5 dispone que los Estados Miembros podrá establecer excepciones en sus leyes nacionales a los derechos de reproducción (5.2)) y de reproducción y comunicación (5.2) y (5.3)). Éstos incluyen:

– Reproducciones sobre papel (fotocopias), siempre que los titulares de los derechos reciban una compensación equitativa[134];

– Reproducciones efectuadas por bibliotecas, centros de enseñanza y museos o archivos que no tengan intención de obtener un beneficio económico[135];

– Grabaciones efímeras realizadas por organismos de radiodifusión y para su archivo[136];

---

133 Considerando 53.
134 Artículo 5.2)a), Directiva de Derechos de Autor.
135 Artículo 5.2)c).

– Reproducciones efectuadas por instituciones que no persigan fines comerciales "tales como hospitales o prisiones" a condición de que los titulares de los derechos reciban una compensación equitativa[137];

– Usos para fines educativos o de investigación científica, en la medida en que esté justificado por la finalidad no comercial perseguida[138];

– Cuando el uso se realice en beneficio de personas con minusvalías, guarde una relación directa con la minusvalía y lo exija la minusvalía considerada[139]; y

– Cuando el uso se realice con fines de seguridad pública o para asegurar una cobertura adecuada de los procedimientos gubernamentales[140].

Tal como se ha señalado, estos actos parecen favorecer los objetivos del Artículo 6 en cuanto que es previsible que las medidas tecnológicas los tengan en cuenta. El Artículo 5 establece excepciones y limitaciones para otros actos tales como formación, crítica o revisión periodística y el uso relacionado con el análisis político o las celebraciones religiosas. Éstos parecen ser también usos legítimos y son objeto de excepciones en las leyes de derechos de autor nacionales. Sin embargo, el Artículo 6 no exige que dichas excepciones adicionales reciban un tratamiento preferencial por parte de los titulares de derechos o de los Estados Miembros.

Copia privada: el Artículo 5(2)(b) permite a los Estados Miembros hacer una excepción para reproducciones realizadas "por una persona física para uso privado". De nuevo, una cláusula de la Directiva de Derechos de Autor establece que los Estados Miembros deben promover medidas voluntarias para incluir esta excepción y que deben tomar medidas en caso de que dicha excepción no se haya incluido en un "plazo razonable"[141]. Tampoco aquí existe certidumbre sobre si los Estados Miembros intervendrán en ausencia de dichas medidas y si lo harán de forma armonizada.

Ninguna de dichas reproducciones permitidas debe ser ni directa ni indirectamente comercial. Además, los titulares de derechos deben recibir "una compensación equitativa" que "tenga en cuenta la aplicación o no de medidas tecnológicas". En cuanto a este último punto, la relación entre la utilización de DRM y otras medidas tecnológicas y los sistemas de pago de un canon por copia privada para que los titulares de derechos reciban una compensación equitativa, han sido objeto de un amplio debate a nivel comunitario y se analizan en 5.1.3.

Esta disposición fue de las más debatidas antes de la aprobación de la Directiva de Derechos de Autor. El Artículo 6(4)(2) establece específicamente que los Estados Miembros pueden tomar medidas en relación con los titulares de derechos para asegurar que sea posible dicho tipo de reproducción personal no comercial, salvo que los titulares de derechos incluyan

---

[Continuación de la nota de la página anterior]

136 Artículo 5(2)(d).
137 Artículo 5(2)(e).
138 Artículo 5(3)(a).
139 Artículo 5(3)(b).
140 Artículo 5(3)(e).
141 Considerando 52, Directiva de Derechos de Autor.

la posibilidad de tales reproducciones en las medidas tecnológicas que utilicen. En este sentido, la Directiva de Derechos de Autor también señala que dichas medidas tecnológicas pueden estar permitidas de forma que limiten el número de reproducciones que pueden hacerse invocando dicha excepción (presumiblemente se refiere al número de copias privadas que puede realizar una persona individual).

En esta disposición, la Directiva de Derechos de Autor es mucho más directa y permisiva que la DMCA en lo que se refiere a la vinculación entre copia privada y elusión. Si bien la elusión en aras de una utilización lícita (incluida la copia privada) sigue estando prohibida en los Estados Unidos de América, la Directiva de Derechos de Autor contempla que la copia privada puede justificar la existencia de un requisito por el cual los titulares de derechos incluyan dicha utilización en las medidas tecnológicas empleadas.

Los considerandos de la Directiva de Derechos de Autor establecen excepciones y limitaciones adicionales. Sin embargo, el lenguaje de los considerandos no está imbuido por el carácter obligatorio de los artículos.

Ingeniería inversa: un considerando de la Directiva de Derechos de Autor establece que los Estados Miembros no deben impedir ni obstaculizar el desarrollo o la utilización de cualquier medio destinado a neutralizar una medida tecnológica necesaria para permitir la ingeniería inversa o el funcionamiento de programas informáticos, tal como autoriza la Directiva de Programas de Ordenador[142]. La ingeniería inversa debe cumplir dicha Directiva, es decir, debe realizarse en aras de la interoperabilidad.

Investigación criptográfica: otro considerando establece que la protección legal no debe "suponer obstáculos para la investigación sobre criptografía"[143].

Disposición de no-obligatoriedad: en relación con el concepto de "no-obligatoriedad" la Directiva de Derechos de Autor no es tan protectora de productos ordinarios como lo es la DMCA, que establece que no es necesario que dichos productos deban responder a medidas tecnológicas específicas. La Directiva de Derechos de Autor no incluye una excepción específica en este sentido, aunque existe un considerando que incluye una expresión similar a la utilizada en la Sección 1201(c)(3) de la DMCA: la protección jurídica de los Estados Miembros "no debe suponer una obligación de conformar los dispositivos, productos, componentes o servicios con dichas medidas tecnológicas, siempre que esos dispositivos, productos, componentes o servicios no se encuentren incluidos por otras razones en la prohibición del Artículo 6"[144]. El considerando establece que las medidas jurídicas no deben restringir dispositivos o actividades "cuyo empleo o finalidad comercial principal persiga objetivos distintos de la elusión de la protección técnica. Este considerando va más allá que el propio texto de la DMCA, aunque la historia legislativa de la DMCA pone de relieve el mismo punto.

---

142 Considerando 50, Directiva de Derechos de Autor, que cita el Artículo 5(3) y el Artículo 6 de la Directiva 91/250/EEC del Consejo sobre la protección jurídica de programas de ordenador, Diario Oficial L 122/42, 17/05/1991 ["Directiva de programas de ordenador"].

143 Considerando 48, Directiva de Derechos de Autor.

144 *Id.*

3.3.1.1(d) Información para la gestión de derechos

El Artículo 7 de la Directiva de Derechos de Autor establece que los Estados Miembros establecerán una protección jurídica adecuada frente a todas aquellas personas que "a sabiendas" supriman o alteren "información para la gestión electrónica de derechos" o distribuyan obras de las que se ha suprimido dicha información o que hayan sido alteradas sin autorización. Dicha supresión o alteración queda prohibida si la persona sabe o tiene motivos razonables para saber que al hacerlo induce, permite, facilita o encubre una violación de los derechos de autor, derechos conexos o el derecho *sui generis* de las bases de datos.

"La información para la gestión de derechos" se define de forma similar a la información para la gestión de derechos de autor de la Sección 1201 de la DMCA. Incluye información que identifique o está relacionada con la obra, sus condiciones de utilización así como cualesquiera números o códigos que representen a dicha información.

El considerando de la Directiva de Derechos de Autor aplicable a la información para la gestión de derechos señala el nexo existente entre el procesamiento de los datos personales obtenidos de la DRM, u otros sistemas técnicos, y los requisitos de las leyes europeas sobre la intimidad[145]. Esta relación se analiza en 5.2.1.

3.3.1.1(e) Vías de recurso

Aunque la Directiva de Derechos de Autor exige que los Estados Miembros apliquen sus disposiciones en sus respectivas leyes nacionales, no establece vías de recurso contra la violación de las disposiciones contra la elusión, dejando éstas al arbitrio de los Estados Miembros. Sin embargo, el Artículo 8 de la Directiva exige específicamente que los Estados Miembros proporcionen "sanciones y vías de recurso adecuadas" contra las transgresiones. Establece que dichas vías de recursos garanticen que los titulares de derechos puedan interponer acciones de resarcimiento de daños y perjuicios, solicitar medidas cautelares y, en su caso, que se incaute el material ilícito y los productos mediante los que se ha realizado la elusión. Este artículo se basa en partes relevantes de las disposiciones sobre observancia del Acuerdo sobre los ADPIC analizado en 3.2.1.1.

3.3.1.1(f) Supervisión y aplicación

La Directiva de Derechos de Autor incluye varios mecanismos para evaluar el efecto de la utilización de medidas tecnológicas sobre el mercado interno y los usuarios finales. En primer lugar, cada tres años la Comisión Europea debe remitir un informe sobre la aplicación de la Directiva de Derechos de Autor. El informe debe examinar si el Artículo 6 "confiere un nivel de protección suficiente y si los actos permitidos por la legislación se están viendo afectados negativamente por el uso de medidas tecnológicas eficaces"[146]. Este estudio es, en cierto modo, similar al procedimiento bianual que debe llevar a cabo la Oficina de Derechos de Autor y que exige la Sección 1201(a)(1) de la DMCA en virtud de la cual se debe analizar si los usuarios están siendo negativamente afectados por las medidas tecnológicas.

---

145 Considerando 57, Directiva de Derechos de Autor.

146 Artículo 12(1), Directiva de Derechos de Autor.

En segundo lugar, la Comisión podrá presentar, cuando sea necesario, propuestas para modificar la Directiva de Derechos de Autor[147]. En tercer lugar, la Directiva de Derechos de Autor establece un comité de contacto para analizar el impacto de la misma sobre el funcionamiento del mercado interior y "actuar como un foro de evaluación del mercado digital de las obras y otras prestaciones, incluidos la copia privada y el uso de medidas tecnológicas"[148]. En su conjunto, el proceso de revisión y de modificación que establece la Directiva de Derechos de Autor parece ser más amplio que el procedimiento establecido en la DMCA, que es de alcance limitado y que establece un nivel de exigencia muy elevado para las excepciones.

3.3.1.1(g) Aplicación

El 14 de julio de 2003 la Comisión Europea publicó una nota de prensa en la que señalaba que solamente Grecia y Dinamarca habían cumplido la fecha límite del 22 de diciembre de 2002 para la aplicación de la Directiva de Derechos de Autor y que Italia y Austria lo habían hecho posteriormente (aprobando leyes en abril y junio de 2003 respectivamente) [149]; la Comisión señaló que iniciaría procedimientos sancionadores contra los Estados Miembros que no hubieran transpuesto la Directiva de Derechos de Autor. Alemania había también promulgado legislación de aplicación de la Directiva de Derechos de Autor y otros Estados Miembros estaban en vías de realizar dicha aplicación. Por ejemplo, en Francia se ha elaborado un proyecto de trasposición y en otros Estados Miembros se han iniciado actividades de consulta.

Italia: Italia transpuso la Directiva de Derechos de Autor en un *Decreto Legislativo* del 9 de abril de 2003[150]. El Decreto Legislativo modifica la Ley italiana sobre la protección de derechos de autor y derechos conexos. El Artículo 23 del Decreto refleja el Artículo 6(3) de la Directiva de Derechos de Autor en su definición de "medidas tecnológicas" y en la descripción de las mismas para que sean consideradas "eficaces". La utilización abusiva de los procesos de elusión (es decir el acto de elusión), incluyendo la compra o alquiler de herramientas de elusión, está sujeto a sanciones administrativas[151]. El tráfico de herramientas y servicios para la elusión está sujeto a sanciones penales[152].

Alemania: a mediados de julio de 2003, Alemania aprobó la legislación para la aplicación de la Directiva de Derechos de Autor. La ley define "medidas técnicas" y medidas técnicas "eficaces" consistentes con la Directiva de Derechos de Autor. Una nueva Sección

147 *Id*.

148 Artículo 12(3) y (4).

149 Véase Comisión Europea: *Internal Market: Commission moves against 13 Member States for failure to implement EU legislation* (July 14, 2003), disponible en *http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/1005|0|RAPID&lg=en&display*.

150 Véase Decreto Ley de 9 de abril de 2003, n. 68, *Gazzetta Ufficiale*, n. 87 (14 de abril de 2003), disponible en *http://www.giustizia.it/cassazione/leggi/dlgs68_03.html*.

151 *Id.* en el Art. 28 (modificación del art. 174-ter de la Ley de Protección delos Derechos de Autor y Derechos Conexos (Ley No. 633 de 22 de abril de 1941, modificada por Decreto Ley de 26 de mayo de 1997, n. 154)).

152 *Id*. en el Art. 26 (modificación del art. 174-ter de la Ley de Protección delos Derechos de Autor y Derechos Conexos).

95a de la Ley de Derecho de Autor de 1965 prohíbe el acto de elusión de medidas técnicas eficaces a sabiendas, así como el tráfico de herramientas de elusión[153].

Determinados actos de tráfico ilegítimo de herramientas de elusión así como la propiedad o posesión de una herramienta con fines comerciales o la provisión de un servicio, son delitos administrativos (no penales); cada Estado alemán determinará qué autoridad será la responsable para tomar medidas administrativas contra quienes infrinjan los derechos de autor. El tráfico ilegítimo de herramientas de elusión para fines comerciales está sujeto a sanciones penales. La elusión internacional también está sujeta a sanciones penales sólo cuando el acto no sea exclusivamente para el uso privativo de la persona (o de personas relacionadas); se prescribe una sanción más estricta cuando el acto se haya realizado con fines comerciales[154]. Aunque la ley no lo establece específicamente, se supone que los titulares de derechos pueden iniciar procedimientos privados ante los tribunales contra aquellos que hubieran vulnerado los derechos.

El enfoque alemán para aplicar las excepciones y limitaciones del Artículo 5 de la Directiva de Derechos de Autor ha atraído la atención y ha preocupado a los titulares de derechos. Una nueva Sección 95(b) de la Ley de Derecho de Autor exige que los titulares de derechos otorguen a las personas la posibilidad de aprovechar las excepciones que prevé la Ley de Derecho de Autor en caso de que tengan acceso legítimo a las obras o al material. La Ley de Derecho de Autor incluye entre dichas excepciones el derecho a hacer una única reproducción de una obra para uso privado en cualquier medio de almacenamiento. Aunque la Sección 95(b) reconoce esta excepción, limita la elusión autorizada (para el único propósito de beneficiarse de la excepción) solamente en la medida en la que la reproducción se hace en papel. Sin embargo, la excepción de copia privada no existe si las copias se hacen a partir de fuentes ilegítimas.

No está claro cómo podrán cumplir los titulares de derechos estos requisitos si, por ejemplo, la medida técnica no está asociada directamente con la propia obra, sino que lo está con el modo de distribución. La forma de cumplir esta disposición es objeto de preocupación para los titulares de derechos porque si no ponen los medios necesarios para aplicar la excepción, estarían cometiendo una infracción administrativa. La ley también establece específicamente que las obligaciones contractuales que impidan a los usuarios aprovechar las excepciones son nulas de pleno derecho. Sin embargo, coherentemente con el Artículo 6(4) de la Directiva de Derechos de Autor, el derecho a beneficiarse de las excepciones no es aplicable cuando las obras se distribuyen de conformidad con acuerdos contractuales que permiten a los usuarios el acceso a las obras donde quieran y cuando quieran[155]. Además, los beneficiarios de las excepciones pueden exigir a los titulares de derechos que suministren los medios (a la discreción de los titulares de derechos) necesarios para beneficiarse de las excepciones. Para cumplir sus obligaciones, los titulares de derechos podrían, por ejemplo, poner a disposición de los usuarios una copia analógica u otra copia protegida; la ley no confiere a los beneficiarios el derecho de pirateo o de elusión.

La ley establece que los titulares de derechos deben etiquetar las obras y materiales protegidos por medios técnicos; no hacerlo sería una infracción administrativa. Dicha

---

153 Véase *Drucksache* 271/03 (2 de mayo de 2003), Art. 1, sección 34 (propuesta de modificación de la Ley de Derecho de Autor para incluir los nuevos §§ 95a hasta 95d).

154 *Id*. en la Sección 42 (propuesta de inclusión de un nuevo § 111a).

155 *Id*. en la Sección 34 (propuesta de inclusión de un nuevo §95b).

obligación, va más allá de lo exigido por la Directiva de Derechos de Autor. La forma de etiquetar obras que, por ejemplo, se descarguen desde servidores situados fuera de Alemania es aún una cuestión pendiente.

La ley también establece que sus diversas disposiciones entrarán en vigor en instantes de tiempo diferentes. La efectividad de las disposiciones relativas a las excepciones se retrasará por un año a fin de permitir que los titulares de derechos y las asociaciones que representan a los beneficiarios negocien y lleguen a acuerdos voluntariamente.

Francia: en Francia, el Ministerio de Cultura y Comunicaciones ha elaborado un proyecto de ley para transponer la Directiva de Derechos de Autor. El actual proyecto contiene un capítulo relativo a medidas técnicas que implica modificar el Código de Propiedad Intelectual a fin de incluir artículos que autoricen a los autores a utilizar medidas técnicas. Los actos de elusión y el tráfico de herramientas de elusión quedarían prohibidos. Sin embargo, al mismo tiempo el proyecto exige que los autores permitan que los beneficiarios de las excepciones establecidas en el Código (incluyendo el derecho a la copia privada) se beneficien de dichas excepciones, con independencia de la utilización de medidas técnicas, siempre que dichos beneficiarios tengan un acceso legítimo a las obras (el proyecto también refleja la excepción establecida en el Artículo 6(4) de la Directiva de Derechos de Autor en relación con los servicios "bajo demanda"). Las sanciones por elusión y tráfico no autorizado mantienen, en líneas generales, lo establecido en el Código por la violación de derechos de autor.

Reino Unido: En agosto de 2002, la Dirección de Derechos de Autor de la Oficina de Patentes publicó un documento de consulta sobre la aplicación de la Directiva en el Reino Unido, en el que se incluían modificaciones jurídicas[156]. Se recibieron comentarios sustanciales sobre las modificaciones necesarias para la aplicación del Artículo 6 de la Directiva de Derechos de Autor. Dada la naturaleza de los comentarios, la Oficina de Patentes señaló en julio de 2003 que la circulación de las modificaciones legales se había retrasado pero que los trabajos realizados en el Reino Unido para la aplicación de la Directiva de Derechos de Autor estaban "en vías de progreso avanzadas".

3.3.1.2 Otras directivas aplicables

La Directiva de Derechos de Autor no fue el primer esfuerzo de la Unión Europea para adoptar medidas de protección de las DRM y otras medidas tecnológicas utilizadas para la protección de las obras con derecho de autor. Merece la pena señalar tres directivas previas que se describen brevemente a continuación.

---

[156] Véase Directiva 2001/29/CE relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información: *Consultation Paper on Implementation of the Directive in the United Kingdom (Copyright Directorate*: 7 de agosto de 2002), disponible en *http://www.patent.gov.uk/about/consultations/eccopyright/pdf/ 2001_29_ec.pdf*.

3.3.1.2(a) Directiva de Programas de Ordenador

La Directiva de Programas de Ordenador que se aprobó en 1991 trata de las medidas tecnológicas utilizadas para proteger los programas de computadora[157]. El Artículo 7 exige específicamente que los Estados Miembros adopten medidas contra las personas que pongan "en circulación" o posean con fines comerciales "cualquier medio cuyo único propósito sea facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se hubiere utilizado para proteger un programa de ordenador"[158].

3.3.1.2(b) Directiva de Acceso Condicional

La Directiva de Acceso Condicional se aprobó en 1998 para proteger el acceso y la remuneración de diversos tipos de servicios distribuidos electrónicamente y a través de sistemas de acceso condicional[159]. La Directiva de Acceso Condicional está destinada a garantizar que se remunera al proveedor de servicios, no al contenido del servicio. El ámbito de la Directiva de Acceso Condicional es ampliable, siendo aplicable a servicios en línea, a la radiodifusión de televisión y de radio ya sea por cable o por medios radioeléctricos (incluido el satélite), así como a "servicios de la sociedad de la información"[160].

