S

OMPI

WCT-WPPT/IMP/3
ORIGINAL: Inglés
FECHA: 3 de diciembre de 1999

ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL
GINEBRA

TALLER SOBRE CUESTIONES DE APLICACIÓN DEL TRATADO DE LA OMPI SOBRE DERECHO DE AUTOR (WCT) Y EL TRATADO DE LA OMPI SOBRE INTERPRETACIÓN O EJECUCIÓN Y FONOGRAMAS (WPPT)

Ginebra, 6 y 7 de diciembre de 1999

LAS MEDIDAS TECNOLÓGICAS DE PROTECCIÓN: EL PUNTO DE ENCUENTRO DE LA TECNOLOGÍA, EL DERECHO Y LAS LICENCIAS COMERCIALES

Documento preparado por Dean S. Marks[*] y Bruce H. Turnbull[**]

[*] Asesor Jurídico Principal en Propiedad Intelectual, *Time Warner Inc.*, Burbank, California
[**] Socio, *Weil, Gotshal & Manges LLP*, Washington, D.C.

ÍNDICE

Conclusiones

Introducción[1]

Los adelantos de la tecnología tanto analógica como digital ofrecen a los propietarios del contenido nuevas posibilidades de distribución de sus obras, y a los consumidores nuevos medios de recepción y disfrute de éstas.[2] Sin embargo, estos adelantos también plantean una seria dificultad: ¿cómo se pueden proteger las obras en un mundo donde: i) la duplicación se puede hacer fácilmente y sin grandes costes; ii) cada copia realizada (ya sea del original o de otra copia) es perfecta; y iii) la distribución a los usuarios de todo el mundo se puede realizar prácticamente sin coste alguno y de forma inmediata por Internet? Este problema es particularmente grave en el mundo actual, donde un consumidor individual ya no sólo recibe obras, sino que también puede enviarlas y redistribuirlas a otros. El problema de la protección de obras se complica aún más debido a que, en la actualidad, las obras protegidas por el derecho de autor circulan en un entorno que engloba los dispositivos electrónicos para el consumidor, los ordenadores, los satélites y las redes mundiales como Internet.

A medida que los legisladores, los propietarios del contenido y los fabricantes de las empresas de la informática (soportes físicos y lógicos) y de la electrónica para el consumidor se han esforzado para enfrentarse a este problema, han surgido varias cuestiones. Primero, ni la tecnología sola, ni las medidas jurídicas solas pueden ofrecer una solución viable. Segundo, la evolución y la aplicación de tecnologías y estructuras de protección de ejemplares requieren cierta cooperación y cierto compromiso entre las empresas del contenido, de la electrónica para el consumidor, de la informática y otras. Tercero, la protección de ejemplares debe centrarse en dos cuestiones fundamentales: i) el tratamiento de obras que se encuentran en un dispositivo (por ejemplo, en lectores individuales, grabadoras u ordenadores), y ii) el tratamiento de obras que pasan de un dispositivo a otro (por ejemplo, de una caja de conexión a un aparato de televisión y a un dispositivo de grabación) y por redes alámbricas o inalámbricas (por ejemplo, Internet). Cuarto, la aplicación de la protección de ejemplares debe tener en consideración las expectativas razonables de los consumidores y el coste. Quinto, las tecnologías y las estructuras de protección de ejemplares deben tener en cuenta la innovación, la velocidad y la sinceridad que han marcado la revolución informática y de Internet. El problema de la protección adecuada de las obras es difícil y complejo; del mismo modo, las soluciones no son sencillas ni unidimensionales.