El acceso condicional se define como "cualquier medida o mecanismo técnico en virtud del cual se condicione el acceso al servicio protegido en forma inteligible a una autorización individual previa"[161]. La Directiva de Acceso Condicional prohíbe la comercialización de "dispositivos ilícitos". Los dispositivos ilícitos se definen como "cualquier equipo o programa informático diseñado o adaptado para hacer posible el acceso a un servicio protegido en forma inteligible sin autorización del proveedor de servicio"[162].

La Directiva de Acceso Condicional establece que los Estados Miembros prohibirán la fabricación, venta y alquiler de dichos dispositivos y su posesión con fines comerciales, así como su instalación, mantenimiento o sustitución y promoción comercial[163]. Las sanciones y vías de recurso previstas en el Artículo 5 son similares a las establecidas en la Directiva de Derechos de Autor. La Directiva de Acceso Condicional no prohíbe el acto de la elusión ni la posesión de un dispositivo ilícito para uso personal. La fecha límite para la transposición en las leyes nacionales fue el 28 de mayo de 2000.

Fundamentalmente basado en la Directiva de Acceso Condicional, el Consejo de Europa elaboró el Convenio Europeo sobre la Protección Jurídica de Servicios basados en, o que

---

157 Directiva 91/250/CEE del Consejo de 14 de mayo de 1991 sobre la protección jurídica de programas de ordenador (91/250/CEE), Diario Oficial L 122/42, 17/05/1991 ["Directiva de Programas de Ordenador"].

158 Artículo 7, Directiva de Programas de Ordenador.

159 Directiva 98/84/CE del Parlamento Europeo y del Consejo de 20 de noviembre de 1998 relativa a la protección jurídica de los servicios basados en, o que constan de, sistemas de acceso condicional, Diario Oficial L 320/54, 28/11/1998 ["Directiva de Acceso Condicional"].

160 Artículo 2(a), Directiva de Acceso Condicional.

161 Artículo 2(b).

162 Artículo 2(e).

163 Artículo 4.

constan de, Sistemas de Acceso Condicional[164]. El Convenio, que fue aprobado por el Consejo de Ministros en octubre de 2000 y que se puso a la firma el 24 de enero de 2001, es de aplicación a las naciones europeas dentro y fuera del ámbito de la Unión Europea.

3.3.1.2(c) Directiva sobre el Comercio Electrónico

La Directiva del Comercio Electrónico se aprobó en julio de 2000 para establecer el marco básico para el comercio electrónico en la Unión Europea[165]. La fecha límite para la transposición en leyes nacionales era el 17 de enero de 2002. La Directiva sobre el Comercio Electrónico contiene varias disposiciones importantes que son aplicables a la utilización de DRM para la entrega y protección de contenidos distribuidos al consumidor de forma electrónica.

En primer lugar, los Estados Miembros deben garantizar que pueden firmarse contratos por vía electrónica y que dichos contratos serán efectivos y válidos desde un punto de vista jurídico[166]. En consecuencia, eso significa que los contratos que se realizan desde una computadora aceptando sus condiciones haciendo un "click" y otros posibles contratos electrónicos, pueden ser la base para permitir que los contenidos estén disponibles en línea para los usuarios finales. Varias disposiciones de la Directiva exigen que los proveedores de servicio presenten la información de forma clara a los consumidores antes de que éstos hagan un pedido y que acusen recibo de los pedidos electrónicos[167].

En segundo lugar, la Directiva sobre el Comercio Electrónico proporciona a los proveedores de servicio intermediarios "salvaguardas" respecto a su responsabilidad sobre los contenidos que transmiten y almacenan, ya sea en memorias tampón de uso frecuente (*cache*) o de forma permanente. Estas disposiciones son similares a las de la DMCA descritas en 3.2.1.2. El artículo aplicable al procedimiento de memoria tampón (*caching*) establece que los Estados Miembros no pueden responsabilizar a un proveedor de servicio que almacene de forma automática y temporal contenidos con el fin de retransmitirlos, sujeto al cumplimiento de determinadas condiciones. Una de dichas condiciones es que el proveedor no interfiera "en la utilización lícita de tecnología ampliamente reconocida y utilizada por el sector, con el fin de obtener datos sobre la utilización de la información". Esta disposición se basa en lo expuesto en materia de salvaguardas en la Sección 512(i)(1)(B) de la DMCA. Tal como ocurre en los Estados Unidos de América, la Directiva sobre el Comercio Electrónico establece en Europa que el proveedor de servicios pierde su inmunidad en la medida en la que el proceso de memoria intermedia (*caching*) de contenidos interfiera con sistemas DRM y otras medidas tecnológicas empleadas por los titulares de derechos para hacer un seguimiento de la utilización de la información. Por lo tanto, existe un poderoso incentivo para que los proveedores de servicio garanticen que preservan las medidas técnicas ampliamente

---

164 Convenio Europeo sobre la protección Jurídica de los servicios de acceso condicional o basados en dicho acceso, ETS 178, disponible en *http://conventions.coe.int/Treaty EN/cadreprincipal.htm*.

165 Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, Diario Oficial L 178/1, 17/07/2000 ["Directiva sobre el Comercio Electrónico"].

166 Artículo 9(1), Directiva sobre el Comercio Electrónico.

167 Artículos 10 y 11.

reconocidas en la industria pues de otra forma están expuestos a una denuncia por infringir los derechos de autor (u otros derechos).

3.3.2 Dirección General de la Sociedad de la Información de la Comisión Europea: Taller sobre Gestión de Derechos Digitales

Tras haber conseguido la aprobación de la Directiva de Derechos de Autor, la Comisión Europea inició un proceso para investigar sobre una serie de asuntos, incluyendo la forma en la que la Comisión podría ayudar en la ulterior elaboración de un régimen para las DRM. En febrero de 2002, la Dirección General de la Sociedad de la Información inició una serie de talleres en los que ha tratado de reunir a las partes interesadas en la discusión de asuntos relacionados con las DRM, intentando determinar si existe consenso para una ulterior actuación por parte de la Comisión[168].

Entre los asuntos más significativos analizados (particularmente desde el punto de vista de las compañías tecnológicas y de los consumidores) se encuentra determinar si la implementación de DRM justificaría la supresión de los gravámenes impuestos a los dispositivos y medios de grabación. Sin embargo, los titulares de derechos se han manifestado más interesados en instar a la Comisión, o a otras instituciones, para que den los pasos necesarios para resolver los problemas relativos a la protección de contenidos en ausencia de desarrollo y acuerdos por parte del sector privado. El proceso se inició más para facilitar el análisis e intercambio de puntos de vista que con un objetivo predeterminado. La Comisión (teniendo en cuenta el potencial papel que podría desempeñar sobre este asunto) lanzó una serie de talleres cuyo telón de fondo eran los estudios en curso del Congreso de los Estados Unidos de América en relación con la Ley del Fomento de la Televisión Digital y la Banda Ancha para los Consumidores (*Consumer Broadband and Digital Television Promotion Act*), en la que se contemplaba el papel del Gobierno de los Estados Unidos de América en el establecimiento de normas.

El Considerando 54 de la Directiva de Derechos de Autor, relativo a la posibilidad de que las diferencias entre medidas tecnológicas podrían conducir a la incompatibilidad entre los sistemas dentro de la Unión, fue uno de los motivos que impulsaron con más fuerza el proceso. En la medida en que podrían desarrollarse barreras al comercio interior, la Dirección General para la Política de Empresa estaba también interesada en analizar la necesidad de normalizar las DRM.

Tras la Directiva de Derechos de Autor, la Comisión Europea solicitó al CEN/ISSS (Sistema de Normalización para la Sociedad de la Información del Comité Europeo de Normalización) que analizara el estado del arte en la normalización de DRM. En octubre de 2001 se estableció el grupo DRM del CEN/ISSS. El 31 de enero de 2003 se publicó para comentarios la primera versión de un proyecto de informe de gran importancia[169]. El documento resume en esencia los puntos de vista de los diversos actores que participan en

---

168 Véase el *informe* del Taller sobre Gestión de derechos digitales (DRM), de 16 de abril de 2002, disponible en *http://europa.eu.int/information_society/topics/multi/digital_rights/doc/workshop2002/workshop_report1.pdf*.

169 Véase *Digital Rights Management: Draft Report*, CEN/ISSS (Draft 1.2, 5 de febrero de 2003), disponible en *http://www.cenorm.be/isss/DRM/draft_report1_2.pdf*.

este asunto de una forma completa sin presentar recomendaciones sobre la política o las normas y sin incluir conclusiones.

Durante el proceso de estudio de la gestión de derechos digitales realizados por la Dirección General para la Sociedad de la Información, se han celebrado cuatro talleres. Cada uno ha estado dirigido por un sector en concreto aunque han sido invitados representantes de todos los sectores. El último taller, en el que se presentaron los puntos de vista recabados, se celebró el 25 de marzo de 2003[170].

Grupos de intereses de usuarios y consumidores: el primer taller estuvo liderado por los grupos de interés de usuarios y consumidores, tales como la Organización Europea de Consumidores (BEUC, *Bureau Européen des Unions de Consommateurs*), y distribuidores de contenidos representados por la Asociación Europea de Medios Digitales ("EdiMA"). Los asuntos analizados incluían la posibilidad de que las DRM limitaran la capacidad de los consumidores para acceder a contenidos, incluida la copia privada. Se exigió que las DRM respetaran el marco jurídico, incluida la posibilidad de beneficiarse de las excepciones de la Directiva de Derechos de Autor, así como que se garantizara la interoperabilidad entre las tecnologías. A este respecto, los consumidores expresaron su preocupación de que mediante las DRM se les pudiera exigir contratar derechos que debían estar garantizados por las excepciones de los derechos de autor. También solicitaron a los gobiernos que no permitieran que los titulares de derechos utilizaran las DRM para obstaculizar el acceso a las obras de dominio público.

Otros asuntos de naturaleza política que fueron planteados por los usuarios son la necesidad de que se muestre a los mismos de forma clara que los productos están protegidos por derechos de autor y que se supriman los gravámenes de forma que los titulares de derechos no sean compensados dos veces, una vez a través de un canon y otra por un pago realizado mediante DRM. Por tanto, solicitaron que los gravámenes desaparecieran una vez que se aplicaran sistemas DRM.

Otro asunto que preocupaba a los consumidores es la posibilidad de que los sistemas DRM recopilen datos personas que puedan afectar negativamente a la privacidad. También urgieron para que las normas DRM no fuera una imposición de los gobiernos sino el resultado de los esfuerzos desarrollados por la industria.

Las industrias de las tecnologías de la información y la comunicación (ICT) y la industria de la electrónica de consumo: el segundo taller fue liderado por las industrias tecnológicas a través de la Asociación Europea de Tecnologías de la Comunicación y la Información (EICTA, *European Information and Communication Technology Association*). El principal objetivo de la sesión era garantizar que todos los participantes compartieron un nivel de conocimiento común sobre el estado y el desarrollo de las tecnologías DRM y explicar que las DRM pretendían "hacer que la gente honesta siguiera siendo honesta", más que erradicar la piratería comercial. Además, las industrias solicitaron que los titulares de derechos aseguraran que las DRM fueran desplegadas de forma que los consumidores pudiera beneficiarse de las excepciones a los derechos de autor coherentes con sus demandas y expectativas legítimas.

---

170 Véase *http://europa.eu.int/information_society/topics/multi/digital_rights/events/ index_en.htm* (donde se describen los eventos en relación con el proceso sobre las DRM llevado a acabo por la DG de la Sociedad de la Información).

Una parte fundamental de la posición de las industrias tecnológicas es que no es necesario establecer gravámenes por copia privada sobre dispositivos y medios en un entorno digital. En primer lugar, las industrias argumentaron que los titulares de derechos pueden controlar la copia privada de sus derechos mediante las DRM, introduciendo por tanto la posibilidad de recibir múltiples pagos de los consumidores. En segundo lugar, señalaron que el ámbito de la imposición de gravámenes en un entorno digital podría ampliarse enormemente, dado que existe una amplia gama de dispositivos y medios (computadoras personales, asistentes digitales personales, dispositivos de adaptación multimedia, o descodificadores, y memorias removibles o integradas) que pueden manipular y almacenar contenidos. Se señaló lo inadecuado de imponer gravámenes sobre dispositivos y medios multipropósito con independencia de su utilización real.

Las industrias tecnológicas expresaron asimismo su preferencia por la participación del sector privado, en lugar de los gobiernos, en relación con las DRM. El sector de las tecnologías de la información y comunicación (ICT) y de la electrónica de consumo se opuso al establecimiento de obligaciones por los gobiernos en lo relativo a la especificación de la tecnología. También hicieron énfasis en que los aspectos de interoperabilidad debían tratarse de forma voluntaria en un foro liderado por la industria.

Titulares de derechos: el tercer taller fue organizado por la comunidad de titulares de derechos, incluida la Asociación de la Industria Cinematográfica (MPA, *Motion Picture Association*), la Federación Internacional de la Industria Discográfica (IFPT, *International Federation of the Phonographic Industry*) y la Federación Europea de Editores. Desde su punto de vista, las DRM debían considerarse como tecnologías habilitadoras: permiten que haya más contenidos disponibles (en lugar de bloquear el acceso a los mismo), hacen posible nuevos modelos de negocio y, en consecuencia, amplían la capacidad de elección de los consumidores para seleccionar e interactuar con contenidos protegidos por derechos de autor. En relación específicamente con los sistemas DRM, los titulares de derechos señalaron que el mercado de DRM aún es incipiente y que existen pocos equipos disponibles, siendo imperativo que las tecnologías DRM se diseñen bajo una concepción de seguridad y renovabilidad (es decir, que permitan recuperar el estado de seguridad en caso de ataque por parte de piratas informáticos u otro tipo de elusión).

Además, dado que las tecnologías DRM aún no están maduras, los titulares de derechos creen que es prematuro utilizar los controles tecnológicos de las DRM como justificación para eliminar gravámenes. Los titulares de derechos también expresaron su preocupación de que las actuales tecnologías DRM sólo permiten una interoperabilidad limitada e instaron a los gobiernos y a la industria a que apoyaran el trabajo realizado en foros internacionales en favor del desarrollo de normas abiertas. Los titulares de derechos expresaron una clara preferencia por las normas desarrolladas por la industria, pero también enfatizaron que el papel de los gobiernos puede ser necesario para garantizar la conformidad con normas acordadas y cuando fracasen las negociaciones del sector privado.

Los titulares de derechos también identificaron asuntos específicos que deberían desarrollarse ulteriormente. Entre los que requieren una atención prioritaria se encuentra la necesidad de garantizar que se desarrolle un entorno seguro para los contenidos en el contexto de las computadoras personales (una tarea realmente difícil dado que se trata de dispositivos multifuncionales que se programan libremente). Los titulares de derechos también destacaron la conveniencia de estudios adicionales sobre lo que describieron como “lagunas” en los sistemas DRM, incluyendo el “agujero analógico” que tiene lugar en la conversión de un formato digital a un formato analógico, sin mantener la protección original, así como la

necesidad de proteger los contenidos que se radiodifunden mediante televisión digital de la amenaza de una retransmisión no autorizada (asunto sobre el que versa la elaboración de una norma sobre la marca – bandera - de radiodifusión de la FCC analizada en 3.2.1.3(b)).

Sociedades de gestión colectiva: las sociedades de gestión colectiva (CMS, *collective management societies*) representan a los titulares de derechos en la negociación y administración de acuerdos sobre licencias, incluida la recaudación y distribución de derechos a través de las sociedades de autor existentes en todo el mundo. Tal como describe en la documentación remitida por las CMS al proceso iniciado por la DG de la Sociedad de la Información, estas sociedades documentan y otorgan licencias sobre derechos, velan por la observancia de las leyes de propiedad intelectual y supervisan, auditan, educan e informan al público en relación con la necesidad de respetar los derechos de autor. Durante el taller, las CMS expresaron su preocupación sobre el hecho de que existía muy poca concienciación de su papel en la sociedad de la información en general (estas sociedades proporcionan el acceso y otorgan licencias para utilizar obras con derecho de autor a nivel mundial), y en particular, en lo que se refiere al desarrollo y utilización de las DRM para llevar a cabo sus funciones. En concreto, las CMS están preocupadas de que en la medida en que las DRM pueden facilitar la relación directa entre los distintos tipos de titulares de derechos y los consumidores, tanto para la concesión de derechos como para la liquidación y compensación de los mismos, pueda disminuir la necesidad de las propias CMS en un entorno digital. En este sentido, las CMS desean mantener su papel actual que consideran que debería mejorar, y no duplicar, las funciones de los sistemas DRM. Señalaron que las CMS están desarrollando componentes DRM y destacaron la importancia de la cooperación en el desarrollo de tecnologías DRM.

Además, tal como hicieron los titulares de derechos, las CMS señalaron que las DRM aún están en una fase inicial de desarrollo y pueden no ser aplicables en muchas circunstancias, incluyendo los dispositivos preexistentes, la reconversión de digital a analógico y la copia privada. En general, las CMS no creen que haya llegado el momento de abolir los gravámenes por copia privada.

Además, las CMS instaron a que se realizaran estudios adicionales sobre la interoperabilidad (señalando la necesidad del desarrollo y aplicación de normas internacionales) así como sobre aspectos de seguridad y observancia (incluida la adaptación a nuevos modelos de negocios). Señalaron que podría ser suficiente el desarrollo voluntario de normas liderado por la industria y que, por tanto, no defendían un papel más activo de los gobiernos.

Resumen de lo tratado en los talleres: aunque no se ha preparado un resumen formal de las conclusiones de los talleres sobre DRM, de las discusiones habidas merecen ser destacados los temas siguientes:

– Puede ser necesario realizar estudios adicionales para una mejor comprensión del alcance y capacidades de las soluciones basadas en DRM.

– Las tecnologías DRM (incluyendo la interoperabilidad entre los distintos sistemas) deben ser desarrolladas sobre la base de esfuerzos voluntarios y liderados por la industria, sin que haya acuerdo en relación con el papel más adecuado que pueden desarrollar los gobiernos.

– Los asuntos relacionados con la protección de contenidos discretos y particulares merecen una atención adicional por todos los grupos del sector privado afectados.

– Aunque las DRM permiten nuevos modelos de negocios y más capacidad de elección para el consumidor, se reconoce que es necesario tener en cuenta las expectativas de los consumidores y las excepciones a los derechos de autor.

– Son necesarios estudios adicionales sobre la implementación de sistemas DRM en relación con la continuación o imposición de gravámenes sobre los dispositivos y medios digitales.

3.3.3 Jurisprudencia

Dada la relativamente reciente aprobación de la Directiva de Derechos de Autor, que aún no ha sido transpuesta en las leyes nacionales de la mayoría de Estados Miembros, no es sorprendente que no exista jurisprudencia significativa aplicable a las disposiciones contra la elusión. Sin embargo, han existido casos en los que se ha hecho una interpretación en base a las leyes nacionales existentes para prohibir determinados tipos de dispositivos de elusión.

Sony Computer Entertainment contra Owen:[171] en el Reino Unido, Sony Computer Entertainment presentó demandas contra varios importadores de "chips de modificación" que podían ser utilizados para infringir la protección contra la copia y la tecnología de control de región de los discos de juegos para la consola PlayStation 2. Los hechos de la denuncia eran esencialmente los mismos que los traídos a colación en un asuntos anterior relativo a la decisión sobre *GameMasters* en los Estados Unidos de América.

El Tribunal inglés se basó en los fundamentos jurídicos sobre derechos de autor establecidos en la Sección 296 de la Ley de Derecho de Autor, Diseños y Patentes (*Copyright, Designs and Patents Act*) de 1988. La Sección 296 se aplica cuando se hacen copias de una obra en formato electrónico que está "protegida contra la copia" y se otorgan derechos al distribuidor de las copias (como si se tratara del titular de derechos de autor en un caso de elusión) a cualquier persona que venda un dispositivo que esté "específicamente diseñado o adaptado para eludir" la protección contra copia, a sabiendas de que el dispositivo se utilizará para realizar copias ilícitas[172]. "Protegida contra la copia" se define de forma que incluye "cualquier medio destinado a impedir o restringir la copia de la obra". El Tribunal resolvió a favor de Sony porque la copia que se pretendía impedir era la descarga no autorizada del juego en una computadora y porque los códigos incluidos en los discos se incluían en la definición de protección contra copia. Los demandados vulneraron la Sección 296 porque sus chips estaban específicamente diseñados para eludir la tecnología de protección de copiado de Sony.

---

171 [2002] EWHC 45 (CH).

172 *Copyright, Designs and Patents Act* 1988 (c. 48), s 296(2).

3.4 Australia

3.4.1 Marco jurídico

3.4.1.1 Ley de Modificación del Derecho de Autor (Agenda Digital) del 2000

3.4.1.1(a) Antecedentes

Australia ha aplicado los tratados de la OMPI mediante la Ley de Modificación de Derechos de Autor, Agenda Digital, del 2000 (*Copyright Amendment - Digital Agenda - Act*, DAA), que entró en vigor el 4 de marzo de 2001 y que modificaba la Ley de Derecho de Autor de 1968[173]. La aplicación comenzó a gestarse en Australia en 1997 con un documento de análisis titulado *Copyright Reform and the Digital Agenda* (*Reforma del derecho de autor y Agenda Digital*), y continuó un proyecto expositivo y comentado sobre la Modificación del Derecho de Autor de la Agenda Digital en 1999. En última instancia, el enfoque utilizado en Australia para aplicar los tratados de la OMPI se ha caracterizado por ser más favorable para los usuarios que sus homólogos en los Estados Unidos de América y en la Unión Europea. Ello refleja el hecho de que Austria importa más productos con derechos de autor de los que exporta.

3.4.1.1(b) Disposiciones contra la elusión

La DAA prohíbe el tráfico de herramientas de elusión, incluida la fabricación, venta, alquiler, ofertad de venta, promoción, publicidad, comercialización, distribución y exhibición de dispositivos. La prohibición incluye la oferta de dispositivos de elusión en línea, pero sólo "en la medida en que afecta perjudicialmente al titular de derechos de autor"[174]. Cuando los actos consisten en la oferta de un "servicio de elusión", la DAA, al igual que sus homólogas en los Estados Unidos de América y Europa, prohíbe dicha actividad[175]. Un elemento de la prohibición es que el acusado debe conocer o debiera razonablemente tener conocimiento de que el dispositivo o servicio podría utilizarse para le elusión o para facilitar la elusión de una medida de protección tecnológica[176]. Sin embargo, la DAA no prohíbe específicamente el acto de la elusión.

La definición de "medida de protección tecnológica" anticipa el enfoque seguido en la Unión Europea, incluyendo tanto medidas de control de acceso como de control del copiado. Sin embargo, el lenguaje empleado siguen básicamente el de la DMCA. En concreto, la DAA define una medida de protección tecnológica como un dispositivo o producto (incluidos sus componentes) diseñado "para que en su utilización normal impida o inhiba la elusión del derecho de autor de una obra o material conexo mediante alguno de los medios siguientes":

– Garantizando que "el acceso a una obra" existe "únicamente utilizando un código de acceso o proceso (incluyendo la desencriptación, desaleatorización u otra transformación de la obra…) que tenga la autorización del titular o licenciatario del derecho de autor;

---

173 Las disposiciones relevantes se incluyen en una nueva División 2A de la Parte V de la *Copyright Act* de 1968 (Cth).

174 *Ley de Derechos de Autor (Copyright Act)* 1968 (Cth) s 116A(1)(b)(i)-(vi).

175 s 116A(1)(b)(vii).

176 s 116(A)(1)(c).

– Mediante un mecanismo de control del copiado[177].

Al limitar las medidas de protección tecnológicas protegidas a las que están "diseñadas para impedir o inhibir la vulneración", la DAA cumple los tratados de la OMPI y coincide con el enfoque utilizado en los Estados Unidos de América y en la Unión Europea: el propósito de dichas medidas es mejorar la capacidad de los titulares de derechos para impedir los usos no autorizados de sus obras.

Sin embargo, de forma muy parecida a como hace la Directiva de Derechos de Autor, la utilización de la frase "mecanismo de control del copiado" sugiere que la DAA no considera fuera de la ley la elusión de medidas tecnológicas utilizadas por los titulares de derechos para impedir otros tipos de utilizaciones no autorizadas que caen dentro de sus derechos exclusivos (tales como la representación pública). La historia legislativa de la DAA presenta casos de tecnologías de control del copiado en serie como ejemplo de medida de "control del copiado". En el caso *Sony contra Stevens* descrito a continuación, el Tribunal Federal interpretó estas expresiones para hacer referencia a un mecanismo que restringe la copia de una obra.

La DAA define los dispositivos y servicios de elusión haciendo referencia a dos pruebas, a saber, el dispositivo tiene 1) solamente un "propósito o uso comercial limitado" de elusión, o 2) ningún propósito o uso distinto a la elusión[178]. La primera de las dos pruebas es similar a una de las pruebas utilizadas en la DMCA y en la Directiva de Derechos de Autor. La segunda prueba (la prueba de propósito o fin único) había sido considerada y rechazada en otras jurisdicciones (no en el caso de la Ley de Prevención de la Competencia Desleal de Japón), porque permitiría el tráfico de un dispositivo o servicio que tuviera alguna utilización legítima, quizá menor o marginal, pero que hubiera sido diseñado para la elusión. Sin embargo, la inclusión de la primera parece estar dirigida a paliar las preocupaciones de los titulares de derechos y de otros que consideran que sería muy sencillo eludir la prueba de propósito único. Una diferencia sustancial entre la DAA y los enfoques utilizados en los Estados Unidos de América y la Unión Europea es que, al amparo de la ley australiana, un dispositivo o servicio que tiene un propósito comercialmente significativo distinto a la elusión resultaría completamente legítimo.

En resumen, el enfoque australiano puede resumirse de la forma siguiente:

	Acto de elusión	**Herramientas de elusión**
Medida tecnológica de control de acceso	No prohibido	Prohibida (s 10(1); s 116A)
Medida tecnológica de control de derecho de autor	No prohibido	Prohibida (s 10(1); s 116A)

3.4.1.1(c) Limitaciones y excepciones

La DAA establece tres excepciones básicas para la prohibición del tráfico de dispositivos o servicios de elusión.

177 s 10(1) (definición de "medida de protección tecnológica").
178 s 10(1) (definición de "dispositivo de elusión" y "servicio de elusión").

Utilización de un propósito permitido: el suministro de un dispositivo o servicio de elusión a una "persona cualificada" para un "propósito permitido", no estará prohibido si la persona cualificada entrega al suministrador una declaración firmada. Estos "propósitos permitidos" se establecen haciendo referencia a las excepciones a las vulneraciones del derecho de autor establecidas en la Ley de Derecho de Autor. Un "propósito permitido" es aquel que se corresponde con al menos una de las excepciones legales a la vulneración del derecho de autor[179]. Están incluidas:

– la reproducción de programas informáticos con fines de interoperabilidad, para corregir errores y para pruebas de seguridad;

– la copia legítima realizada por bibliotecas, archivos, instituciones educativas y de otra naturaleza, incluidas las instituciones para la ayuda a personas con algún tipo de incapacidad intelectual; y,

– una utilización legítima de material con derecho de autor para servicios del Estado o de la Commonwealth.

Es importante señalar que un "propósito permitido" no incluye cualquier utilización que signifique una "manipulación lícita" ("*fair dealing")* (es decir, se autorizan determinados actos de reproducción sin retribución), como por ejemplo, la copia privada o los "usos lícitos"(*fair uses*). Dada la potencial amplitud de dicha excepción y la incapacidad de controlar que los dispositivos de elusión sólo se suministren legítimamente a personas que realizan una "manipulación lícita", habría sido difícil limitar el alcance e impacto de dicha excepción únicamente a personas "cualificadas" de forma demostrable y que hubieran remitido declaraciones a tal efecto.

Una "persona cualificada" es aquella autorizada a utilizar material con uno de los propósitos incluidos en las excepciones antes mencionadas[180]. Finalmente, la persona cualificada debe entregar una declaración firmada confirmando que el dispositivo o servicio será utilizado solamente para el propósito permitido y que el material con derechos de autor sólo estará disponible en una forma protegida por una medida tecnológica[181]. Para evitar que los piratas y cualquier otro usuario malintencionado utilice este mecanismo para acceder a dispositivos destinados a eludir medidas tecnológica, la DAA considera delito penal que una persona haga, a sabiendas o de forma irresponsable, una declaración falsa o engañosa[182].

Por tanto, la fortaleza del enfoque australiano puede depender en gran medida de la integridad del proceso de declaración. Por ejemplo, se ha señalado que si una declaración no es falsa o engañosa en el momento en que se hizo, pero el dispositivo o servicio se utiliza posteriormente con un propósito distinto del que está "permitido", no se habría incurrido en ningún delito. En tales casos, los suministradores no pueden considerarse responsables porque han suministrado el dispositivo o servicio de elusión después de haber recibido una declaración válida. Tampoco los usuarios de dichos dispositivos pueden considerarse responsables debido a que los actos de elusión no están expresamente prohibidos por la DAA:

---

179 s 116(A)(7).
180 s 116(A)(8).
181 s 116(A)(3)(b).
182 ss 203G(1), (2).

Fabricación o importación para un propósito permitido: una disposición similar se aplica a la fabricación o importación de un dispositivo de elusión. Para poder estar incluido en esta excepción, debe demostrarse que el dispositivo se fabricó o importó para un "propósito permitido" (tal como se ha analizado anteriormente) y que el material con derechos de autor no está disponible sin la protección de una medida tecnológica[183].

Además, es posible fabricar e importar un dispositivo si éste permite suministrar a una persona un dispositivo o servicio de elusión pero sólo si ello se hace para un "propósito permitido"[184].

Observancia de la ley o seguridad nacional: cualquier acto realizado legítimamente para el cumplimiento de la ley, o para la seguridad, se considera incluido en una excepción de carácter general[185].

3.4.1.1(d) Información para la gestión de derechos electrónicos

La DAA también aplica las disposiciones para la gestión de derechos de los tratados de la OMPI. Prohíbe la supresión o alteración no autorizada, a sabiendas, de información para la gestión de derechos electrónicos a fin de inducir, permitir, facilitar u ocultar una vulneración[186]. Además, prohíbe la distribución, importación o comunicación al público, a sabiendas, de una copia o de una obra con derecho de autor cuando la información para la gestión de derechos electrónicos haya sido eliminada y la persona sepa, o sea razonable pensar que sabe, que al hacerlo está ayudando a que se cometa una vulneración[187]. Para ambos tipos de violaciones, las disposiciones legales suponen que los acusados tienen pleno conocimientos de sus actos: sobre ellos recae la carga de la prueba de que no eran conscientes de que alteraban o suprimían la información y de que desconocían que el tráfico que ejercían de copias alteradas contribuía a colaborar con el acto de vulneración.

3.4.1.1(e) Vías de recurso

Las vías de recurso que existen en caso de incumplimiento de las disposiciones civiles incluyen medidas cautelares y reclamaciones por daños y perjuicios[188]. También pueden imponerse castigos ejemplares en el caso de incumplimiento flagrante de la ley[189]. Los titulares de derechos pueden asimismo interponer una demanda por apropiación indebida o por la utilización de dispositivos de elusión para realizar copias fraudulentas[190]. Los castigos por delitos penales incluyen multas y penas de prisión (de hasta cinco años)[191].

---

183 s 116(A)(4)(a).
184 s 116(A)(4)(b).
185 s 116(A)(2).
186 s 116B.
187 s 116C.
188 s 116(D)(1).
189 s 116(D)(2).
190 s 116.
191 s 132(6)(A).

3.4.1.2 Otras leyes

Existen otras disposiciones en el marco jurídico australiano que prohíben el acceso no autorizado a computadoras y a contenidos encriptados. En particular, los servicios de radiodifusión encriptados están protegidos al amparo de la parte VAA de la Ley de Derecho de Autor (*Copyright Act*) de 1968, y por la propia DAA. La DAA fue redactada en parte tomando como referencia la Directiva de Acceso Condicional pero tiene un alcance más reducido y sólo se aplica a "radiodifusión codificada" (encriptada) tal como se define en dicha ley.

La parte VAA prohíbe la fabricación, diversas formas de tráfico (incluido hacer que la información esté disponible en línea) y el uso comercial de "dispositivos de decodificación de radiodifusión"[192]. Dicho dispositivo se define como un dispositivo "(incluido un programa informático) diseñado o adaptado para permitir que una persona acceda a una emisión de radiodifusión codificada sin la autorización del radiodifusor para la elusión o para facilitar la elusión de los medios técnicos o configuraciones empleadas para proteger el acceso de forma inteligible al producto radiodifundido"[193]. La "radiodifusión codificada" incluye 1) las emisiones de radiodifusión de televisión o radio disponibles únicamente para personas autorizadas o que hayan pagado un canon, y 2) la radiodifusión de televisión distribuida mediante servicios de radiodifusión y cuyo acceso de forma inteligible está protegido mediante medidas técnicas[194]. El vídeo y el audio bajo demanda, el teletexto y los servicios de emisión de datos en tiempo real en Internet (*streaming*) no se consideran incluidos en la definición de servicios de radiodifusión y por lo tanto la parte VAA no los protege contra el acceso no autorizado[195].

Cuando los radiodifusores realicen emisiones codificadas pueden denunciar la utilización comercial no autorizada de dispositivos de decodificación de radiodifusión por parte de quienes lo hagan para acceder a la información sin autorización, a sabiendas (o cuando razonablemente debían conocer) de que el acceso no estaba autorizado[196]. Los radiodifusores pueden conseguir que se establezcan medidas cautelares y una compensación por daños y perjuicios[197]. La distribución comercial de un dispositivo de decodificación de radiodifusión también puede constituir un delito penal[198].

Existen dos elementos que conviene destacar en el régimen jurídico australiano. En primer lugar, la Ley de Derecho de Autor otorga al radiodifusor, no al titular de derechos de autor, el derecho de demandar por la vía civil. En segundo lugar, no está prohibida la posesión privada o la utilización no comercial y no autorizada de dispositivos de decodificación para la radiodifusión.

---

192 s 135AN(1)(b).

193 s 135AL (definición de "dispositivo de decodificación de radiodifusión").

194 s 135AL (definiciones de "difusión codificada" (a) y (b)).

195 *Broadcasting Services Act* 1992 (Cth) s 6 (definición de "servicio de radiodifusión"); definición al amparo del párrafo (c) de "servicio de radiodifusión" (No. 1 de 2000), Notificado en *Gaz GN38* del 27 de septiembre de 2000 (el *streaming* de programas de televisión o de radio utilizando Internet está excluido de la definición de "servicio de radiodifusión").

196 *Id*. s 135ANA(1).

197 *Id*. s 135ANA(4).

198 *Id*. s 135AS(1).

3.4.2 Jurisprudencia

Autodesk, Inc. contra Dyson:[199] antes de la aprobación de la DAA, el Tribunal Supremo de Australia aplicó los principios hasta entonces existentes en la Ley de Derecho de Autor australiana para prohibir un dispositivo que se utilizaba para eludir una medida tecnológica destinada a proteger un programa informático. En este acaso Autodesk era el propietario de un programa de diseño asistido por computadora con derechos de autor; los usuarios podían conseguir el acceso autorizado solamente a través de un dispositivo físico, un "dispositivo conector antipiratería" ("*dongle*") adquirido junto con el programa y que se conectaba a la computadora para que se ejecutara el programa. Una parte separada y sustancial del programa requería que el propio dispositivo conector antipiratería se autenticara; dicho módulo comparaba las respuestas recibidas con una "tabla de búsqueda". Solamente si se recibía la respuesta correcta permitía la ejecución del programa completo

El acusado fabricó un dispositivo de elusión por ingeniería inversa del dispositivo conector antipiratería. El Tribunal Supremo sostuvo que la fabricación del dispositivo de elusión infringía el derecho del autor del programa de Autodesk debido a que para la reproducción de la "tabla de búsqueda" en el dispositivo conector antipiratería, era necesario copiar una parte sustancial del programa. En consecuencia, se dictaminó la responsabilidad del acusado por la fabricación de un dispositivo de elusión por la violación que suponía del derecho de autor de Autodesk.

Kabushiki Kaisha Sony Computer Entertainment contra Stevens:[200] en una interpretación y aplicación de la Sección 116A de la DAA, el Tribunal Federal de Australia admitió en julio de 2003 la apelación de Sony Computer Entertainment en relación con la decisión de un tribunal de primera instancia contra un demandado de haber vendido e instalado chips de modificación para la elusión de la codificación utilizada en los juegos PlayStation 2 (así como por falsificar copias de dichos juegos). Las medidas de protección de Sony incluían una memoria ROM de arranque situada en la tarjeta de sus consolas diseñada para leer y verificar los códigos de almacenados en la pista de arranque de los discos y los códigos de región, para garantizar que solamente los discos codificados para Australia pudieran funcionar en consolas vendidas en dicho país. La Comisión Australiana del Consumidor y la Competencia (*Australian Competition and Consumer Commission*) se personó como *amicus curiae* en los procedimientos previos al juicio de primera instancia y en defensa del acusado sobre la base de que la codificación regional supone un perjuicio para el consumidor y limita su capacidad de elección.

El juez de primera instancia analizó cuidadosamente la posición de Australia en relación con los tratados de la OMPI y los diversos texto borradores de la DAA, así como la Directiva de Derechos de Autor, con el fin de entender cabalmente el término "medida de protección tecnológica" tal como se define en la DAA. Determinó que las medidas de Sony no eran "medidas de protección tecnológica" en el contexto de la Sección 116(A), pues aunque eran una medida destinada a desalentar o impedir el acceso a la obra, no lo hacían mediante un proceso o código de acceso como el descrito en la Sección 10(1) de la Ley de Derecho de Autor de 1968. El magistrado Lindgren analizó ampliamente en la apelación tanto el texto como la historia legislativa de la DAA.

---

199 173 CLR 330 (1992).

200 [2003] FCAFC 157.

Al admitir la apelación, el Tribunal Federal adoptó una posición más amplia en relación con la definición de "medida de protección tecnológica" y sostuvo que la definición incluía dispositivos que pretendían conseguir, impedir o desalentar la vulneración y no, como había sostenido el juez de primera instancia, impedir o inhibir en la práctica actos que pudieran constituir una vulneración. En este sentido, el Tribunal interpretó la Sección 116A para aplicarla no sólo a la reproducción no autorizada sino también a la venta de artículos, cuya fabricación constituye una vulneración del derecho de autor. En la medida en que las medidas de protección de Sony hacían que las copias de los juegos de computadora resultaran inutilizables, el Tribunal señaló que impedían la vulneración en el sentido de hacer impracticable o imposible la venta de copias. El juez de primera instancia no consideró necesario dictaminar si los chips de modificación eran en sí mismos dispositivos de elusión. Sin embargo, señaló su opinión de que a la vista de la limitada utilización comercial de los chips para cualquier otro fin distinto a la elusión, si los códigos de acceso se hubieran considerado "medidas de protección tecnológica", los chips habrían sido dispositivos de elusión ilícitos.

La decisión conseguida en apelación es consistente con la decisión del caso *Owen* analizado en 3.3.3, en el que se concluyó que un chip de modificación similar era una violación ilegítima de la tecnología de protección de copiado de la PlayStation 2 de Sony de conformidad con la Ley de Derecho de Autor, Diseños y Patentes (*Copyright, Designs and Patent Act*) del Reino Unido.

3.5 Japón

Las disposiciones contra la elusión de los tratados de la OMPI japonesas se han aplicado en las modificaciones hechas en 1999 a la Ley de Derecho de Autor (*Copyright Law)* y a la Ley contra la Competencia Desleal (*Unfair Competition Prevention Law*). Las modificaciones a la Ley de Derecho de Autor tratan de la elusión de la protección técnica contra la vulneración del derecho del autor. Las modificaciones a la Ley contra la Competencia Desleal prohíben la elusión de las medidas tecnológicas de control del copiado y de control de acceso, teniendo en cuenta que los análisis realizados en Japón en relación con los enfoques jurídicos para la protección de medidas tecnológicas son anteriores a la Conferencia Diplomática de la OMPI, y que el Grupo de Trabajo del Subcomité Multimedia del Consejo de Derechos de Autor ha publicado sendos informes preliminares en febrero de 1995 y en febrero de 1997. Un grupo de trabajo del Subcomité realizó un proceso de consulta pública y estudió los desarrollos realizados en los Estados Unidos de América y en la Unión Europea. En diciembre de 1998 publicó su informe sobre medidas tecnológicas y gestión de derechos[201].