Los esfuerzos que actualmente se están haciendo para crear unas estructuras de protección de ejemplares han mostrado la necesidad de un enfoque ternario. El primer aspecto de este enfoque tiene que ver con el desarrollo de medidas tecnológicas de protección y la puesta a disposición de dichas medidas de una forma razonable. El segundo aspecto está relacionado con leyes que refuerzan las tecnologías de protección y prohiben la elusión de dichas tecnologías. El tercer aspecto tiene que ver con las negociaciones entre países y las

---

[1] Los autores participaron de forma activa en las cuestiones relativas a las licencias legislativas y tecnológicas que se discuten en este trabajo. Dean S. Marks participó en nombre de *Time Warner* desde la perspectiva de las empresas propietarias del contenido, y Bruce H. Turnbull en nombre de su cliente, *Matsushita Electric Industrial Co., Ltd.*, desde la perspectiva de la industria de la electrónica para el consumidor. Sin embargo, las opiniones expresadas en este trabajo son únicamente las de los autores y no reflejan necesariamente las posturas de las empresas o clientes respectivos.

[2] Este trabajo se centra en las obras audiovisuales y las grabaciones sonoras. No obstante, existen aspectos similares en cuanto a las obras escritas y literarias (incluidos los programas informáticos) y algunos de los principios generales que se examinan en este trabajo podrían ser pertinentes en esos contextos.

licencias de las medidas tecnológicas de protección. Estas licencias imponen obligaciones para asegurar que cuando se obtiene acceso a las obras protegidas por las medidas tecnológicas se siguen ciertas normas de control de utilización y de copias apropiadas. En este estudio se examinarán los tres aspectos y se explicará por qué todos estos elementos son necesarios.

Para dar un contexto a todas estas cuestiones, empezaremos haciendo una breve descripción de algunos de los acontecimientos que han dado lugar a esta problemática. A continuación analizaremos los tres aspectos desde una perspectiva general. A lo largo de nuestro análisis del segundo aspecto, expondremos nuestra opinión en lo referente al modo en que deberían aplicarse las disposiciones antielusión de los dos Tratados de la OMPI. Después, describiremos en detalle una serie de tecnologías y estructuras de protección de ejemplares que han aparecido recientemente, que están en estudio o que se están negociando. Aunque muchos asuntos en materia de política, de tecnología e incluso de derecho siguen sin resolverse, el trabajo finalizado hasta la fecha ha dado algunos resultados concretos, así como algunos puntos de referencia útiles para seguir adelante.

ANTECEDENTES: LOS AVANCES TECNOLÓGICOS QUE PLANTEAN EL PROBLEMA ACTUAL DE LA PROTECCIÓN DE OBRAS

A menudo, los avances tecnológicos son un arma de doble filo para los creadores y para los propietarios del contenido. Por un lado, proporcionan unas herramientas más sofisticadas para la creación y difusión legítima de obras. Por otro lado, esas mismas tecnologías a menudo facilitan la reproducción y distribución no autorizadas de obras, violando así los derechos de los propietarios del contenido. Este dilema no es nuevo: comenzó con la introducción de la imprenta. Sin embargo, en los últimos años, algunos avances tecnológicos han conferido un nuevo aspecto sorprendente al tema. Estos avances son los siguientes:

La copia digital: Las copias analógicas de obras audiovisuales pierden calidad con cada generación. Así pues, si alguien hace una copia de una cinta de vídeo analógica y se la da a un amigo, esa copia no será tan buena como el original. Si se hiciese una nueva copia a partir de aquella, la calidad sería aún peor. Así, la tecnología analógica tiene una barrera inherente contra las copias hechas a partir de copias que constituye un obstáculo para las copias en gran número no autorizadas de los consumidores. En cambio, la copia digital implica la reproducción bit a bit. Esto significa que cada copia es perfecta, y que se pueden hacer copias perfectas a partir de otras copias y así hasta el infinito. Además, las copias digitales se pueden hacer con gran velocidad y sin sufrir ninguna pérdida de calidad. Por lo tanto, con la llegada de la copia digital, el peligro de las copias no autorizadas es mucho mayor. Actualmente, la facilidad con la que una señal analógica se puede convertir a un formato digital y a continuación difundirla rápidamente supone que la entrega analógica también constituye un problema que debe tomarse en consideración en los esfuerzos para proteger los ejemplares.