[201] Los informes preliminares de 1995 y 1997 y el Informe Final de diciembre de 1998 del Subcomité se citan en Koshida, nota 203.

3.5.1 Marco jurídico

3.5.1.1 Disposiciones contra la elusión

3.5.1.1(a) Ley de Derecho de Autor

La Ley No. 77 de 1999 modificó la Ley de Derecho de Autor para prohibir diversos tipos de tráfico de herramientas de elusión así como la oferta de servicios de elusión al público. No prohíbe específicamente el acto de elusión.

La Ley de Derecho de Autor define "medidas de protección tecnológica" como "medidas para impedir o disuadir dichos actos como constitutivos de vulneración de derechos morales o derechos de autor… o derechos conexos"[202]. Tal como se hizo en Australia, las "medidas" se definen en relación con sus objetivos.

La Ley de Derecho de Autor no define "impedir" aunque en un comentario que acompaña a las modificaciones de 1999 a la Ley de Derecho de Autor se señala que "impedir" significa detener[203]. En la Ley de Derecho de Autor "disuadir" se define como causar "una obstrucción considerable al resultado de dichos actos". Tal como ocurre en Australia, para "impedir" y "disuadir" son necesarios medios físicos o técnicos (más que simplemente desalentar o tener un efecto disuasorio). El comentario señala que una medida debe utilizar medios electromagnéticos para llevar a cabo su labor de impedir o disuadir[204].

Las disposiciones penales de la Ley de Derecho de Autor prohíben los programas y dispositivos de elusión. Un programa o dispositivo de elusión se define como aquel que tiene como "función principal" la elusión de una protección tecnológica[205]. La Ley de Derecho de Autor no define "función principal". Sin embargo, el comentario que la acompaña establece que sólo están prohibidos los dispositivos que tengan una "función que en la práctica esté significativamente limitada para lo que no sea la elusión"[206]. En este sentido, la ley japonesa es consistente con otros enfoques que dejan fuera de la ley a los dispositivos de elusión.

Aunque no está prohibido el acto de elusión, la Ley de Derecho de Autor establece que pueda darse la circunstancia de que una persona no pueda eludir una medida de protección tecnológica para reproducir una obra para fines no comerciales privados[207]. En general, la Ley de Derecho de Autor permite dichas reproducciones. Sin embargo, cuando la reproducción la hace una persona que sabe que dicho acto es posible mediante la elusión o que la medida ya no impide la copia, la excepción por copia privada deja de ser aplicable. No obstante, dicha persona no está sujeta a las sanciones penales previstas en la Ley de Derecho de Autor.

---

202 Artículo 2(xx), Ley de Derecho de Autor (*Copyright Law*) de Japón.

203 T. Koshida, *On the Law to Partially Amend the Copyright Law (Part 1): Technological advances and new steps in copyright protection* (1999), disponible en *http://www.cric.or.jp/cric_e/cuj/cuj.html*. ["Koshida"].

204 *Id*.

205 Artículo 120bis, Ley de Derecho de Autor de Japón.

206 Koshida, nota 203.

207 Artículo 30(1), Ley de Derecho de Autor de Japón.

Esta disposición define la "elusión" como lo que permite que una persona "cometa actos que se tratan de impedir con medidas de protección tecnológicas" (es decir, existe impedimento), o que inhabilitan las "obstrucciones" a los actos "que se tratan de disuadir mediante dichas medidas" (existe disuasión)[208]. Ello también incluye la eliminación de la información para la gestión de derechos. No se considera elusión la supresión o alteración de medidas o de información que son esenciales para la conversión o compresión.

3.5.1.1(b) Ley contra la Competencia Desleal

La Ley contra la Competencia Desleal (*Unfair Competition Prevention Law*) al igual que la Ley de Derecho de Autor, sólo prohíbe el tráfico de dispositivos y no el acto de elusión en sí mismo. La Ley contra la Competencia Desleal protege las "medidas de restricción técnica". Éstas se definen como aquellas que incluyen "los medios para restringir la reproducción de imágenes y de material sonoro, la ejecución de programas o la grabación mediante un método electromagnético, es decir, un método de grabación y transmisión de señales al que los dispositivos de reproducción pueden responder específicamente... o un método de grabación y transmisión en medios de grabación mediante la conversión de imágenes, material de audio o programas ..."[209].

La definición contempla el control de acceso y el control del copiado en la medida en que estas medidas restringen la "grabación". Al igual que la Directiva de Derechos de Autor y la DAA, la referencia a "grabación" sugiere que los medios técnicos que restringen la utilización no autorizada de derechos de autor distintos al derecho de reproducción pueden no estar amparados por la Ley contra la Competencia Desleal. Sin embargo, tal como se ha señalado, la Ley de Derecho de Autor contempla medidas tecnológicas de protección que pueden utilizarse para proteger otros derechos de autor.

El Artículo 2(1)(x) de la Ley contra la Competencia Desleal establece que es un acto de "competencia desleal" el hecho de "transportar, entregar [o] exhibir... equipos que solamente tengan la función de impedir la aplicación de las medidas de restricción técnicas y hacer posible la visualización y escucha de imágenes y material sonoro [etc.]... o grabar imágenes [etc.]... que están restringidas por medios técnicos de restricción utilizados comercialmente", e incluye dispositivos de incorporan tales mecanismos[210]. Asimismo, está prohibida la distribución en línea de dichos programas. Los comentarios de la Oficina de Patentes de Japón señalaban que este artículo abarca actos que eluden la tecnología de "restricción de copia", mientras que el Artículo 2(1)(xi) trata de las tecnologías de control de acceso[211]. El Sistema de Gestión de Copia en Serie se identifica como un ejemplo del primero, mientras que el CSS se describe como una tecnología de control de acceso[212]. Los chips de

---

208 Artículo 30(1)(ii).

209 Artículo 2(5), Ley contra la Competencia Desleal (*Unfair Competition Prevention Law*). Véase Japan Patent Office, Asia-Pacific Industrial Property Center & Japan Institute of Innovation and Invention, *Outline and Practices of Japanese Unfair Competition Law* 22 (1999) (donde traduce y comenta la ley), disponible en *http://www.apic.jiii.or.jp/facility/text/2-10.pdf* ["JPO/APIC Outline"].

210 Artículo 2(1)(x), Ley contra la Competencia Desleal.

211 JPO/APIC Outline, nota 209, en 21.

212 *Id*. at 45.

modificación utilizados para la reproducción no autorizada de videojuegos se identifican como dispositivos de elusión[213].

Tal como se ha señalado, el Artículo 2(1)(xi) se aplica a la protección de tecnologías de control de acceso frente a los dispositivos de elusión. En resumen, prohíbe el tráfico (incluyendo la distribución en línea) de dispositivos (incluyendo productos que se incorporan en otros dispositivos) que eluden medios técnicos utilizados comercialmente para impedir que las personas (distintas a las especificadas) vean y escuchen obras visuales y sonoras, en la medida en que dichos productos sólo tengan la función de permitir que las personas reproduzcan dichas obras, ejecuten programas o graben obras o programas con imágenes o sonidos que están restringidas[214].

El texto de dichas disposiciones así como los comentarios a las mismas, destacan que solamente están prohibidos los dispositivos que tengan la función exclusiva de eludir medidas técnicas. Ninguna de las restantes jurisdicciones que se analizan en este documento limitan el ámbito de la prohibición a productos de "propósito exclusivo".

La ley japonesa aplica los tratados de la OMPI de la forma siguiente:

	Acto de elusión	**Herramientas de elusión**
Medida tecnológica de control de acceso	No prohibido	Prohibida (Art. 2(1)(xi) de la Ley contra la Competencia Desleal)
Medida tecnológica de control de derechos de autor	No prohibido	Prohibida (Art. 120bis de la Ley de Derecho de Autor; Art. 2(1)(x) de la Ley contra la Competencia Desleal)

3.5.1.1(c) Limitaciones y excepciones

La Ley de Derecho de Autor no contiene una disposición de "no-obligatoriedad". Sin embargo, los comentarios que la acompañan señalan que no se considera elusión la utilización de la "denominada máquina sin reacción, es decir, aquella que no responda a la señal utilizada por la medida tecnológica"[215].

La Ley contra la Competencia Desleal proporciona una excepción a la prohibición general de la ley, permitiendo que sea lícito distribuir dispositivos utilizados para probar o investigar sobre medidas de protección tecnológica[216]. El propósito de la excepción es permitir el desarrollo de medidas mejoradas.

---

213 *Id*. Véase también el documento (borrador) del Ministerio de Industria y Comercio Internacional (*Ministry of International Trade and Industry*), *Amendment to the Unfair Competition Prevention Law* (marzo de 1999) (en el que se describen chips de modificación que permiten la reproducción de software copiado como ejemplo de dispositivo que elude los medios de control de uso), disponible en *http://www.meti.go.jp/english/report/data/gCD1103e.html*.

214 Artículo 2(1)(xi), Ley contra la Competencia Desleal. Véase JPO/APIC Outline, nota 209, en 23-24.

215 Koshida, nota 203.

216 Artículo 11(1)(7), Ley contra la Competencia Desleal.

3.5.1.2 Vías de recurso

La Ley de Derecho de Autor sólo incluye vías de recurso penales para el tráfico de tecnologías de elusión: la multa no puede superar un millón de yenes, o la condena a prisión no puede ser mayor de un año. Los comentarios que la acompañan explican que no se ha introducido ninguna disposición que permita demandar civilmente debido a que cuando se introduce en el mercado el dispositivo de elusión no está claro cuáles son las obras que van a sufrir la elusión y en consecuencia, no es posible determinar en ese momento cuál será el titular de derechos de autor que tendrá el derecho a solicitar una medida cautelar debido a la inminente vulneración de su obra[217].

La Ley contra la Competencia Desleal señala que el tráfico de dispositivos y de programas de elusión se clasifica como "competencia desleal". Se pueden solicitar medidas cautelares.

3.5.1.3 Información para la gestión de derechos

La Ley de Derecho de Autor japonesa sigue los principios de los tratados de la OMPI y de otras legislaciones para definir la "información para la gestión de derechos". La Ley de Derecho de Autor define con precisión la información para la gestión de derechos como información relativa a derechos morales o derechos de autor que está grabada en la memoria de una computadora o que se transmite electrónicamente junto con las obras y se utiliza comercialmente en relación con la autorización de utilización de obras para la gestión del derecho de autor. La información para la gestión de derechos incluye información que especifica obra y titular, así como otros elementos que "en el futuro" puedan será especificados mediante una Orden Ministerial que hagan referencia a la forma y condiciones de explotación y que permite lo anterior "en comparación con otra información"[218]. La definición parece ser más limitada que la utilizada en otras jurisdicciones en el sentido de que, por ejemplo, no incluye los avisos del derecho de autor y otros títulos o advertencias incluidas en las obras.

La Ley de Derecho de Autor no establece como un derecho separado al margen del derecho de autor, la adición, supresión o alteración de la información para la gestión de derechos. En lugar de ello, se considera que dichos actos vulneran los derechos morales, los derechos de autor y los derechos conexos de autores y ejecutantes. Específicamente, la Ley de Derecho de Autor prohíbe la adición intencionada de información falsa, la supresión o alteración intencionada de información (salvo cuando hacerlo sea inevitable) y la distribución de copias de obras a sabiendas que se ha producido una adición, supresión o alteración ilícita de la información para la gestión de derechos.[219]. Sin embargo, a diferencia de otros países, para que una persona sea responsable no existe el requisito adicional de que haya proporcionado, suprimido o alterado información para la gestión de derechos, a sabiendas de que colaboraba en una vulneración. Asimismo, se considera que si la supresión forma parte de un proceso de conversión técnica o de compresión, no existe vulneración. Las sanciones penales por la vulneración de dichas disposiciones son las mismas que las arriba señaladas para la vulneración de las disposiciones contra la elusión.

---

217 Koshida, nota 203.
218 Artículo 2(xxi), Ley de Derecho de Autor.
219 Artículo 113(3), Ley de Derecho de Autor.

3.5.2 Otras leyes

En el Japón existen otras leyes que se ocupan de la protección legal de los sistemas DRM o de otras tecnologías de acceso condicional. Por ejemplo, la Ley de Radiodifusión prohíbe que las personas puedan recibir un servicio de radiodifusión de pago salvo que haya alcanzado un acuerdo con el radiodifusor[220].

4. PARTES INTERESADAS Y APLICACIONES DE LA GESTIÓN DE DERECHOS DIGITALES (DRM)

4.1 Introducción

La funcionalidad necesaria para la gestión de derechos digitales (DRM) ha sido explicada con detalle en este documento. Los usuarios de las tecnologías (los interesados) son aquellos que participan en la cadena de valor de derechos de propiedad intelectual, con un interés moral o financiero, en la creación, distribución y consumo de material protegido. Son dichas partes interesadas las que se beneficiarán de la DRM creando las condiciones adecuadas para la distribución y consumo de propiedad intelectual en el entorno digital. Ha habido muchos puntos de vista diferentes, algunos de ellos coincidentes, otros convergentes y otros que aún mantienen desacuerdos muy relevantes.

En esta sección se identifican las partes interesadas y su situación en la cadena de valor, describiéndose sus posiciones en relación con el desarrollo, despliegue y utilización de la DRM para distribuir, proteger y consumir contenidos protegidos.

4.1.1 Titulares de derechos

Según el Convenio de Berna, un derecho de autor comienza a existir con la creación de una obra. Los titulares del derecho de autor pueden ser creadores individuales (personas naturales), corporaciones (personas jurídicas), o bien, la propiedad puede ser conjunta. Además, puede otorgarse un derecho exclusivamente a una tercera parte que, a los efectos de sección, se considerará como titular de los derechos.

Los titulares de derechos tienen la expectativa legítima de poder autorizar, normalmente a cambio de un pago, la explotación de la propiedad intelectual que les pertenece. En el dominio analógico (edición física, etc.) se han acostumbrado a una serie de métodos por los cuales reciben una compensación por uso. Dichos métodos incluyen el pago directo por los usuarios, los pagos a través de acuerdos colectivos gestionados por sociedades de gestión colectiva y los pagos a través de intermediarios que revenden a los consumidores.

La introducción de las DRM puede crear nuevas oportunidades para que los titulares de derechos gestionen éstos. Por ejemplo, un creador individual puede contratar con un proveedor de servicios DRM (como Overdrive o DWS) y ofrecer sus obras directamente al público. Los propietarios o titulares de derechos corporativos, como empresas discográficas y editores también pueden llegar a dicho tipo de acuerdos, acortando la cadena de suministro al eliminar intermediarios mayoristas y minoristas. Hasta ahora, sólo se ha comenzado a

---

220 Artículo 52-5, Ley de Radiodifusión.

apreciar el efecto de dichos cambios en la cadena de valor, y son necesarios estudios adicionales y negociaciones entre las partes.

4.1.2 Sociedades de gestión colectiva

Las sociedades de gestión colectiva (CMS, *collective management societies*) que liquidan y administran los derechos de grupos de autores, han jugado tradicionalmente un papel central en la concesión de licencias y en la distribución y recaudación de regalías (*royalties*) de contenidos con derechos de autor. Dada su amplia experiencia en la gestión de derechos, tienen un interés fundamental en la utilización de tecnologías digitales para la gestión de derechos. La gestión de derechos es algo cada vez más complejo, debido tanto a la naturaleza global de la explotación y concesión de licencias de obras, como por la enorme cantidad de medios y formatos en que pueden concederse licencias de derechos. Por tanto, no es sorprendente que las CMS consideren que las DRM son elementos fundamentales para desarrollar sus funciones. De hecho, algunas CMS ya están utilizando tecnologías digitales para liquidar ciertos derechos de una forma rápida y eficaz.

Al mismo tiempo, algunas partes interesadas pueden considerar que, en un contexto digital, el papel de las CMS debería estar más limitado, particularmente cuando los titulares de derechos puedan conceder directamente licencias a usuarios. Dichas partes pueden asimismo considerar que la naturaleza colectiva de las actividades de las CMS impide realmente, o de forma efectiva, que los titulares de derechos ejerzan éstos individualmente. Las CMS rechazan estos puntos de vista haciendo notar que los titulares de derechos pueden, al menos en teoría, elegir siempre entre una gestión de derechos individual u otra colectiva. Las CMS también consideran que su crítica posición en la distribución digital de contenidos exige que sus necesidades y funciones sean plenamente entendidas y asimiladas en el diseño y despliegue de cualquier sistema DRM.

Las CMS, quizás preocupadas por el hecho de que la utilización de las DRM puede hacer que se prescinda de ellas, han señalado que estos sistemas no pueden reemplazar las funciones prácticas que realizan. Por lo tanto, incluso en el caso de que las DRM alcanzaran un papel muy relevante, las CMS consideran que seguirán realizando una labor de auditoria de pagos por regalías, así como las actividades propias de una organización cuyos miembros requieren sus servicios para actividades tales como la negociación de descuentos colectivos frente a otros titulares de derechos y usuarios, y la participación directa en el desarrollo de normas y en debates públicos de naturaleza política sobre los derechos de autor y su observancia.

Las CMS han señalado que están participando activamente en el desarrollo de componentes de sistemas DRM, incluida la colaboración en la creación de normas para identificadores (por ejemplo, el ISWC) y la participación en foros internacionales para promover normas comunes (por ejemplo, MPEG 21).

4.1.3 Intermediarios

Cuando se analizan los "intermediarios" que existen en el mundo físico, se tiende a pensar en ellos en términos de cadena de suministro, particularmente en mayoristas y minoristas (las organizaciones que conforman el canal de distribución entre las "compañías de contenido" y sus clientes finales). Sin embargo, un análisis detallado de los papeles que se deben asumir en la cadena de valor digital, conduce inexorablemente a reconocer que cualquier organización situada entre el creador y el consumidor debe considerarse un "intermediario" en la cadena. Ello incluye a organizaciones comerciales tales como los sellos discográficos y los editores asociados a éstos; también incluye organizaciones de "interés público" tales como bibliotecas que tradicionalmente han jugado papeles muy importantes de agregación y acceso en la cadena de la información.

La distribución tradicional de papeles en la cadena de suministro física parece tener una aplicación limitada a largo plazo en el entorno de red. Las tareas que deben realizarse en la cadena pueden ser desagregadas arbitrariamente y posiblemente reagrupadas en una forma completamente diferente.

Sin embargo, la medida en que puede reconfigurarse la cadena depende considerablemente de la efectividad de la comunicación. La red proporciona la infraestructura física para dicha comunicación y (a través del "efecto red") permite la implementación simultánea de una infraestructura normalizada que facilite una comunicación eficiente entre máquinas.

Para que la reconfiguración de la cadena de valor sea verdaderamente efectiva, es esencial que esta infraestructura basada en normas sea tan abierta y no prescriptiva como sea posible. Por ejemplo, es importante que no existan condicionantes *a priori* sobre la agregación de funciones en la cadena de valor. Ello puede incomodar notablemente a las organizaciones tradicionalmente establecidas, que tienen una tendencia natural a mantener prácticas y modelo de negocios existentes (aunque éstas puedan ser a menudo inapropiadas e irrelevantes en un entorno de red).

Por lo tanto, los intereses de los intermediarios pueden ser a menudo conflictivos entre sí (y posiblemente también con los intereses de los consumidores). Puede resultar muy difícil para dichas organizaciones separar sus intereses a corto y a largo plazo. Sin embargo, es por un interés común a largo plazo que los sistemas e infraestructuras DRM deben diseñarse para proporcionar el mayor grado de flexibilidad en términos de apoyo a modelos de negocio y a la cadena de suministro digital, más que simplemente imitar los modelos físicos existentes.

4.1.4 Intermediarios de telecomunicaciones

Los proveedores de red no se han visto tradicionalmente implicados en la cadena de valor de la propiedad intelectual. En su papel de "operadores de redes", han sido proveedores de cables y sistemas sobre los que la información (llamadas telefónicas o datos) se ha transmitido desde un lugar a otro. Sin embargo, con el advenimiento de la economía de la información digital, los proveedores de redes han manifestado un gran interés en entrar en la cadena de valor como proveedores de servicios de Internet a fin de conseguir ingresos por el suministro de servicios de contenidos a sus clientes.