La compresión: Las obras audiovisuales, al convertirlas a un formato digital de alta resolución, contienen cantidades enormes de datos. Antes de la tecnología de compresión digital, las obras de estas características requerían una anchura de banda considerable o intervalos de tiempo muy extensos para entregar algo a través de una red. Las tecnologías de compresión, como MPEG-2 para el vídeo y MP 3 para la música, han cambiado esta situación. Actualmente, algunas tecnologías de compresión permiten crear copias perfectas y sin pérdida alguna que ocupan menos del 25% del tamaño digital original. Esto significa que

estas copias se pueden entregar en un cuarto del tiempo que se tardaba en entregar los originales sin comprimir. Se prevé que aparezcan nuevas técnicas de compresión que permitan hacer copias sin que haya pérdidas y que ocupen el 5% del tamaño original. Y lo que es más importante, algunos métodos de compresión hacen copias de calidad algo inferior. Si bien no son reproducciones perfectas del original, estas copias suelen tener imperfecciones que no son perceptibles para el espectador o el oyente. Hoy en día, la compresión normal de este tipo permite hacer copias que ocupan menos del 2% del tamaño digital original, y los pronósticos prevén llegar a un 0,5% del original. Estos adelantos enormes de la tecnología de compresión significan que la transmisión de obras audiovisuales íntegras de alta calidad por redes como Internet resultará cada vez más sencilla, rápida y práctica.

La anchura de banda: El aumento de la anchura de banda significa que se dispone de mayor capacidad para entregar más datos con mayor rapidez. Para establecer las conexiones a Internet se están poniendo a disposición de los consumidores módem para cable y líneas de teléfono ADSL de alta velocidad. Estos servicios pueden entregar datos aproximadamente 9 veces más rápido que el módem para teléfono común de 56Kbaudios. Hay quien predice que en el futuro la capacidad de la anchura de banda aumentará hasta el punto de alcanzar velocidades que serán varios cientos de veces mayores que la de los módem corrientes actuales. Estos adelantos con respecto a la anchura de banda facilitarán enormemente la distribución de obras con una calidad excepcional a muchas personas en poco tiempo y con un coste reducido.

Las conexiones en redes: A medida que hay más personas “en línea”, se dan más conexiones en dos sentidos: desde el mundo exterior al hogar y al revés. Entre los usuarios existe cierta demanda de mayor interacción entre los dispositivos que compran, y por ello la conexión en redes de los dispositivos personales en el hogar (como ordenadores personales, televisores, grabadoras y cadenas de música) está aumentando. Ello permite que los usuarios reciban y manden obras desde casa y, al mismo tiempo, que pasen obras de un dispositivo a otro en sus hogares (por ejemplo, del ordenador personal a la grabadora digital). Todas estas conexiones hacen que para los no profesionales resulte sencillo hacer y distribuir múltiples copias de gran calidad de obras audiovisuales. De hecho, cada consumidor conectado a Internet puede convertirse en un reeditor no autorizado y distribuir obras.

Los adelantos tecnológicos mencionados significan que la piratería del contenido ya no necesita de piratas dedicados que usen un equipo caro para copiar obras, ni canales físicos de distribución (desde los mercados de baratijas a la venta por las esquinas o los comercios al por menor) para distribuir dichas copias no autorizadas. Actualmente, un consumidor individual con algunos miles de dólares invertidos en un equipo para su casa puede crear y distribuir un número ilimitado de copias de obras no autorizadas y de gran calidad.

PRIMER ASPECTO: LAS MEDIDAS TECNOLÓGICAS DE PROTECCIÓN: EL USO DE LA TECNOLOGÍA PARA RESOLVER LOS PROBLEMAS QUE ÉSTA PLANTEA Y LOS LÍMITES DE LAS TECNOLOGÍAS DE PROTECCIÓN DE EJEMPLARES

Una frase que a menudo se ha repetido en foros sobre políticas, y acuñada por Charles Clark, es que “la respuesta a una máquina se encuentra en ella misma”. En efecto, se ha creado toda una serie de medidas tecnológicas para ayudar en la protección de las obras. Estas medidas están descritas brevemente en el Anexo A. Si bien es cierto que las medidas tecnológicas existentes, y otras nuevas en estudio, se pueden usar para tratar algunos de los

problemas que plantean los adelantos de la tecnología digital y analógica que hemos descrito, la tecnología de protección de ejemplares sola no es la solución adecuada por varias razones.

En primer lugar, las medidas tecnológicas de protección, independientemente de lo potentes que sean, siempre serán vulnerables al ataque de piratas dedicados, en particular porque las capacidades de procesamiento de los soportes físico y lógico de los ordenadores sigue aumentando a gran velocidad. Por lo tanto, debe existir cierta protección legal contra la elusión de la tecnología de protección de ejemplares. Además, existen verdaderas restricciones económicas sobre la fuerza de las medidas tecnológicas de protección que se pueden aplicar a las obras protegidas por el derecho de autor y a los dispositivos de lectura. Así pues, las medidas tecnológicas de protección no pueden impedir la piratería por parte de individuos u organizaciones con recursos, sino que más bien su uso se limita a “hacer que la gente que sea honesta lo siga siendo”: a facilitar el respeto de los derechos de las obras, y a poner un obstáculo a aquellos que intentan violar esos derechos.

En segundo lugar, el público, al ver, oír y leer las obras de los propietarios del contenido hace que el valor de éstas aumente. Por lo general, los creadores quieren que haya quien aprecie sus obras, y tanto los inversores como los creadores dependen de un público amplio compuesto de consumidores legítimos y que paguen para mantener la creación y la distribución de obras. Las obras no son como el oro; de nada sirve guardarlas bajo llave en una cámara acorazada. Por lo tanto, la tecnología de protección de ejemplares debe aplicarse de tal modo que no interfiera en la distribución y la comunicación legítimas de obras al público. Este imperativo aumenta enormemente la complejidad de fomentar y utilizar la tecnología de protección de ejemplares. Ello significa que, en todas las cuestiones prácticas, las medidas de protección de ejemplares no pueden ser unilaterales. Sólo se podrá disfrutar de las grabaciones sonoras y de las obras audiovisuales mediante el uso de dispositivos de recepción y lectura, como televisores, lectores de discos y de discos compactos (CD), magnetoscopios, ordenadores personales, etc. Así pues, los propietarios del contenido no pueden aplicar a sus obras unas medidas tecnológicas que hagan que todos los dispositivos de recepción y lectura sean incapaces de recibir o leer sus obras. Igualmente importante es el hecho de que no se puede conseguir proteger las obras si los dispositivos de recepción, lectura y grabación no reconocen las tecnologías de protección de ejemplares y no responden a ellas, sino que sencillamente hacen caso omiso de ellas. Por lo tanto, para funcionar como es debido, las tecnologías de protección de ejemplares deben ser bilaterales: las tecnologías que los propietarios del contenido aplican deben funcionar con los dispositivos electrónicos e informáticos que usan los consumidores, y estos deben respetar las tecnologías utilizadas y responder a ellas. Este requisito bilateral significa que las soluciones no son sólo una cuestión de innovación tecnológica, sino más bien que para que la tecnología de protección de ejemplares sea eficaz, es necesario que los prestadores del contenido y los fabricantes de productos electrónicos e informáticos para el consumidor estén considerablemente de acuerdo y la apliquen ampliamente. Esto se puede conseguir mediante las legislaciones, en virtud de las cuales determinados tipos de dispositivos deben responder a una tecnología de protección de ejemplares concreta, o mediante acuerdos negociados entre las empresas.

En tercer lugar, la puesta en práctica de las tecnologías de protección se puede ver muy limitada si existe una serie de dispositivos para el consumidor ya instalados que no funcionen con dichas tecnologías. Por ejemplo, la música de los CD no está codificada. Si las compañías discográficas comenzasen a codificar la música de los discos compactos, éstos no funcionarían en los reproductores de CD que poseen normalmente los consumidores. El momento ideal para poner en marcha las tecnologías de protección de copias es con la

introducción de nuevos formatos o sistemas de entrega, como el Videodisco Digital (DVD) o las emisiones digitales.