Los proveedores de red están cada vez más preocupados sobre la potencial responsabilidad por la eventual vulneración de derechos de los contenidos que distribuyen. Tradicionalmente, los operadores de telecomunicaciones no han sido responsables por la transmisión de contenidos que supongan una violación de derechos. Sin embargo, en su papel de proveedores de servicio Internet (ISP, *Internet Service Providers*), los operadores y los nuevos entrantes en este mercado están sujetos a reclamaciones como responsables directos o indirectos cuando transmiten, y almacenan de forma temporal (caché) o permanente contenidos que supongan una violación de derechos. Tanto los Estados Unidos de América a través de la DMCA, como la Unión Europea en su Directiva sobre el Comercio Electrónico, han reconocido que un ISP no comete un acto doloso cuando participa sin conocimiento de causa en este tipo de actividades. Por este motivo, los regímenes jurídicos en los Estados Unidos de América y en la Unión Europea limitan la responsabilidad potencial de los ISP al caso en que éstos tengan conocimiento de contenidos que supongan una violación de derechos, en cuyo caso han de suprimirlos o inhabilitar el acceso a los mismos (véanse 3.2.1.2 y 3.3.1.2.c)).

Los ISP están muy interesados en el despliegue de herramientas para la gestión de derechos digitales que les proporcionen una cierta protección contra los peligros jurídicos existentes. Por otro lado, no desean poner en peligro las relaciones con sus clientes estableciendo barreras notorias (si es que la DRM se percibe como una barrera) al disfrute de los contenidos que distribuye.

4.1.5 Suministradores de tecnología – Software

El sector de la industria del *software* que desarrolla tecnologías para la gestión de derechos digitales ha pasado por diversas fases. Para entender cómo se relacionan los suministradores de *software* para DRM con el resto de actores de la cadena de valor, es necesario entender la reciente historia del mercado del *software*. Inicialmente, el sector se componía casi exclusivamente de pequeñas empresas que iniciaron su actividad en los Estados Unidos de América. Aunque algunas de ellas iniciaron su actividades de investigación y desarrollo durante la segunda mitad de los años ochenta, la mayor parte se crearon en la primera mitad de los años 90. Conforme creció el interés por la tecnología DRM, asimismo creció la aparente fortuna de muchas de las compañías. Aunque las empresas no tuvieron éxito en la captación de un gran número de clientes, muchas de ellas registraron patentes en esta fase, de forma que el creciente portafolio de patentes les permitió atraer cantidades importantes de capital riesgo, dando lugar a un importante crecimiento del sector, especialmente durante la época de crecimiento explosivo de los últimos años 90. Ello hizo que muchas compañías ampliaran sus modelos de negocio para proporcionar servicios adicionales al *software*. Las expectativas en aquél momento eran que las compañías generarían beneficios por los ingresos que producirían las transacciones en las que se utilizaran sus servicios y su *software*. Aunque no era un panorama muy atractivos para los titulares de derechos, en aquél momento parecía que la situación podía ser controlada por dichas compañías.

Sin embargo, con el inicio del nuevo milenio, la situación del mercado cambió sustancialmente. El colapso de la confianza en el sector del *software* en su conjunto, hizo que muchas compañías pequeñas quedaran en un estado de insolvencia, e incluso que algunas perdieran todos sus clientes. Las que resistieron, intentaron sobrevivir al colapso mediante fusiones o siendo adquiridas, junto con todo su portafolio de patentes, por otras empresas de mayor tamaño.

Ello ha dado lugar a un sector del *software* DRM que está ampliamente dominado por unos pocos actores de talla mundial, tales como Microsoft, IBM y Adobe. Estas empresas son las que parecen estar dictando los pasos del software DRM, quedando las pequeñas empresas relegadas a proporcionar elementos auxiliares a las tecnologías base propietarias que desarrollan aquéllas. Sin embargo, y de forma muy importante, los titulares de derechos han comenzado recientemente a mostrarse muy activos a la hora de establecer sus requisitos para DRM, participando en iniciativas de normalización. Este debate en torno al grado de normalización de la tecnología DRM para aplicaciones en línea o fuera de línea, tendrá un efecto sustancial en la interoperabilidad, determinando el futuro de las compañías de *software* y sus ingresos por la utilización de DRM. También debe señalarse que el resultado del debate sobre normalización determinará en gran medida las relaciones entre los titulares de derechos y las empresas tecnológicas. Estos asuntos se tratan con más detalle en 2.5.5 (normalización) y 4.2.7 (interoperabilidad).

4.1.6 Suministradores de tecnología – Hardware

Algunos de los desarrolladores más importantes de tecnologías de protección de contenidos han sido empresas de hardware, tanto compañías de electrónica de consumo como de tecnologías de la información. Desde los años 80 (e incluso antes), la industria tecnológica se ha resistido a imponer limitaciones legales a los dispositivos de copia, tales como grabadores de videocintas y productos de grabación de audio.

Con la introducción de las tecnologías digitales, se alcanzaron acuerdos con los titulares de derechos. El principal incentivo para el acercamiento era la constancia de que los nuevos formatos digitales, tanto desde el punto de vista de los contenidos como de la tecnología, requerían la cooperación y el apoyo de todos los sectores afectados de la industria. Sin el apoyo de los titulares de derechos, los nuevos productos de procesamiento y grabación digital pueden nacer muertos. Dicho apoyo exige que las tecnologías de protección de contenidos se desarrollen e implementen en los productos digitales.

A finales de los años 80 y principios de los 90, las compañías tecnológicas propusieron esquemas de protección de contenidos bastante sencillos. Entre ellos estaba, tal como se ha señalado anteriormente, el sistema de gestión de copias en serie (SCMS, *Serial Copy Management System*), que limita la copia de audio digital. El sistema analógico de gestión de generación de copias (CGMS-A, *Copy Generation Management System-Analog*) se propuso para limitar la copia mediante dispositivos de grabación digital de contenidos analógicos marcados. Desde mediados de los años 90 hasta ahora, las principales compañías tecnológicas han desarrollado sistemas de protección más sofisticados de protección de contenidos y de carácter propietario, incluyendo los descritos en 3.2.1.

Por ejemplo, para proteger los contenidos audiovisuales sobre DVD, Matsushita Electric Industrial Co. y Toshiba desarrollaron el CSS que, tal como se ha señalado anteriormente, está siendo utilizado bajo licencia a través de la Asociación para el Control del copiado en DVD (DVD CCA, *DVD Copy Control Association, Inc*). Hitachi, Intel, Matsushita, Sony y Toshiba desarrollaron el Sistema de protección de contenidos transmitidos digitalmente (DTCP, *Digital Transmission Content Protection*). Intel ha sido el principal promotor del Sistema de protección de contenidos digitales de banda ancha (HDCP, High-*bandwidth Digital Content Protection*), cuya licencia se distribuye para proteger contenidos de video digital recibidos en monitores de PC y en otros dispositivos de visualización a través de los *buses* normalmente utilizados. Matsushita, Toshiba, Intel e IBM han desarrollado

varias tecnologías de protección de contenidos de Audio sobre DVD y tecnologías de grabación asociadas, incluyendo la Protección de contenidos para medios pregrabados (CPPM, *Content Protection for Prerecorded Media*) y la Protección de contenidos para medios grabables (CPRM, *Content Protection for Recordable Media*).

Las compañías de hardware también han estado al frente del desarrollo y promoción de las tecnologías de marcación por filigrana. Actualmente, la DVD CCA está considerando la aprobación de una tecnología para la marcación de videodiscos DVD, de entre dos que han estado siendo analizadas durante cierto tiempo. Una ha sido desarrollada por el "Grupo VWM," que incluye compañías tecnológicas de la talla de Hitachi, NEC, Philips, Pioneer y Sony, así como dos actores pequeños pero centrales en la protección de contenidos, Macrovision Corp. y Digimarc. Toshiba ha desarrollado otra técnica de marcación mediante filigrana.

El principal impulsor del desarrollo de estas tecnologías es el imperativo de negocio de utilizarlas para apoyar la proliferación de productos digitales, incluyendo los dispositivos de grabación y reproducción, computadoras personales y otros procesadores. Para entender cabalmente cada una de las tecnologías mencionadas, destinadas a ser complementarias entre sí en una arquitectura de hogar conectado, es fundamental que estén basadas en sistemas de protección de contenidos obligados por la propia licencia. A su vez, los términos y condiciones de dichas licencias son objeto de un proceso largo e intenso de colaboración, consulta y negociación con los titulares de derechos. Dado que están confiando sus valiosos contenidos a la protección que ofrecen estas tecnologías, los titulares de derechos insisten en que no se hagan cambios sustanciales a dichas tecnologías o a las condiciones de concesión de licencias asociadas sin que ellos tengan ciertos derechos de revisión o de aprobación.

4.1.7 Usuarios finales profesionales y comerciales

Los requisitos de los usuarios profesionales de contenidos (principalmente de información) en un contexto profesional o comercial, no son sustancialmente diferentes de los de un usuario individual en su vida privada. Sin embargo, puede ponerse el énfasis en puntos diferentes, entre los que cabe señalar tres aspectos que merecen especial atención.

En primer lugar, es previsible que el asunto de la *autoridad* y *autenticidad* ocupe una posición más central: ¿es este documento lo que dice ser que es?, ¿procede de una fuente confiable?. Estas cuestiones pueden ser particularmente apremiantes si existen aspectos relacionados con la responsabilidad o reputación profesional.

En segundo lugar, la cuestión de la *confidencialidad*, el "derecho a una lectura anónima," puede tener un significado completamente diferente. Un ejemplo sencillo es que un competidor pueda hacer un seguimiento de lo publicado sobre una investigación científica farmacéutica, debería poder extraer conclusiones suficientemente precisas sobre la dirección de la investigación y los posibles resultados.

En tercer lugar, existe el requisito del acceso a un contenido condicionado a la *pertenencia a una clase o colectivo* de individuos, por ejemplo, ser empleado de una corporación o miembro de una asociación. Hoy día, estos mecanismos tienden a ser relativamente toscos, en base a la ubicación física o la autenticación de una dirección IP. Se está avanzando en el sentido de reconocer la necesidad de una gestión mucho más sofisticada de la identidad digital; sin embargo, las implicaciones sobre la vida privada son de gran

alcance. Dado que una persona puede también ser miembro de un grupo con privilegios otorgados por la Ley de Derecho de Autor, identificar el contexto en el cual se hace la utilización del material con derechos de autor puede ser un asunto muy difícil de resolver en relación con la aplicabilidad de excepciones legales a los derechos exclusivos del titular de derechos. Por ejemplo, un individuo que ejerza como profesor en actividades educativas puede utilizar un material en virtud de "excepciones educativas" existentes en ciertas jurisdicciones, o en otro caso, dicho uso puede calificarse como un "uso lícito"; sin embargo, dichas excepciones pueden no ser aplicables con respecto al mismo material cuando el individuo lo utiliza para su uso privado.

A la hora de analizar la aplicación de la DRM, es esencial reconocer la existencia de estos retos, aunque actualmente su resolución parezca difícil de alcanzar.

4.1.8 Usuarios finales consumidores

Los consumidores tienen sus propias expectativas sobre cómo puede acceder a y utilizar los contenidos. Dichas expectativas se basan en prácticas asentadas durante mucho tiempo, con respecto al contenido que adquieren lícitamente y los contenidos que cada vez más pueden conseguir sin autorización, tal como ocurre en el intercambio de ficheros entre particulares (*peer-to-peer*).

Por un lado, los usuarios consideran que tienen el derecho de hacer copias del contenido adquirido legítimamente, con independencia de que su origen sea la radiodifusión abierta o un CD que hayan comprado. Asimismo, los consumidores se han acostumbrado a copiar contenidos de televisión con dispositivos de grabación, aunque el contenido se haya conseguido de un sistema de acceso condicional (televisión de pago) o de una sesión de pago por visión. Al menos en los Estados Unidos de América se ha hecho un esfuerzo para reflejar dichas expectativas y hábitos en las "reglas de codificación" que forman parte de los sistemas de protección de contenidos descritos en 3.2.1 y 4.1.6, e incluidas en la Ley de Derecho de Autor para el Milenio Digital[221] .

Por otro lado, los consumidores pueden reconocer sinceramente lo inapropiado de determinados tipos de comportamientos (la piratería comercial y la distribución masiva de contenidos con derechos de autor incluso en un contexto no comercial). Aunque a muchos consumidores les encanta no pagar por un contenido (de ahí la popularidad del intercambio de ficheros), la mayoría está dispuesta a pagar algo en circunstancias adecuadas por el producto adecuado.

Por lo tanto, no es sorprendente que ni los consumidores ni las organizaciones de consumidores reciban de buen grado las tecnologías utilizadas para restringir el comportamiento tradicional del consumidor. En muchas jurisdicciones, existen grupos con ideas claras que representan los intereses públicos o de los consumidores en relación con la tecnología digital, incluido el despliegue de los sistemas DRM. Por ejemplo, en los Estados Unidos de América, la Coalición de los Derechos de Grabación en el Hogar (*Home Recording Rights Coalition*) ha participado desde 1981 en asuntos relacionados con la grabación en el ámbito de los de consumidores y no comercial. Más recientemente, la Fundación para la Frontera Electrónica y el Conocimiento Público (*Electronic Frontier Foundation and Public*

---

[221] Véase la nota 56, que describe lo establecido en el Artículo 1201.k) de la DMCA.

Knowledge) ha participado, entre otros, en debates políticos públicos en el marco de las negociaciones entre las industrias sobre normas para la protección de contenidos y otros asuntos relacionados con la DRM, habiendo participado activamente en debates ante el Congreso y la Comisión Federal de Comunicaciones (FCC) sobre el papel del gobierno para obligar la observancia de acuerdos negociados por la industria. En Europa, la Organización de Consumidores Europeos ha representado los intereses de los usuarios en los asunto relacionados con la DRM e iniciativas sobre derechos de autor de la Unión Europea.

Además de examinar los efectos potenciales del despliegue de la DRM sobre los hábitos de los consumidores, se ha expresado la preocupación del impacto de las tecnologías DRM sobre la vida privada del consumidor, particularmente porque los esquemas de DRM pueden permitir que los titulares de derechos o los distribuidores recopilen y utilicen datos personales sobre los hábitos de compra de los consumidores y su utilización de material protegido con derechos de autor. Dichos aspectos que afectan a la privacidad se analizan en 5.2.1.

4.2 Puesta en marcha de la DRM

4.2.1 Introducción

Aunque este documento recoge los antecedentes jurídicos y tecnológicos sobre la utilización y funcionalidad de la tecnología DRM, los usuarios de la misma a lo largo de la cadena de valor están principalmente interesados en su despliegue. A este respecto, es importante señalar que éste se encuentra aún en una fase preliminar por motivos de índole jurídica, técnica y comercial. Por ejemplo, los diversos instrumentos jurídicos que protegerán el despliegue y utilización de medidas técnicas de protección no se han puesto en marcha a nivel mundial. En segundo lugar, lo modelos comerciales utilizados por los titulares de derechos para proteger sus contenidos, no van más allá de esquemas muy básicos. En tercer lugar, la tecnología necesaria para crear estos modelos, incluidas las normas en que se basará la tecnología, se encuentra aún en fase de desarrollo.

No obstante, pueden hacerse algunas observaciones relevantes sobre su implementación actual.

a) La mayoría de las implementaciones de DRM están actualmente limitadas a sectores de contenidos específicos (como las industrias editorial y musical). La DRM no se aplica aún a contenidos multimedia complejos, en los que se combina la música con lo audiovisual y el texto. Dicha separación vertical entre sectores refleja la situación de la distribución de contenidos analógicos, en donde es técnica y físicamente difícil combinar tipos de medios diferentes. Es previsible que conforme la DRM se haga más flexible, permitiendo la combinación de diversos tipos de contenidos, la separación vertical entre los diferentes sistemas de distribución de contenidos comenzará a diluirse hasta llegar a desaparecer.

b) Los modelos disponibles que permitan la distribución de contenidos son aún bastante simples. Los modelos de suscripción, pago por visión / audición y la compra directa son las modalidades dominantes. Es previsible que en el futuro, existirá una variedad de modelos de negocio, muchos de los cuales se basarán en la compara de productos híbridos; los modelos en los que existe relación directa entre individuos (*peer-to-peer*) de carácter comercial en los que se compense a los titulares de derechos seguirán siendo poco habituales. La mayoría de los modelos en los que existe una relación directa entre individuos o éstos trasiegan con contenidos no autorizados.

c) Los sistemas de pago son aún primitivos, realizándose la mayoría de los pagos con tarjeta de crédito.

4.2.2 Servicios DRM para audio

Durante los últimos dos años han surgido una serie de servicios de música en línea, liderados por las principales compañías discográficas y compañías de distribución de contenidos en línea, tales como RealNetworks y su servicio Rhapsody. Estos servicios de descarga legal de música han surgido como alternativa a los servicios ilegítimos en los que existe relación directa entre individuos (*peer-to-peer*). Es aún demasiado pronto para evaluar el éxito de los servicios legítimos de música en línea.

MusicNet fue fundada por BMG, Warner Music y EMI. El consorcio ha llegado a acuerdos con Sony y Universal. Por tanto, actualmente existen servicios de música en línea que proporcionan contenidos de las cinco marcas discográficas principales. Los usuarios acceden al contenido de MusicNet mediante distribuidores asociados tales como Rand AOL. El sistema permite que los usuarios se descarguen música o utilicen un servicio de emisión de datos en internet en tiempo real (*streaming*) de contenidos musicales con habilitación DRM. De conformidad con el tipo de suscripción elegido, los usuarios pueden incluso almacenar la música en sus discos duros y grabarla en CD. Un usuario paga aproximadamente 10 $ de los Estados Unidos de América para escuchar una cantidad ilimitada de canciones del catálogo en línea de MusicNet.

Apple lanzó iTunes en los Estados Unidos de América en la primavera de 2003. El servicio utiliza el dispositivo iPod de Apple como reproductor, y almacena canciones protegidas con DRM descargadas del servicio iTunes con una computadora. El servicio ha resultado ser extremadamente popular y Apple anunció en Junio de 2003 que había vendido más de cinco millones de canciones en su tienda iTunes Music Store.

Vivendi Universal y Sony han lanzado el servicio Pressplay. En principio, el modelo de negocio es similar al de MusicNet y todas las canciones distribuidas en la red utilizan DRM. Pressplay ha sido adquirido recientemente por Roxio, una compañía de *software* de copia de CD, que también compró los activos de Napster a finales de 2002.

Más recientemente, varias de las principales empresas de venta al por menor de los Estados Unidos de América, incluyendo a Best Buy, Tower Records, Virgin Entertainment Group, Wherehouse Music, Hastings Entertainment y Trans World Entertainment constituyeron una empresa de música en línea llamada Echo.

OD2 es un servicio de descarga de música europeo, cofundado por el músico e intérprete Peter Gabriel. OD2 proporciona servicios de distribución a sellos de primer nivel, tales como Sony y BMG.

4.2.3 Servicios DRM para productos audiovisuales

Los principales estudios cinematográficos han comenzado recientemente a proporcionar servicios de películas bajo demanda sobre la Internet pública. La aplicación de DRM es una parte esencial de su estrategia. Las iniciativas más exitosas se han producido hasta la fecha en relación con la industria de contenidos para adultos. En cuanto al mercado de consumo en general, en 2002 se lanzó un nuevo portal de servicios bajo demanda denominado MovieLink. MovieLink es una empresa participada por MGM Studios, Paramount Pictures, Sony Pictures Entertainment, Universal Studios y Warner Bros. Studios. El servicio, sólo disponible para residentes de los Estados Unidos de América, se lanzó como un proyecto piloto en noviembre de 2002 y permite acceder a unas 200 películas de los principales estudios cinematográficos.

El servicio permite a los usuarios pagar por un contenido mediante su tarjeta de crédito descargando la película en su disco duro. Cada película integra tecnología propietaria DRM, como la incluida en el Windows Media Player de Microsoft. Una vez descargada, la película reside en el disco duro del usuario durante 30 días. Si la película no se reproduce durante ese periodo, expira. Una vez que la película se ha reproducido se inicia un contador de 24 horas, transcurridas las cuales el fichero queda inutilizado.

4.2.4 Servicios DRM para productos de texto

También se han lanzado iniciativas DRM en la industria del texto. Microsoft ha desarrollado un sistema DRM para publicaciones electrónica a medida denominado *Digital Asset Server* (Servidor de Activos Digitales), su principal competidor en el mercado, Adobe, vende el *Adobe Content Server* (Servidor de Contenidos Adobe). Palm Digital Media, la división de software de Palm, ha desarrollado asimismo un sistema DRM a medida para la distribución de sus libros electrónicos (eBooks). La mayoría de las tiendas de libros electrónicos han adoptado dichas tecnologías. Los agregadores de DRM, tales como Overdrive, están utilizando tecnologías de varios vendedores de DRM para construir sistemas de diseño a medida para la industria editora en línea.

4.2.5 Servicios DRM para programas informáticos

Las consolas de juegos y los sistemas de juegos en línea están cada vez más siendo protegidos con sistemas DRM. Por ejemplo, la consola de juegos Xbox de Microsoft, incluye un sistema de encriptación por hardware de 128 bits, que impide que los usuarios jueguen con juegos pirateados así como utilizar la consola para cualquier otro propósito. Sony ha incluido también DRM en su consola PlayStation 2 y Nintendo en su GameCube.

Sin embargo, la proliferación de los denominados “chips de modificación”, que son circuitos que se conectan a la placa principal de una consola, permiten a los usuarios burlar la protección de copiado de la consola. Aunque el problema que plantean los “chips de modificación” puede no ser aún tan crítico como el uso sin autorización de música, películas y texto, las industrias de videojuegos y del *software* están cada vez más preocupadas por la penetración de los “chips de modificación” en los mercados más importantes. Por este motivo, tal como se analiza en la sección 3, Sony ha denunciado con éxito a distribuidores de “chips de modificación” en los Estados Unidos de América, en el Reino Unido y (después de apelación) en Australia.

4.2.6 Extensión de la DRM a otras industrias

Poco a poco se está admitiendo que la tecnología DRM se puede aplicar a otros sectores distintos de las industrias de contenidos con derechos de autor. Auque la gestión segura de información propietaria siempre ha sido un asunto importante en el comercio y la industria, existe una concienciación cada vez mayor de que el conocimiento de una organización es su activo más importante (y valioso). En este contexto, la definición del valor del conocimiento va más allá de las definiciones tradicionales de propiedad intelectual mediante patentes, derechos de autor y bases de datos propietarias. Cada vez más, los miembros de un consejo de administración y los ejecutivos principales están bajo la presión tanto de las autoridades reguladoras como de las partes con intereses en la empresa (accionistas, acreedores, ...) para demostrar que cuidan diligentemente la seguridad de la información que, en muchos casos, representa el principal valor para dichas partes.

Por estos motivos, se ha despertado un notable interés por las tecnologías analizadas en este documento. Utilizando técnicas DRM, las empresas esperan poder controlar la utilización de la información, mientras que hasta ahora, sólo podrían controlar el acceso a la misma. De esta forma, sus activos estarán mejor protegidos y se podrá hacer un seguimiento de dónde se consume la información. Ello proporcionará un nivel de seguridad mucho mayor que el actualmente posible.

4.2.7 Interoperabilidad

La interoperabilidad es un asunto que está presente en todos los debates sobre DRM y que se trata en la sección 2.5 de este documento, y cuya importancia no debe infravalorarse para el futuro de la distribución segura de contenidos. Posiblemente, la mejor forma de definir la interoperabilidad es como "la capacidad de dar cabida a reglas relativas a la utilización de derechos y contenidos, de interpretarlas de forma inequívoca y cuya observancia sea obligada en los distintos sistemas DRM *privados* y en dispositivos del usuario final". El término también se refiere a la capacidad de utilizar conjuntos de datos de orígenes diferentes como si hubieran sido creados con una norma común (algo esencial para la utilización de metadatos procedentes de diferentes comunidades).

Actualmente, la interoperabilidad no está al alcance de los titulares de derechos o de los usuarios, puesto que la mayoría de las aplicaciones de DRM se basan en "soluciones tipo isla" de un suministrador concreto, más que en normas ampliamente aceptadas. Además, la mayoría de las aplicaciones están limitadas a un único tipo de medio. Esto puede estar relacionado con la segmentación tradicional de las industrias de medios, así como con la disponibilidad de la tecnología.

Aunque las normas son esenciales para que exista interoperabilidad, también es necesario que los negocios se desarrollen impulsados por la demanda de los consumidores. Mientras no exista un grado adecuado de interoperabilidad que permita el interfuncionamiento de distintos sistemas sin que ello suponga un inconveniente para el usuario (ya sea un titular de derechos o un consumidor), es poco probable que la DRM tenga un éxito completo. Dada la importancia de la interoperabilidad, no es sorprendente que se haya suscitado la eventual intervención de los gobiernos para obligar al desarrollo de sistemas DRM interoperables. Este asunto se analiza en 5.2.3.

5. ASPECTOS POLÍTICOS DERIVADOS DE LAS TECNOLOGÍAS DRM

El desarrollo, aplicación, protección y uso de las tecnologías DRM suscita numerosos aspectos de índole política para los gobiernos y las instituciones internacionales, incluida la Comisión Europea y la OMPI, muchos de los cuales han sido sugeridos e identificados en el análisis precedente. En esta sección se presentan y analizan algunos de ellos.

5.1 Aspectos relativos a la propiedad intelectual

5.1.1 Aplicación de los Tratados de la OMPI

El Tratado de la OMPI sobre Derecho de Autor ("WCT", *WIPO Copyright Treaty*) entró en vigor el 6 de marzo de 2002, cuando 30 estados los habían ratificado o habían accedido al mismo. El Tratado de la OMPI sobre Interpretación o Ejecución de Fonogramas ("WPPT", *WIPO Performances and Phonograms Treaty*) entró en vigor el 20 de mayo de 2002. Unos 42 estados son actualmente (agosto de 2003) partes del WCT, y 42 lo son del WPPT.

La aplicación de los Tratados de la OMPI ha sido relativamente rápida en los Estados Unidos de América, Japón y Australia[222], aunque más lenta en la Unión Europea, donde el proceso de aprobación de la Directiva de Derechos de Autor ha llevado cierto tiempo. Además, en la Unión Europea sólo dos Estados Miembros cumplieron el plazo de transposición de dicha Directiva, y a fecha de agosto de 2003, solamente cinco lo habían hecho. Varios de los países principales aún no han aplicado los Tratados de la OMPI.

En relación con los países que han aplicado los Tratados de la OMPI y con la Unión Europea, han existido distintos enfoques. Dichas posibles variaciones ya fueron contempladas por las Partes Contratantes y están permitidas por los textos de los Tratados de la OMPI. Se han identificado varios tipos de variaciones.

En la mayoría de los países las disposiciones contra la elusión se han aplicado directamente mediante leyes de derechos de autor y leyes conexas o mediante disposiciones adyacentes a las mismas. Además, algunos países han ratificado los Tratados de la OMPI sin realizar cambios relevantes en sus regímenes nacionales, en el convencimiento de que su marco jurídico existente es adecuado para cumplir con las obligaciones derivadas de los Tratados.

Cada jurisdicción responsable de su aplicación ha determinado qué tipos de medidas tecnológicas deben protegerse, es decir, las que controlan el acceso a las obras así como aquellas que limitan los derechos exclusivos de los titulares de derechos. La mayoría de las jurisdicciones parecen proteger ambos tipos de medidas tecnológicas.

Además, las disposiciones que aplican los tratados de la OMPI generalmente restringen actos asociados a la elusión, incluyendo la fabricación y tráfico de herramientas de elusión. Algunas de las legislaciones de aplicación han ido más lejos y prohíben diferentes tipos de actos de elusión. En tales casos, la legislación puede eximir a determinadas personas de responsabilidad en relación con ciertas clases de actos de elusión. También puede ocurrir,

---

[222] Aunque Australia ha aplicado los Tratados de la OMPI, véase Sección 3.4, aún debe ratificarlos.

como es el caso de los Estados Unidos de América, que los actos de elusión no estén prohibidos en relación con medidas tecnológicas que protegen los derechos de autor, sobre la base de que dicha elusión es asimilable a una vulneración de derechos de autor.

Las diferencias son evidentes en la medida en la que se aplican excepciones o limitaciones a los actos o productos para la elusión. Además, en lo que se refiere a las disposiciones contra el tráfico, las leyes difieren respecto a si un dispositivo debe considerarse fuera de la ley o debe estar permitido, en función de si está dedicado "exclusivamente" o "principalmente" a la elusión.

Hasta la fecha no parece que la velocidad de aplicación de los Tratados de la OMPI, o las diferencias en la aplicación jurídica de los mismos, haya tenido un efecto mensurable en el desarrollo o utilización de las DRM. Es previsible que, con el tiempo, todas las Partes Contratantes cumplan las obligaciones derivadas de los Tratados, estando por ver si las diferencias en la aplicación de los mismos influyen en el desarrollo de las DRM o la protección de contenidos distribuidos mediante soluciones DRM.

5.1.2 Efecto de la DRM en las excepciones y limitaciones a los derechos de autor

Cuando se utilicen las tecnologías DRM, los titulares de derechos deben ser conscientes de las excepciones y limitaciones a las disposiciones contra la elusión y las excepciones a los derechos de autor (al menos en la Unión Europea). Por otro lado, puede que no sea fácil conseguir un engranaje perfecto entre, por un lado, las capacidades tecnológicas y comerciales de las DRM y, por otro, el resultado de consideraciones jurídicas y políticas reflejadas en las excepciones y limitaciones.

Por ejemplo, si en la Unión Europea los titulares de derechos utilizan medidas que impidan que los beneficiarios de una excepción accedan a ésta, puede que, algún tiempo más tarde, se lamenten de las medidas que los Estados Miembros puedan tomar para garantizar que dichas personas disfruten, de hecho, de tales beneficios. Así, tal como refleja la legislación propuesta en Alemania, el hecho de que los titulares de derechos no garanticen que los beneficiarios disfruten de la excepciones, puede acarrearles una sanción. Las DRM pueden desarrollarse y utilizarse con reglas que sean más o menos coherentes con las excepciones, pero inevitablemente no abarcarán absolutamente todas las excepciones que haya (o pueda haber), para las que la tecnología DRM no es capaz, por sí misma, de verificar la legitimidad del derecho del beneficiario a la excepción.

De hecho, en los Estados Unidos de América, la relación entre la utilización de DRM y las excepciones al derecho de autor se discutió extensamente en relación con la inclusión en la DCMA del concepto de elusión legítima (basada en el uso lícito). La doctrina del "uso lícito" es tan maleable y sujeta a casos y circunstancias particulares que, finalmente, el Congreso determinó que no podría haber una excepción basada en dicho "uso lícito" a las disposiciones contra la elusión; sin embargo, esta cuestión vuelve a estar presente de nuevo con motivo de legislación actualmente en desarrollo en los Estados Unidos de América. Igualmente, salvo que se desarrollen DRM que puedan autorizar la utilización sobre la base de casos concretos, es decir, determinando cuándo una petición de uso es "lícita", será difícil que las soluciones DRM acomoden dicha excepción al derecho de autor.

En numerosas ocasiones han surgido en los Estados Unidos de América cuestiones sobre si una medida tecnológica admite la copia privada legítima o los usos lícitos. En uno de

tales casos, se ha señalado que la ley o la tecnología ha tenido en cuenta de forma sólo aproximada las preocupaciones existentes sobre el uso lícito, aplicando lo que se denomina "justicia aproximada" ("*rough justice*"), reconociendo al mismo tiempo que determinados "usos lícitos" legítimos no serían tecnológicamente posibles.

Por ejemplo, en relación con la Ley de Grabación de Audio en el Hogar (*Audio Home Recording Act*), la aplicación requerida del sistema de gestión de copia en serie (o su equivalente funcional) significa que no serían técnicamente posibles más de dos generaciones de copias de audio (incluso de copias legítimas propiedad del usuario de obras protegidas por derechos de autor); no sería posible la copia digital de un copia digital. Sin embargo, en relación con la primera de estas dos limitaciones, dicha copia en serie sería presumiblemente consentida por el titular de los derechos de autor. Con respecto a la segunda, la copia en serie de audio digital puede constituir, en algunos casos, un uso lícito (para fines tales como hacer grabaciones de mezclas y selecciones), siendo en tal caso legítima.

Tal como se describe en 3.2.1 y 4.1.8, en los Estados Unidos de América ciertas "reglas de codificación" han sido objeto de discusión durante varios años [223]. Dichas reglas permiten un numero ilimitado de copias en serie en determinadas circunstancias, una generación de copias en otras y ninguna en otras. También en este caso, pueden existir casos de copia privada autorizada o de uso lícito que se verían obstaculizados por la aplicación de estas reglas. De nuevo en este caso, los compromisos que reflejan estas reglas de codificación han sido interpretados (por algunos) en el sentido de permitir una cantidad adecuada de reproducciones privadas no comerciales, de forma que sean admisibles las restricciones que se derivan de las reglas.

En un sentido similar, los Tratados de la OMPI exigen a las Partes Contratantes que proporcionen una protección adecuada a las medidas tecnológicas utilizadas para proteger derechos de autor y derechos conexos. En general, la legislación de aplicación de los mismos ha seguido la esencia de dicho mandato. Entonces, ¿cuál es la situación jurídica de las DRM que se utilicen para distribuir contenidos de dominio público de forma protegida?, ¿son los actos de elusión y los productos diseñados para la elusión de dichas DRM legítimos porque el contenido que protegen no está sujeto a derechos de autor?.

Los consumidores, instituciones educativas y académicas han manifestado su preocupación porque dichas DRM pueden utilizarse para bloquear el acceso a contenidos cuyo periodo de aplicación de derechos de autor haya expirado. Sin embargo, a ese respecto se estima que las disposiciones contra la elusión dejarán de ser aplicables en dicho momento. Los titulares de derechos y los proveedores de DRM no han adoptado uniformemente la posición de que las protecciones legales de las DRM sean inaplicables cuando la DRM se utilice para proteger una obra de dominio público. En lugar de ello, desde su punto de vista, en tanto que una DRM se utilice para proteger obras con derecho de autor, debería seguir siendo ilegítimo desarrollar herramientas que pudieran ser utilizadas para la elusión de dicha DRM, incluso cuando la herramienta se utilice para la elusión de medidas tecnológicas aplicadas a una obra de dominio público. Argumentan que la actividad ilegítima es el tráfico de un dispositivo que eluda una DRM utilizada para proteger una obra con derechos de autor. Por lo tanto, los esfuerzos para limitar las disposiciones contra la elusión solamente a las DRM utilizadas para proteger obras amparadas por el derecho de autor pueden resultar

---

223 Véase la nota 42, Marks/Turnbull.

relativamente estériles debido a que los dispositivos que eludan dichas DRM (incluso cuando se apliquen para proteger obras sin derechos de autor) pueden seguir siendo ilegítimos.

El hecho de si las DRM y las protecciones legales conexas tendrán en cuenta adecuadamente las excepciones y limitaciones legítimas incluidas en las leyes de derechos de autor nacionales, se irá aclarando conforme se implementen dichos sistemas. Parece probable que una DRM o contrato específico no permita todos los casos de copia privada, copia para la realización de ingeniería inversa o copia para un uso lícito. Sin duda alguna, ninguna legislación que aplique los Tratados de la OMPI permitirá la elusión en todas las situaciones anteriores. Inevitablemente, los usos legítimos pueden verse frustrados por las DRM, los contratos con los titulares de derechos y distribuidores de contenidos, así como por las leyes que les dan legitimidad. Los usuarios finales y los gobiernos han mostrado su preocupación por el hecho de que los contratos puedan eventualmente impedir las excepciones establecidas por ley o por vía judicial, o limitar los derechos judiciales[224]. Debe asimismo señalarse la preocupación expresada por los usuarios relacionada con que una de las limitaciones más significativas de los derechos de autor (la limitación en el plazo de aplicación de los mismos) pueda verse anulada por contrato; en concreto, si los titulares de derechos podrán ejercer el control de obras de dominio público una vez que hayan expirado los derechos de autor, condicionando el acceso a dichas obras (mediante una DRM que controle dicho acceso) de usuarios que cumplan las restricciones de utilización[225].

Los precedentes parecen sugerir que incluso puede resultar aceptable una aplicación inexacta de dichos usos legítimos mediante DRM y contratos de distribución. Los titulares de derechos pueden poder ofrecer ciertos tipos de licencias a colectivos específicos de beneficiarios de excepciones establecidas por ley, o pueden ofrecer contenidos en determinados formatos a diferentes tipos de personas. También es previsible que los titulares de derechos tengan gran interés por conocer los mecanismos de supervisión y aplicación puestos en juego para la utilización efectiva de la DRM. Además, si los titulares de derechos no incluyen la copia privada en su implementación de soluciones DRM, al menos en la Unión Europea, la Directiva de Derechos de Autor deja bien claro que los Estados Miembros podrán intervenir directamente (o imponer sanciones) para garantizar que las prácticas, permitidas al amparo de excepciones a los derechos de autor, no se vean bloqueadas por las medidas tecnológicas utilizadas.

Los consumidores, educadores, bibliotecarios y otros usuarios de contenidos con derechos de autor pueden tolerar cierto nivel de imprecisión en relación con la forma en la que las DRM acomoden sus requisitos. Sin embargo, su voluntad para actuar así, puede depender de la medida en la que perciban que los titulares de derechos no abusen de la utilización de tecnologías DRM, y si son manifiestos los beneficios de carácter más amplio derivados de disponer de contenidos en un entorno basado en DRM.

---

224 Véanse, por ejemplo, el informe del Comité para la Revisión de la Ley de Derecho de Autor, *Copyright and Contract* (abril de 2002) (informe Australiano que resume las propuestas recibidas sobre la preponderancia, efectos y conveniencia de contratos destinados a obliterar las excepciones a los derechos de autor), que está disponible en http://www.law.ecel.uwa.edu.au/ipcr339/CopyrightContractAct.pdf.

225 Véase, por ejemplo, B. Hugenholtz, *Copyright, Contract and Code: What Will Remain of the Public Domain*, 26 Brook. J. Int'l L. 77, 78 (2000) (donde se argumenta que la "combinación de contrato y tecnología supone una amenazada directa al sistema de derechos de autor tal como lo conocemos hoy en día").

5.1.3 Las DRM y el canon por copia privada

Tal como se ha analizado en 3.3.2, y en relación con las discusiones habidas en el Taller de la Comisión Europea sobre la gestión de derechos digitales, en Europa se ha prestado una gran atención a la relación entre los cánones por copia privada y la aplicación de las tecnologías DRM (aunque en los Estados Unidos de América se aplican cánones a los dispositivos y medios de grabación de audio digital, al amparo de la *Audio Home Recording Act*, la gama de dispositivos y medios sobre los que se impone el canon está relativamente restringida y la eliminación de dichos cánones no ha sido recientemente objeto de un debate relevante). La justificación histórica de dichos cánones es compensar a los titulares de derechos por la copia privada no específicamente autorizada de sus obras y por la que no recibirían remuneración alguna. Las leyes de derechos de autor de la mayoría de los Estados Miembros de la Unión Europea incluyen cánones sobre dispositivos y medios de grabación .

En Europa, la Directiva de Derechos de Autor señala específicamente que en relación con la copia privada, los Estados Miembros proveerán excepciones al derecho de autor " siempre que los titulares de los derechos reciban una compensación equitativa, teniendo en cuenta si se aplican o no a la obra o prestación de que se trate las medidas tecnológicas"[226]. Por lo tanto, se reconoce que la aplicación de las DRM afectará a si los titulares de derechos obtienen una "compensación equitativa". En la medida en que se imponen cánones por copia privada a dispositivos y a medios, los consumidores y la industria tecnológica han señalado que permitir que los titulares de derechos obtengan una compensación adicional mediante la utilización de la tecnología DRM puede dar lugar a una doble compensación que exceda lo que es "equitativo".