En cuarto lugar, la tecnología no puede proteger de forma retroactiva el contenido que ya está en el mercado sin ninguna tecnología de protección de ejemplares. No obstante, este contenido desprotegido se puede manipular sin grandes dificultades para sacar provecho de los adelantos en la tecnología de copias y entrega. Actualmente, por ejemplo, los consumidores pueden grabar música de CD a discos vírgenes o cargarla en Internet. Es obvio que esta actividad infringe las leyes relativas al derecho de autor y los derechos conexos. Sin embargo, la cuestión es que la tecnología no puede hacer mucho - si es que hay algo que pueda hacer - para resolver este problema concreto.

Además de las limitaciones descritas antes, es poco probable que las protecciones tecnológicas se apliquen en todos los entornos y a todos los formatos. Por ello, siguen siendo indispensables regímenes jurídicos de legislación sobre derecho de autor y derechos conexos sólidos respaldados por una aplicación y unos recursos eficaces. Hace poco, el *Global Business Dialogue on Electronic Commerce* (GBDe) reconoció este imperativo.[3] En los principios y recomendaciones unánimes que publicó en París en septiembre de 1999 con respecto a la propiedad intelectual, el GBDe insistió en lo siguiente:

"El comercio electrónico no alcanzará su potencial máximo hasta que se resuelvan los problemas relativos a la observancia de las legislaciones sobre derecho de autor.

Acción necesaria por parte de los gobiernos:

- facilitar a los titulares de derechos unos medios eficaces y prácticos para continuar con las acciones de observancia del derecho de autor en cada jurisdicción en la que se den infracciones;
- fomentar una mejora de los procedimientos judiciales, los recursos y unas normas de responsabilidad factibles contra la infracción del derecho de autor en todos los países, con el objeto de conseguir una observancia eficaz y disuadir la infracción; y
- impulsar un programa de toma de conciencia sobre el derecho de autor entre organizaciones públicas, empresariales y educativas para educar a los usuarios acerca de la importancia de la protección del derecho de autor y la conformidad con las legislaciones de derecho de autor, las cuales, unidas, propician las actividades creativas".

Hemos determinado que la tecnología por sí sola no puede ofrecer una solución al problema de proteger las obras para que no se hagan copias de ellas en gran número sin autorización y que se distribuyan en los nuevos entornos. También hemos determinado algunas de las dificultades relacionadas con la aplicación de las tecnologías de protección de ejemplares. Estas limitaciones indican que deben proporcionarse garantías jurídicas concretas que refuercen las tecnologías de protección de ejemplares.

---

[3] El *Global Business Dialogue on Electronic Commerce* ("GBDe") representa la colaboración mundial entre empresas del ámbito del comercio electrónico. Varios cientos de empresas y asociaciones comerciales han participado en el proceso consultivo del GBDe; los representantes proceden de lugares y sectores distintos.

SEGUNDO ASPECTO: LEYES QUE REFUERZAN LAS TECNOLOGÍAS DE PROTECCIÓN: LA NECESIDAD DE LEYES EFICACES CONTRA LA ELUSIÓN Y LA APLICACIÓN DE LOS TRATADOS DE LA OMPI

Las medidas tecnológicas de protección necesitan un apoyo jurídico y legislativo adecuado, en primer lugar, para asegurar que se respetan dichas medidas y, en segundo lugar, para disuadir la anulación de estas medidas por parte de personas que, de otro modo, infringirían los derechos de los propietarios del contenido. Tanto en el Tratado de la OMPI sobre Derecho de Autor como en el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas se reconoce este imperativo. El Artículo 11 del Tratado de la OMPI sobre Derecho de Autor dispone que:

"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 los autores concernidos o permitidos por la Ley".

El Artículo 18 del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas contiene una disposición semejante.