La Directiva de Derechos de Autor sólo trata explícitamente las relaciones entre los sistemas de canon nacional y la utilización de DRM en sus Considerandos. En el Considerando 38 se establece que en relación con el uso privado, los Estados Miembros pueden permitir una excepción que esté acompañada de una "compensación equitativa"; a este respecto, pueden introducirse o mantenerse "sistemas de remuneración"[227]. El Considerando permite que se mantengan los sistemas para la reproducción privada analógica, pero reconoce que "la copia privada digital puede extenderse mucho más", que existen diferencias entre la copia privada digital y analógica, y que "debe establecerse entre ellas una distinción en determinados aspectos."[228]

El Considerando 39 ha sido básico en las discusiones sobre las relaciones entre cánones y DRM. Establece lo siguiente:

> *"Al aplicar la excepción o limitación relativa a la copia privada, los Estados Miembros deben tener en cuenta el desarrollo económico y tecnológico, en particular, en lo relativo a la copia digital privada y a los sistemas de retribución, siempre que existan medidas tecnológicas de protección eficaces. Dichas excepciones o limitaciones no deben impedir ni el uso de medidas tecnológicas ni su aplicación en caso de elusión."*[229]

---

226 Artículo 5.2)b), Directiva de Derechos de Autor.
227 Considerando 38, Directiva de Derechos de Autor.
228 *Id*.
229 Considerando 39.

El Considerando reconoce claramente la relación entre copia privada, sistemas basados en un canon y sistemas DRM asociados. Cuando "existan" medidas DRM "eficaces", la Directiva de Derechos de Autor sugiere que se modifiquen o incluso se supriman los sistemas basados en canon. Aunque los conceptos de eficacia y existencia pueden ser teóricamente transparentes, puede resultar extremadamente difícil determinar en la práctica lo que existe o lo que es eficaz. Aunque es posible establecer si un sistema DRM "existe" (está disponible), ¿en relación con qué tipos de contenidos debe un sistema DRM "existir" de una forma suficiente, de forma que deje de ser necesario imponer un canon por copia privada de dicho contenido?.

Posiblemente surgen preguntas más difíciles de contestar en relación con el concepto de "eficacia". Aunque una medida DRM puede ser "eficaz" para limitar la copia no autorizada, ¿qué significa ser "eficaz" para los fines de modificar o eliminar un sistema basado en un canon?. Por ejemplo, si una DRM sólo permite la copia privada de un tipo concreto de contenido sobre ciertas clases de dispositivos y medios de grabación, ¿debería eliminarse el canon para dichos tipos?. Pero, ¿qué ocurre si dichos tipos pueden también utilizarse para hacer copias privadas de contenidos no sujetos a una DRM, contenidos para los que los titulares de derechos no obtendrían así compensación alguna? ¿será necesario que los Estados Miembros examinen la DRM asociada a cada tipo de contenido y cada clase de dispositivo o medio de grabación digital para llevar a cabo la transición?. Dado que actualmente parece que dichas medidas se tomarán a nivel nacional ¿ qué probabilidad existe de que se desarrollen sistemas inconsistentes en el seno del mercado interior?.

También en este caso es improbable que exista una precisión absoluta entre la protección total del contenido mediante DRM y la eliminación de cánones sobre dispositivos y medios de grabación utilizados para la copia digital de dicho contenido. De nuevo, puede ser adecuado adoptar un sistema de "justicia aproximada" ("*rough justice*") que deje en manos de los Estados Miembros decidir si existe en el mercado una utilización real o potencial suficiente de DRM para los contenidos digitales que permita una remuneración adecuada a los titulares de derechos por copia privada. Tras sondear su propio entorno, los Estados Miembros podrían concluir que, en su conjunto, los titulares de derechos reciben una compensación equitativa por dichos usos. En dicha situación, en la que se considera que "existen" sistemas DRM eficaces que pueden ser utilizados, los Estados Miembros podrán considerar el abandono del sistema de canon por el que los titulares de derechos vienen siendo remunerados.

5.2 Otros asuntos de naturaleza política

5.2.1 Privacidad

La utilización de tecnologías DRM suscita aspectos que van más allá de la protección de la propiedad intelectual, incluyendo posiblemente como aspecto más notable, lo relacionado con la privacidad individual. Tal como se describe en 2.4.9, la utilización de estas tecnologías puede considerarse que presenta dos aspectos bien diferentes, a saber, la mejora de la privacidad y la posible amenaza a la misma.

Las tecnologías DRM generalmente se basan en comunicaciones seguras y en la autenticación entre dos o más dispositivos. A menudo garantizan que el contenido se entrega a una persona que ha acordado los términos y condiciones por los cuales se permite su acceso al material con derecho de autor. Los pagos pueden realizarse del mismo modo. En dichas

circunstancias, la transacción entre el titular de derechos y el consumidor se mantiene en privado frente a terceros. De la misma forma, en la medida en que las tecnologías DRM permiten a un consumidor hacer una transferencia lícita de una obra o de la autorización para que la utilice una tercera parte, las tecnologías DRM mantienen la privacidad e integridad de la transacción. Finalmente, en la medida en que las tecnologías DRM permiten que los titulares de derechos y los distribuidores mantengan registros con datos de los consumidores e historias de las transacciones, el proceso por el que el consumidor realiza la compra y recibe el contenido protegido mediante DRM puede resultar ser más rápido y eficiente. En relación con dichos aspectos, los consumidores pueden apreciar los beneficios que aportan las tecnologías DRM.

Sin embargo, los consumidores y los defensores de la privacidad ven un lado potencialmente oscuro en la utilización de sistemas DRM. Han expresado su preocupación de que la utilización de dichas tecnologías facilitará inevitablemente la recogida y agregación de datos personales de los consumidores por parte de los titulares de derechos y de los distribuidores de contenidos. Los consumidores recelan de las posibilidades que existen para conformar perfiles y de las tecnologías que combinan datos sobre sus hábitos de uso y sus identidades. Existe la preocupación de que terceras partes puedan acceder a la computadora personal de una persona para la autenticación de dispositivos a fin de asegurar que éstos son "confiables".

Una preocupación adicional es que los consumidores puedan perder la capacidad de hacer un uso legítimo pero anónimo de contenidos con derechos de autor. Por ejemplo, en determinadas situaciones de "uso lícito", los usuarios de contenidos protegidos por derechos de autor pueden desear utilizar material sin que se les asocie personalmente con el mismo. Sin embargo, las tecnologías DRM a menudo exigen una transacción bilateral entre el titular de derechos y un consumidor conocido, y los derechos para utilizar la obra pueden acompañar al contenido. De esta forma, se pierde la posibilidad de un uso anónimo del contenido.

Para estar seguros, el consumidor preocupado por la pérdida de su intimidad puede deshabilitar los sistemas DRM, o simplemente renunciar a adquirir contenidos en línea. Sin embargo, se ha señalado que de esta forma los consumidores se privan a si mismos (aunque sea por elección propia) del acceso a materiales protegidos con derechos de autor que, cada vez más, sólo pueden obtenerse mediante tecnologías DRM.

Varias instituciones gubernamentales han estudiado en distinto grado las relaciones entre la utilización de sistemas DRM y la preocupación sobre la privacidad. En la Unión Europea, el Considerando 57 de la Directiva de Derechos de Autor arroja luz sobre el asunto al señalar que los sistemas de gestión de derechos "pueden, simultáneamente, procesar los datos personales sobre hábitos de consumo de las prestaciones protegidas por parte de personas individuales y permitir el seguimiento de los comportamientos en línea."[230]. El Considerando señala que dichas medidas técnicas deben incluir "garantías de respeto de la intimidad" de conformidad con lo dispuesto en la Directiva europea de Protección de Datos, que protege los datos personales[231]. La Directiva de Protección de Datos establece un marco

---

230 Considerando 57.

231 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos derechos de autor y otros derechos afines a los derechos de autor

[Sigue la nota en la página siguiente]

completo que se aplica a la recopilación, uso, procesamiento, revelación y seguridad de los datos personales en los Estados Miembros, así como la transferencia de dichos datos a terceros países. La Directiva de Protección de Datos se aplica directamente a los sistemas de recogida y de procesamiento automáticos, tal como los utilizados un sistema DRM.

De conformidad con la Directiva de Protección de Datos, los datos personales solo pueden ser recopilados y utilizados para los fines específicos autorizados por la "persona afectada" es decir, la persona de cuyos datos se trate. Además, la Directiva requiere que el responsable de los datos implemente "las medidas técnicas y de organización adecuadas para la protección de los datos personales contra... la difusión o el acceso no autorizado, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red ... "[232]. Dada la amplitud de miras de la Directiva de Protección de Datos y su relevancia directa para los sistemas DRM, se deberían disipar en cierta medida las preocupaciones sobre el posible abuso que los titulares de derechos y los distribuidores puedan ejercer en relación con los datos que recopilen de los consumidores.

En los Estados Unidos de América, la protección de los datos personales se ha descrito a menudo como un mosaico de medidas de protección, con diferentes prescripciones legales a nivel estatal y federal. Durante los últimos años, la Comisión Federal del Comercio y los Fiscales Generales de los Estados han sido muy activos para garantizar que las compañías que utilizan medidas tecnológicas de protección o recopilación de datos, hagan saber a los consumidores de manera precisa cuales son sus políticas de seguridad, privacidad y de recopilación de datos. Estas instancias del gobierno pueden presentar denuncias ante los tribunales y conseguir que se impongan sanciones civiles a las empresas que no hayan aplicado las medidas de seguridad adecuadas para salvaguardar los datos en sus sistemas [233] .

Asimismo, en los Estados Unidos de América, los aspectos sobre la privacidad fueron analizados durante el proceso de aprobación de la DMCA, reconociendo ésta específicamente la existencia de relaciones entre la utilización de las tecnologías digitales y las preocupaciones existentes sobre la privacidad. Tal como se analiza en 3.2.1.1(c), la Sección 1201(i) de la DMCA establecer una excepción a las disposiciones contra la elusión basada en el derecho a

---

[Continuación de la nota de la página anterior]

en el mercado interior, Diario Oficial L 281/31, 23/11/1995 ["Directiva de Protección de Datos"].

232 Artículo 17, Directiva de Protección de Datos.

233 Véase *In the Matter of Microsoft Corp.*, FTC No. 012 3240 (2002) (véase *http://www.ftc.gov/os/2002/08/microsoftcmp.pdf* (denuncia interpuesta) y *http://www.ftc.gov/opa/2002/08/microsoft/htm* (acuerdo) (acuerdo sobre la denuncia relativa al sistema de autenticación Passport y prohibición de prácticas de falseamiento de la información y exigencia de mantener un programa completo de seguridad de la información); véase *In the Matter of Eli Lilly and Co.*, FTC No. 012 3214 (2002) (en *http://www.ftc.gov./opa/2002/01/elililly.htm*) (acuerdo para realizar un programa intensivo de supervisión en caso de que se desvelen inadvertidamente direcciones de correo electrónico) (seguido de un acuerdo con los fiscales generales de ocho estados); véase *In the Matter of Ziff Davis Media, Inc.,* Aseguramiento de que se abandonan determinadas prácticas (28 de agosto, 2002) (en *http://www.oag.state.ny.us/press/ 2002/aug/aug28a_02_attach.pdf*) (tras una exposición errónea de los datos personales de clientes, aseguramiento de la discontinuidad de tales prácticas ante el fiscal general de Vermont, New York y California, con exigencia de revisión, supervisión en aplicación de medidas relativas a la intimidad, seguridad e integridad de los datos, y del pago a los clientes afectados).

la intimidad, a saber, que no es una vulneración de la prohibición legal que una persona eluda una medida tecnológica que proteja las *cookies* o determinadas obras con derecho de autor (tales como programas informáticos utilizados en un sistema DRM) que recopilen o diseminen información sobre las actividades en línea de una persona sin advertirlo.

Está aún por determinar si la excepción de la Sección 1201(i) tendrá consecuencias significativas sobre la armonización de aspectos relativos a la intimidad y la utilización de sistemas DRM. Sin embargo, es previsible que el impacto de dicha excepción sea bastante limitado. Sólo se permite la elusión si la única consecuencia de ésta es identificar e inhabilitar la medida (y no obtener el acceso no autorizado a una obra). Además, la excepción solo se aplica si el único objetivo de la elusión es impedir la recopilación o diseminación de información de identificación personal.

5.2.2 Jurisdicción y ley aplicable

Las DRM se utilizarán inevitablemente para proteger y distribuir contenidos a nivel internacional. Por ese motivo cabe plantearse cuál será la jurisdicción cuya ley sea "aplicable" tanto para la protección de la DRM como del contenido subyacente. En múltiples foros de carácter internacional y regional se están planteando las cuestiones sobre la elección de la ley y la jurisdicción aplicable en el entorno de los servicios en línea, incluyendo las cuestiones surgidas como consecuencia de acuerdos de propiedad intelectual.

En relación con la utilización de las tecnologías DRM, se plantean tres cuestiones de carácter jurisdiccional que están estrechamente relacionadas:

– Primero, ¿cuál será el país cuya ley contra la elusión resulte aplicable a la protección (o a la elusión o la piratería) de tecnologías DRM?

– Segundo, ¿cuál será la ley aplicable por la utilización, o utilización indebida, de un contenido protegido con DRM?

– Tercero, ¿cuál será la ley nacional aplicable a los acuerdos relativos a la distribución de contenidos mediante DRM?

En primer lugar, las leyes contra la elusión y sobre el acceso condicional son de alcance territorial. Si un acto de elusión, incluido el tráfico de un dispositivo, se produce dentro de las fronteras de un país, resulta aplicable la ley de dicho país. La jurisdicción de dicho país podría incluso resultar aplicable a la distribución en línea en dicho país desde el extranjero de un programa de elusión, aunque resulte difícil ejercer dicha jurisdicción sobre el distribuidor extranjero.

En el caso de *los Estados Unidos de América contra Elcom, Ltd.*, analizado en 3.2.2, una compañía extranjera asentada en el país y una compañía extranjera fueron acusadas en los Estados Unidos de América de violación de las disposiciones contra el tráfico del Artículo 1201.b), por haber creado y distribuido software que desencriptaba el software de seguridad de los libros electrónicos (eBook) de Adobe. El tribunal rechazó expresamente el argumento de que estaba pretendiendo aplicar su jurisdicción extraterritorialmente. Determinó que el demandado tenia suficientes conexiones con los Estados Unidos de América, puesto que los actos demandados habían ocurrido en el territorio de dicho país: el

software de elusión delictivo era ofrecido y vendido a través de internet a residentes en los Estados Unidos de América, el servidor de Internet desde el que se vendía el *software* estaba situado en los Estados Unidos de América y el servicio de pago en línea del software también estaba ubicado en los Estados Unidos de América[234].

En segundo lugar, si una persona consigue utilizar una obra con derechos de autor de forma distinta a la permitida por un sistema DRM, dicho uso constituirá muy probablemente una violación del derecho de autor según la ley nacional relevante. En relación con el acceso en línea y la utilización del contenido, la jurisprudencia y los principios internacionales están evolucionando, tanto en relación con el país en el que una persona puede ser acusada por un acto de vulneración ocurrido en múltiples jurisdicciones, como en relación con la ley que debe regir en ese caso. Los principios aplicables pueden derivarse de la legislación nacional y de los Tratados ADPIC de la OMPI; los estudios sobre estos asuntos se están realizando en el contexto del Proyecto de Convención de la Haya sobre Jurisdicción Internacional y Juicios en el Extranjero sobre Asuntos Civiles y Comerciales[235]. En enero de 2001, la OMPI organizó un foro sobre Derecho Internacional Privado y Propiedad Intelectual para analizar, entre otros asuntos, las cuestiones relativos a la jurisdicción, (sobre las partes y la demanda) y la elección de la ley en relación con las obras transmitidas sobre redes digitales[236].

En tercer lugar, la determinación de la ley aplicable a un acuerdo por el que un consumidor recibe un contenido mediante un sistema DRM implica identificar la sede en que se celebra dicho contrato y los principios jurídicos pertinentes. En general, resulta aplicable la ley especificada en el contrato. Cuando las partes no hayan elegido la ley aplicable, puede apelarse a otros principios, tales como el establecido en el convenio de Roma de 1980, a saber, el tribunal debe aplicar la ley del país en el que la parte que realiza la "prestación característica" mediante el contrato tiene su residencia o su principal establecimiento comercial[237].

En la Directiva sobre el Comercio Electrónico se incluyen directrices sobre los principios jurídicos aplicables en la Unión Europea, que adopta la "regla del país de origen". Un proveedor de servicio está sujeto a las leyes de los Estados Miembros en los que está establecido, entendiéndose por establecimiento el lugar desde el que se realiza su actividad

---

234 *United* States *contra Elcom, Ltd.*, No. CR 01-20138 RMW (N.D. Cal. 27 de marzo de 2002) (decisión que deniega la solicitud de sobreseimiento para desestimar el auto de procesamiento por falta de jurisdicción sobre el asunto).

235 Véase *http://www.hcch.net/e/workprog/jdgm.html*.

236 Los documentos fueron preparados por los profesores André Lucas y Jane C. Ginsburg. Véase A. Lucas, *Private International Law Aspects of the Protection of Works and of the Subject Matter of Related Rights Transmitted Over Digital Networks*, Foro del a OMPI sobre Derecho Internacional Privado y Propiedad Intelectual (WIPO/PIL/01/1 Prov. 17 de diciembre de 2000); J. Ginsburg, *Private International Law Aspects of the Protection of Works and Objects of Related Rights Transmitted Through Digital Networks (2000 Update)*, Foro de la OMPI sobre Derecho Internacional Privado y Propiedad Intelectual (WIPO/PIL/01/2, 18 de diciembre de 2000), ambos disponibles en *http://www.wipo.int/pil-forum/en/index.html*.

237 Artículo 4.2, Convenio de la CE sobre la ley aplicable a las obligaciones contractuales (Roma 1980) ("se presumirá que el contrato presenta los vínculos más estrechos con el país en que la parte que deba realizar la prestación característica tenga, en el momento de la celebración del contrato, su residencia habitual o, si se tratare de una sociedad, asociación o persona jurídica, su administración central").

económica o proporciona su servicio[238]. En los Estados Unidos de América, cada estado tiene un principio de elección de ley que indica al tribunal la ley que debiera aplicar en ausencia de un acuerdo entre las partes.

5.2.3 El papel de los gobiernos en el establecimiento de normas y en la interoperabilidad

Una cuestión básica presente en los debates sobre el desarrollo e implementación de las tecnologías DRM se refiere al papel adecuado y necesario que han de jugar los gobiernos o las instituciones gubernamentales. Como caso más representativo, cabe señalar que el desarrollo de la Ley de Fomento de la Televisión y la Banda Ancha para el Consumidor (*Consumer Broadband and Digital Television Promotion Act*), analizada en 3.2.1.4, estuvo especialmente motivado por la preocupación de los titulares de derechos porque el sector privado no actuara con la rapidez suficiente para dar respuesta a las cuestiones relativas a la protección de los contenidos. Quienes apoyaban el proyecto de ley argumentaban que el gobierno debía intervenir cuando la industria no encontrase soluciones tecnológicas en un plazo dado. El proceso de Talleres sobre DRM llevado a cabo por la Comisión Europea y analizado en 3.3.2 comenzó y terminó con una investigación sobre si la Comisión debía tomar medidas adicionales para acelerar el desarrollo de soluciones DRM, con un énfasis especial en la normalización e interoperabilidad.

En relación con este asunto, pueden hacerse varias observaciones. En primer lugar, si bien los titulares de derechos y las sociedades de gestión colectivas han sido más receptivos a que la participación de los gobiernos sea un último recurso, las industrias tecnológicas se han opuesto frontalmente y de forma homogénea a la mera sugerencia de intervención directa de los gobiernos en el establecimiento de normas. Ciertamente, las compañías tecnológicas y la mayor parte de los titulares de derechos han reconocido que un proceso de normalización dirigido por el sector privado y con participación voluntaria es preferible a una actuación del gobierno. Poco a poco, la colaboración entre las industrias para el desarrollo de DRM ha aumentado, y puesto que han progresado rápidamente los estudios sobre aspectos tales como la protección de contenidos en la radiodifusión digital, la necesidad de una intervención gubernamental en las actividades del sector privado parece haberse reducido sustancialmente.