Aunque los Tratados de la OMPI estipulan la prohibición general de la acción de elusión de las medidas tecnológicas de protección, se ha abierto un debate sobre cómo debería incorporarse este principio general en las legislaciones nacionales. Una buena parte del debate se ha centrado en tres cuestiones: i) si la prohibición debería aplicarse tanto a los dispositivos como a los comportamientos; ii) si se debería exigir que los equipos respondiesen a unas medidas de protección particulares; y iii) cuáles son las excepciones apropiadas a la prohibición del acto de elusión. A nuestro juicio, la Ley sobre Derecho de Autor para el Milenio Digital de 1998 (*Digital Millenium Copyright Act 1998- DMCA*) adoptada en los Estados Unidos de América (EE.UU.), halló una buena solución para cada una de estas cuestiones al incorporar las disposiciones contra la acción de elusión de los dos Tratados. No es nuestra intención aquí hacer una descripción detallada de la DMCA, sino que más bien nos inspiraremos en los conceptos y las soluciones de esta Ley en nuestro examen de los tres aspectos y en nuestra opinión en cuanto a los elementos necesarios para que las legislaciones contra la elusión sean efectivas y equilibradas.

El comportamiento y los dispositivos

Las disposiciones contra la acción de elusión de los dos Tratados de la OMPI no mencionan si se aplican sólo al comportamiento de elusión o si también se aplican a los dispositivos y servicios que se diseñan o distribuyen para anular las tecnologías de protección. Una concepción que sólo tenga en cuenta el comportamiento es insuficiente por varias razones. Por lo general, el comportamiento de elusión no es público; las personas normalmente lo llevan a cabo en la intimidad de sus hogares o lugares de trabajo. Si bien los resultados de esta actividad, como un programa informático de servicio que eluda una medida de protección de ejemplares, se pueden hacer públicos, el comportamiento que lleva a forzar el sistema de protección suele ser privado. No es factible ni deseable iniciar un control sistemático de los comportamientos privados para impedir las acciones de elusión. En todo caso, la mayoría de la gente desperdiciará su tiempo y esfuerzos en forzar una medida de protección de ejemplares por sí sola. No obstante, si se pueden adquirir de forma legal (o

recibir gratis) dispositivos o servicios que anulen estas medidas, es mucho más difícil mantener la integridad de las tecnologías de protección y que éstas cumplan su objetivo. Este concepto no es nuevo. Por ejemplo, muchos países prohiben la fabricación, la venta o la distribución de "tarjetas inteligentes" pirata o de cajas negras pirata que se usan para descifrar y obtener el acceso condicionado a emisiones de televisión por cable o por satélite sin autorización y sin pagar. En consecuencia, para proporcionar unos recursos efectivos contra la elusión, la ley debe proscribir los dispositivos y los servicios que se crean o se distribuyen con el objeto de eludir las tecnologías de protección.

El GBDe también recomendó que la legislación nacional que incorpore los dos Tratados de la OMPI debería "prohibir las actividades perjudiciales relacionadas con la elusión mediante la regulación del comportamiento y de los dispositivos, al mismo tiempo que establecer unas excepciones apropiadas... que mantuviesen un equilibrio global entre los titulares de derecho y los usuarios". (Añádase énfasis)

Aunque deben aplicarse a los dispositivos y servicios unas leyes efectivas contra la elusión, no es fácil establecer los límites sobre qué dispositivos y qué servicios deberían prohibirse. Los casos extremos son relativamente sencillos. No cabe duda de que las llamadas "cajas negras" que sirven únicamente, por ejemplo, para descifrar señales de televisión sin autorización (es decir, eludir el control de acceso a la codificación) o para anular las medidas de protección, son dispositivos que deberían ser ilegales. En el otro extremo están los ordenadores personales comunes, que a veces usan los piratas para forzar las medidas de protección de ejemplares que se incorporan a los soportes lógicos. A pesar de que dichos ordenadores a veces se utilizan con estos fines ilícitos, no deberían prohibirse por considerarlos dispositivos de elusión porque generalmente tienen funciones y fines totalmente legítimos. El problema es dónde trazar la línea entre estos dos extremos.

La mayoría de gente estaría de acuerdo en que la incorporación de un reloj en una "caja negra" no debería legitimar el dispositivo sencillamente porque las funciones de cronómetro de la parte del dispositivo donde se encontraría el reloj son legítimas. No obstante, no faltaría quien sostendría que un dispositivo que permita reproducir contenidos visuales analógicos a través de un ordenador cuya acción también tenga como resultado la eliminación de los indicadores de control de copias del contenido debería de estar permitido. En nuestra opinión, la DMCA consigue un equilibrio apropiado en esta materia tan delicada. Este equilibrio lo consigue, primero, estableciendo tres principios alternativos para determinar si el servicio o dispositivo debería prohibirse por su carácter elusivo. Después dispone que estos principios se pueden aplicar a una parte o a un componente de un dispositivo o de un servicio, y no sólo al dispositivo o servicio en su totalidad. Por lo tanto, un servicio o dispositivo, o una de sus partes o componentes, que corresponda a cualquiera de las siguientes categorías está prohibido:

- está diseñado o producido, ante todo, para llevar a cabo una acción de elusión;
- tiene un fin o uso comercial distinto de la elusión limitado; o
- se ha comercializado para llevar a cabo acciones de elusión.

Un dispositivo, servicio, parte o componente que corresponda a cualquiera de las categorías enunciadas arriba está prohibido y no se puede fabricar, importar, vender ni distribuir. La segunda parte del equilibrio la da la disposición de "no obligatoriedad" que se analiza más abajo. Este planteamiento puede constituir un modelo útil para otros países cuando incorporen a sus legislaciones nacionales las disposiciones contra la elusión de los

Tratados de la OMPI. Consideramos que es necesaria una estrategia en esta línea con respecto a las legislaciones contra la elusión para proporcionar un apoyo legal adecuado a las medidas tecnológicas de protección.

La respuesta a tecnologías de protección concretas

Actualmente, las tecnologías de protección de ejemplares están repartidas entre dos categorías generales: las medidas que controlan el acceso al contenido, como la codificación, y las medidas que controlan las copias del contenido, como SMCS o Macrovision.[4] Las tecnologías de control del acceso, como la codificación, tienden a plantear situaciones bien definidas con respecto a la aplicación de leyes contra la elusión. Si el contenido está codificado, un dispositivo de lectura o grabación puede pasar el contenido codificado sin descodificarlo, o puede descodificarlo para que el usuario final pueda acceder a él y verlo. Esta descodificación no puede darse de forma casual. Para llevar a cabo la descodificación es necesario que el dispositivo lleve a cabo una acción afirmativa que "desbloquee" el control del contenido y lo haga accesible. Por lo tanto, la descodificación sin autorización es una acción de elusión.[5]

Las tecnologías que controlan la copia del contenido, como los indicadores de control de copias, plantean cuestiones más complejas con respecto a la aplicación de las leyes contra la elusión. Ello se debe a que el funcionamiento satisfactorio de dichas tecnologías suele depender de una respuesta del dispositivo de lectura o grabación. En el caso de la codificación, si el dispositivo de lectura no responde afirmativamente para desbloquear - descodificar - el contenido, éste permanece codificado y protegido. Sin embargo, en el caso de los indicadores de control de copias, si el dispositivo no busca y responde afirmativamente a los indicadores, el contenido no está protegido y puede ser objeto de una copia no autorizada.

Algunas de las tecnologías de protección de ejemplares más avanzadas que se usan actualmente, como SCMS y Macrovision, no funcionan con eficacia en los ordenadores personales. No es tanto que los ordenadores anulen o supriman estas protecciones, sino más bien que no las "buscan" ni responden a ellas. Las empresas de informática opusieron una gran resistencia a la idea de cualquier orden legislativa que exigiese que los ordenadores personales se diseñasen para buscar y responder a unos indicadores o unos bits de control de copias concretos. La industria informática está especialmente en contra de la idea de obligar a un ordenador a analizar todos los flujos de datos que llegan en busca de dichos indicadores o bits. Este motivo de preocupación lo es aún más dada la posibilidad de que los ordenadores deban responder a todas y cada una de las tecnologías de protección de ejemplares que cualquier propietario del contenido decida adoptar. La industria de la electrónica para el consumidor comparte esta preocupación.