En segundo lugar, en la medida en que las diversas soluciones DRM actualmente adoptadas pueden tener carácter propietario y no ser completamente interoperables, se ha planteado si los gobiernos deberían iniciar o impulsar el proceso de normalización, así como asegurar que las tecnologías evolucionan hacia la interoperabilidad. La mayor parte del sector privado, ya sean compañías tecnológicas o desarrolladores de soluciones DRM, sigue creyendo firmemente que estos asuntos deben dejarse en manos de la industria. Desde su punto de vista, las fuerzas del mercado y las necesidades de los consumidores son los factores que impulsarán más decididamente la compatibilidad e interoperabilidad entre sistemas DRM. También opinan que, por el contrario, los gobiernos no están bien preparados para realizar un papel activo y de liderazgo en el desarrollo de soluciones orientadas al mercado.

Sin embargo, en este sentido los gobiernos pueden ayudar considerablemente, en particular promoviendo foros de discusión en los que participen los distintos sectores industriales afectados. En dichas reuniones, los participantes del sector privado pueden

---

238 Considerando 19, Directiva sobre el Comercio Electrónico.

compartir y documentar sus progresos en pro de determinadas soluciones, así como contribuir a la formación de otros agentes, incluidos quienes toman decisiones políticas. Además, los gobiernos pueden asumir un papel más activo creando un entorno jurídico que facilite la normalización y la cooperación. Cuando los gobiernos impulsen el proceso de maduración de las DRM y de otras industrias tecnológicas, y fomenten una amplia utilización de las tecnologías DRM, podrán adoptar medidas que reconozcan la importancia de las tecnologías DRM en las respectivas leyes sobre la competencia y en los procedimientos empleados para la observancia de dichas leyes de la competencia.

En tercer lugar, la mayoría de los participantes del sector privado reconocen que el gobierno debe ejercer un papel para garantizar y hacer cumplir las soluciones acordadas por el sector privado. El ejemplo de los Tratados de la OMPI y de la legislación que los aplica demuestra que las leyes adoptadas por los gobiernos son necesarias para salvaguardar las protecciones tecnológicas. Los antecedentes jurídicos que consideran ilegal el pirateo de sistemas de acceso condicional van en el mismo sentido. Las actuaciones del sector privado y los acuerdos entre partes privadas tienen serias limitaciones para localizar y sancionar a quienes se beneficien del acceso a contenidos sin pagar por ello. Las leyes son esenciales para que todo el mundo (individuos y fabricantes de productos y similares) respete las mismas reglas de protección de contenidos. En este sentido, la disposición reglamentaria de la FCC sobre la marca (bandera) de radiodifusión es un ejemplo claro de un actuación adecuada por parte de un gobierno para hacer cumplir las soluciones acordadas por la industria.

En cuarto lugar, el poder de los gobiernos para dictar obligaciones está necesariamente limitado al ámbito de soberanía en el que ejercen su autoridad. Incluso las instituciones de la Unión Europea, con poder para el desarrollo y observancia de normas jurídicas por parte de los Estados Miembros, carecen de autoridad fuera de sus fronteras. Pero como los Tratados de la OMPI ponen de relieve, es obvia la necesidad de un enfoque armonizado sobre las tecnologías de protección de contenidos, incluyendo los sistemas DRM. En este sentido, y mediante un ejemplo, en la sección 3.2.1.3.b) se refleja la situación de desprotección en que quedan los titulares de derechos sobre contenidos cuando la radiodifusión en formato digital de los mismos está técnica y jurídicamente protegida contra la redistribución en un país, pero la señal de televisión se recibe también en un país vecino desde el que puede ser redistribuida impunemente. En consecuencia, una importante tarea en curso de los gobiernos es determinar como pueden cooperar razonablemente para facilitar un enfoque sin fisuras para la protección de contenidos y de sistemas DRM conexos.

5.2.4 Prácticas y obligaciones relacionadas con la concesión de licencias de tecnología

Las prácticas de negocio y las leyes asociadas en relación con la concesión de licencias DRM y, más generalmente, la normalización tecnológica, están íntimamente relacionadas con el papel del gobierno en el establecimiento de normas. Las tecnologías y normas DRM pueden estar protegidas o regirse por las leyes de patentes, de derecho de autor y de secretos comerciales.

Frecuentemente, las normas se clasifican en "abiertas" y "propietarias". Las normas "abiertas" son las desarrolladas por una entidad de naturaleza abierta, de amplia base, en la que pueda participar cualquier parte interesada, sujeta a las reglas específicas de dicho foro. A nivel internacional, la Unión Internacional de Telecomunicaciones (UIT) y la Comisión Electrotécnica Internacional (CEI) son ejemplos de entidades de elaboración de normas "abiertas". A nivel Europeo, el Instituto Europeo de Normas de Telecomunicaciones (ETSI, *European Telecommunications Standards Institute*) es un ejemplo de dicho tipo de organismo. Las entidades nacionales incluyen organizaciones tales como el *American National Standards Institute* de los Estados Unidos de América y la *Japan Electronics and Information Technology Industries Association* de Japón.

Las normas "propietarias" son desarrolladas, y sus licencias otorgadas, por compañías individuales, o grupos de compañías, con derechos de propiedad intelectual aplicables a las mismas. Las tecnologías DRM específicas, incluyendo algunas de las antes analizadas, son producto de actividades de desarrollo individuales o conjuntas y cuyas licencias se conceden sobre una base propietaria y con regalías (*royalties*).

La concesión de licencias de tecnologías incluidas en normas adoptadas mediante procesos abiertos, así como las incluidas en sistemas propietarios, se rige por una serie de requisitos jurídicos. Para garantizar que las normas no se adoptan sin una comprensión cabal de los derechos de patentes que pueden afectar a cada caso concreto, los participantes en un organismo de elaboración de normas con "garantías de procedimiento" y de naturaleza abierta, normalmente acuerdan notificar a los demás participantes la existencia de derechos de propiedad intelectual asociados a una norma propuesta y, más aún, que concederán una licencia sobre dichos derechos en términos razonables y no discriminatorios[239]. En los Estados Unidos de América, la Comisión Federal de Comercio declaró que es una práctica ilícita que un participante en un organismo de normas abiertas no desvele que tiene alguna demanda sobre una patente esencial pendiente hasta después de que se haya adoptado una norma, y resolvió sobre este asunto mediante una orden que prohíba al titular de una patente

---

239 Véase*, por ejemplo,* ETSI *Intellectual Property Rights Policy* (abril 2003) (que requiere a los participantes que notifiquen a los demás sus reclamaciones de derechos esenciales, solicitar que las licencias se concedan en términos razonables y no discriminatorios, buscar alternativas si no están disponibles en dichos términos y publicar las reclamaciones de derechos de propiedad intelectual notificadas junto con la norma adoptada), disponible en *http://portal.etsi.org/directives /directives_apr_2003.doc*; ANSI Essential Requirements: requisitos de las garantías de procedimiento de la American National Standards, sección 3.1 (marzo de 2003) (los participantes deben reconocer que no tienen propiedad intelectual al respecto o que, si la tienen, concederán una licencia sin coste alguno o sobre la base de términos y condiciones razonables que estén "demostrablemente libres de cualquier discriminación injusta"), disponible en *http://public.ansi.org/* ansionline/Documents/Standards%20Activities/American%20National%20Standards/Procedures,%20Guides,%20and%20Forms/ER2003.doc.

reclamar sus derechos sobre dicha patente a quienes habían implementado la norma adoptada[240].

Algunas entidades van más lejos e insisten en que si existe una reclamación de patente esencial, debe concederse una licencia sin pago de regalías. Por ejemplo, en mayo de 2003, el consorcio W3C publicó una política de patentes para garantizar que sus recomendaciones puedan implementarse sin pagar regalías[241]. El W3C intenta garantizar que no adoptará una recomendación si un participante tiene una reclamación de patente esencial sobre la que no concederá licencias sin cobrar regalías.

Las tecnologías propietarias (basadas o no en normas abiertas) se ofrecen mediante acuerdos negociados sobre licencias, que típicamente incluyen regalías, ámbito de utilización, derechos a futuros desarrollos y similares. Las licencias de algunas de las tecnologías de protección contra la copia, particularmente muchas de las desarrolladas por compañías fabricantes de equipos, se conceden generalmente con una orientación prácticamente "a costes", estando los costes administrativos cubiertos por las tasas cobradas.

Tanto para normas abiertas como propietarias, las licencias de normas y tecnologías DRM deben cumplir la ley aplicable, incluidas las leyes sobre la competencia de las jurisdicciones para las que se conceden las licencias de propiedad intelectual. Las leyes de la competencia son relevantes porque las leyes de propiedad intelectual confieren derechos exclusivos al titular de la propiedad intelectual y porque es importante impedir prácticas abusivas o ilegítimas relacionadas con la concesión de licencias. Varias jurisdicciones importantes han establecido directrices o regulaciones relativas a aspectos comunes de los acuerdos de concesión de licencias de tecnología y de propiedad intelectual[242], sobre que las leyes aplicables también se nutren de decisiones judiciales.

5.3 Asuntos de naturaleza política: el papel de la OMPI y de otras organizaciones internacionales

A la luz de los desarrollos comerciales, técnicos y jurídicos analizados en este informe, los autores han analizado posibles acciones o iniciativas que podrían tomar la OMPI y otras organizaciones internacionales, según convenga, para promover la aplicación efectiva de las disposiciones relativas a DRM de los Tratados de la OMPI sobre Internet. En coherencia con el mandato de la OMPI de "fomentar la protección de la propiedad intelectual en todo el

---

240 Véase *In the Matter of Dell Computer Corp.*, Decision and Order, No. C-3658 (May 20, 1996), versión disponible en *http://www.ftc.gov/opa/1995/11/dell.htm*.

241 Véase W3C Patent Policy (20 de mayo de 2003), disponible en *http://www.w3.org/Consortium/Patent-Policy-20030520.html*.

242 Véase, por ejemplo, U.S.A. Department of Justice and Federal Trade Commission, Antitrust Guidelines for the Licensing of Intellectual Property (6 de abril de 1995), disponible en *http://www.usdoj.gov/atr/public/guidelines/ipguide.htm*; Reglamento de la Unión Europea (EC) No. 240/96 de 31 de enero de 1996 relativo a la aplicación del apartado 3 del artículo 85 del Tratado a determinadas categorías del acuerdos de transferencia de tecnología, Diario Oficial L 031 , 09/02/1996; Japan Fair Trade Commission, Guidelines for Patent and Know-How Licensing Agreements Under the Antimonopoly Act (30 de julio de 1999), disponible en *http://www2.jftc.go.jp/e-page/guideli/patent99.htm*; Canada Competition Bureau, Intellectual Property Enforcement Guidelines (publicado el 21 de septiembre de 2000), disponible en *http://strategis.ic.gc.ca/SSG/ct01992e.html*.

mundo"[243], los autores de este informe sugieren que la OMPI tome en consideración las recomendaciones siguientes.

5.3.1 Diversidad de enfoques utilizados para la aplicación de los Tratados de la OMPI sobre Internet

En las secciones 3 y 5.1.1 de este informe se describen los diversos enfoques utilizados por gobiernos nacionales y por la Unión Europea para aplicar sus obligaciones derivadas de los Tratados de la OMPI sobre Internet. Tal como se ha señalado, hasta la fecha la legislación para la aplicación de éstos ha sido variada.

Primera Recomendación:

La OMPI podría realizar un estudio completo sobre los distintos enfoques posibles para la aplicación de las obligaciones derivadas de los Tratados de la OMPI sobre Internet. El estudio resumiría las opciones adoptadas por los legisladores al respecto y examinaría las consecuencias previsibles de los distintos enfoques sobre el alcance y la amplitud de la protección jurídica de las DRM y de los contenidos distribuidos mediante soluciones DRM.

5.3.2 Utilización de sistemas DRM y acceso a contenidos

Durante los debates nacionales y europeo sobre la aplicación de los Tratados de la OMPI, uno de los temas debatidos más intensamente es si las DRM y su desarrollo jurídico ulterior limitará el acceso legítimo de los consumidores a los contenidos. Está muy extendida la preocupación del posible "bloqueo" del acceso a las obras con derecho de autor, así como los temores de que se camina rápidamente hacia una sociedad de "pago por uso", incluso en las jurisdicciones que aún deben aplicar los Tratados de la OMPI y la Directiva de Derechos de Autor.

Tal como se ha señalado anteriormente, los Estados Unidos de América y la Comisión Europea han desarrollado mecanismos reglamentarios y gubernamentales para evaluar si el control de acceso está actualmente perjudicando, y en qué medida, a determinados hábitos que, aunque no expresamente autorizados por los titulares de derechos, se consideran "usos lícitos" o "excepciones" al derecho de autor. Estos mecanismos incluyen una revisión periódica realizada por la Oficina de Derechos de Autor de los Estados Unidos de América, así como informes periódicos y la supervisión y revisión por parte de la Comisión Europea. No obstante, los consumidores, bibliotecas, archivos y organizaciones educativas han expresado su preocupación sobre si la amplitud y la aplicación de autoridad que debe acompañar a estos procesos son las adecuadas para los ajustes que pueda ser necesario realizar de forma sincronizada.

Además de las actividades periódicas de supervisón de la Comisión Europea, no existen propuestas para examinar de forma sistemática los efectos actuales y futuros sobre los consumidores de los controles de acceso. Sin embargo, hasta la fecha, y salvo excepciones limitadas (como ocurre en relación con la CSS y los discos DVD), las medidas tecnológicas parecen no tener un efecto significativo sobre el derecho legítimo de los usuarios de acceder a

[243] Convenio que establece la Organización Mundial de la Propiedad Intelectual (OMPI), Art. 3.i).

obras con derecho de autor. Esta situación podrá cambiar (o no hacerlo) a lo largo del tiempo en función de cómo desplieguen las DRM los titulares de derechos. El impacto íntegro de estos efectos puede no ser bien entendido o evaluado dado lo restringido de los procesos hasta ahora implementados.

Segunda Recomendación:

La OMPI podría realizar periódicamente la tarea de recopilar datos o de revisar el grado de utilización de las DRM, así como la influencia que tienen las medidas tecnológicas en el acceso legítimo a obras protegidas por el derecho de autor. Dicha revisión no significaría necesariamente duplicar los mecanismos adoptados a nivel nacional y europeo. Esta tarea podría tener un alcance más abierto y analizar la situación internacional de forma más completa.

5.3.3 Excepciones o limitaciones legales a las disposiciones contra la elusión

Los Tratados de la OMPI no establecen nada sobre si la aplicación de los mismos requiere (o limita) la adopción de excepciones o limitaciones en relación con las obligaciones destinadas a garantizar que exista una "protección jurídica adecuada" y "recursos jurídicos eficaces" contra el abuso de las medidas tecnológicas. Sin embargo, tal como ilustra el análisis realizado en este documento, la aplicaciones legislativas incluyen excepciones o limitaciones que varían bastante entre sí, reflejando preferencias políticas diferentes y la influencia de determinados grupos de interés durante los trámites legislativos.

Algunas de dichas excepciones o limitaciones han sido expresas y otras implícitas; algunas se han incorporado en la parte vinculante del texto y otras en considerandos o comentarios complementarios; unas se aplican sólo a los usuarios (como es el caso de ciertos tipos de reproducción o copia privada) y otras se aplican a actividades concretas (tales como la ingeniería inversa y la prueba de computadoras); finalmente, determinadas excepciones o limitaciones sólo son aplicables a productos y dispositivos, como por ejemplo las disposiciones de "no-obligatoriedad" (para productos legítimos de electrónica de consumo, computadoras y telecomunicaciones) y las disposiciones relativas a la distribución de medios para garantizar la interoperabilidad entre programas de computadora.

En resumen, en el ámbito internacional e incluso regional, no existe uniformidad o armonización entre las excepciones o limitaciones aplicadas y, en consecuencia, se extraen dos consecuencias. En primer lugar, y al menos en cierta medida, los consumidores de contenidos idénticos (y para los cuales los titulares de derechos son los mismos) y protegidos por las mismas DRM, pueden tener capacidades jurídicas diferentes para acceder y utilizar dicho contenido libre de cualquier ley contra la elusión, dependiendo de si están incluidos en alguna excepción o limitación aplicable en el país donde residan.

En segundo lugar, las excepciones y limitaciones aplicables a los actos y herramientas de elusión afectan obviamente a la medida en que las DRM pueden proteger el contenido. En el futuro, cuando se hayan implantado las DRM y los usuarios y fabricantes de productos de electrónica de consumo y de productos de computación las invoquen, deberá entenderse cabalmente a nivel internacional cuáles son los efectos de dichas medidas. A modo de ejemplo, cuando una persona accede a un contenido o lo utiliza (a pesar de que exista DRM) realizando un acto legítimo de elusión en un país, dicho contenido podría ponerse a

disposición de usuarios en un ámbito mayor mediante su distribución a través de Internet o de cualquier otra forma.

Igualmente, un producto o programa informático capaz de eludir una medida tecnológica puede ser legal en un país porque, por ejemplo, tenga un propósito diferente a la elusión y la ley de dicho país solo prohíba los productos cuyo propósito exclusivo sea la elusión. Además, a pesar de que cuando se utiliza dicho producto en ese país para acceder a un contenido protegido mediante medidas tecnológicas, el contenido deja de estar protegido en el mismo y queda potencialmente sujeto a una redistribución de ámbito mundial, dicho contenido puede estar aún sujeto a usos no autorizados en algún otro país.

Este análisis sugiere que las excepciones y limitaciones deben redactarse con sumo cuidado, siendo de importancia vital que en las excepciones sólo tengan cabida determinadas actuaciones legítimas. Las directrices sobre cómo elaborar dichas excepciones o limitaciones pueden ser útiles no solo para reflejar necesidades legítimas de acceso y utilización, sino también para tener en cuenta las preocupaciones igualmente legítimas de los titulares de derechos sobre la amenaza que se cierne sobre contenidos que (en virtud de una excepción) escapan de las protecciones basadas en DRM.

Tercera Recomendación:

Conforme aumente la utilización de las DRM por los titulares de derechos, pueden resultar cada vez más significativas las excepciones o limitaciones a la aplicación de las disposiciones contra la elusión que se adopten en las distintas jurisdicciones. La OMPI podría analizar los efectos a nivel internacional de las disparidades entre dichas excepciones o limitaciones en relación con 1) personas que deseen hacer un uso legítimo de obras protegidas con derechos de autor invocando excepciones y limitaciones, 2) fabricantes de productos legítimos, y 3) titulares de derechos.

5.3.4 Modificación de los sistemas de canon por copia privada en la transición hacia la DRM

Tal como se ha señalado en 5.1.3, en varias jurisdicciones se han puesto en marcha cánones sobre dispositivos y medios en relación con la copia privada. Durante varios años, las discusiones se han centrado sobre las cuestiones siguientes: 1) si debería existir dicho canon; 2) si así fuera, sobre qué productos deberían imponerse; 3) la magnitud del canon, y 4) a quien debería pagarse el mismo. Tal como ha quedado patente en el análisis realizado sobre la Unión Europea, con la evolución del entorno digital, la potencial extensión del método del canon para a dispositivos y medios digitales, particularmente aquellos de carácter multifuncional, ha suscitado la preocupación sobre la equidad de tal medida entre consumidores e industrias tecnológicas. En particular, se ha argumentado que los consumidores no deberían pagar dos veces (una a través de un canon sobre un dispositivo y/o medio digital, y otra a través de un sistema de acceso DRM) para un mismo y único contenido. Por el contrario, se ha señalado que donde se mantienen y aumenta el grado de aplicación de los cánones, existen de hecho menos incentivos para el desarrollo y adopción de soluciones basadas en DRM.

Cuarta Recomendación:

La OMPI, a la luz de la eventual extensión de la adopción de tecnologías DRM en la economía mundial digital, podría evaluar el efecto de los diversos sistemas de canon por copia privada. En Europa se ha instado a la Comisión Europea para que ayude a los Estados Miembros a determinar cuándo y cómo se deben modificar los cánones en el proceso de transición a un entorno regido por las DRM. La OMPI podría jugar un papel neutral promoviendo encuentros de expertos para fomentar el intercambio de información que permita mejorar la comprensión cabal colectiva de las relaciones entre los cánones y las DRM. Dicho proceso sería útil para evaluar el ritmo con que deberían impulsarse las modificaciones y para el desarrollo de los mecanismos necesarios para realizarlas cómo y cuándo sea pertinente.

[Fin del documento]