---

[4] En el Anexo A se presentan descripciones de la codificación, el SCMS y Macrovision.

[5] Todas las estructuras de protección de ejemplares descritas más adelante que se han aplicado recientemente o que están en proceso de negociación entre las empresas se basan en la codificación del contenido. Esta es precisamente la razón por la que el contenido codificado no se puede descodificar "por casualidad". Los fabricantes de productos legítimos que deciden participar en las estructuras de protección de los ejemplares "se inscriben", obtienen una licencia y aceptan seguir las normas de protección de los ejemplares como condición para obtener las claves que descodifican el contenido. Llevar a cabo dicha descodificación sin autorización (es decir, sin una licencia) constituye claramente el tipo de actividad que, en general, las legislaciones contra elusión deben prohibir.

Así pues, un aspecto fundamental que ha surgido en el debate sobre el alcance y las condiciones de unas leyes contra la elusión adecuadas es si el hecho de que no haya respuesta ante una tecnología de protección de ejemplares constituye un acto de elusión. Es comprensible que los fabricantes de equipos no quieran ser responsables de asegurar que sus dispositivos son capaces de responder a toda una serie de tecnologías de protección de ejemplares conocidas e incluso desconocidas. En cambio, los propietarios del contenido consideran, con razón, que no debería permitirse que los fabricantes de equipos diseñen sus productos de tal forma que estos eviten o pasen por alto las tecnologías de protección. Este asunto espinoso quedó resuelto en la DMCA mediante la promulgación de la llamada disposición de "no obligatoriedad". Esta disposición aclara que la prohibición de los dispositivos de elusión no obliga a los fabricantes de productos electrónicos, de telecomunicaciones o de informática para el consumidor a diseñar dichos productos o a seleccionar partes o componentes que respondan afirmativamente a cualquier medida tecnológica concreta, siempre y cuando el producto o la parte de éste no infrinja ninguna de las prohibiciones de los tres principios alternativos descritos más arriba (es decir, que el producto o una de sus partes estén diseñadas o producidas principalmente para la elusión; que tenga un fin comercial distinto de la elusión limitado; o que se comercialice para llevar a cabo acciones de elusión).[6]

Excepciones consideradas pertinentes

Generalmente, las legislaciones nacionales establecen algunas limitaciones y excepciones a los derechos de los autores y a los titulares de derechos conexos, como el uso lícito/prácticas lícitas. El Convenio de Berna y los dos Tratados de la OMPI adoptados en 1996 presentan algunas pautas en lo relativo a las excepciones y las limitaciones de los derechos. Por lo general, estas excepciones y limitaciones sólo se pueden prever "en ciertos casos especiales que no entren en conflicto con la explotación normal de la obra ni causen un perjuicio injustificado a los intereses legítimos del autor" o de los titulares de derechos conexos.[7]

Con frecuencia se ha expresado el temor de que la evolución de las medidas tecnológicas de protección lleve a que los propietarios del contenido "bloqueen" sus obras e impidan que los usuarios puedan hacer valer las excepciones legítimas a los derechos de dichos propietarios. Este temor puede ser alarmista por varias razones. Primero, los propietarios del contenido suelen depender de un consumo público amplio de sus obras. Así pues, incluso si algunas versiones o formatos de estas obras están asegurados mediante tecnologías de protección, estas tecnologías deben ser lo suficientemente transparentes para permitir un acceso fácil cuando se trate de usos autorizados. Segundo, asegurar la disponibilidad de las obras con fines públicos, como es el caso de bibliotecas, archivos y escuelas, es algo que se puede organizar fácilmente mediante acuerdos de licencia o incluso

---

[6] En este estudio sólo nos referimos a las leyes contra la elusión. En algunos casos, otras leyes exigirán que se diseñe el equipo para responder a tecnologías de control de ejemplares concretas. La DMCA, por ejemplo, contiene una provisión en virtud de la cual los magnetoscopios analógicos deben responder a Macrovision.

[7] Véanse los Artículos 9 (2), 10 y 10 bis del Convenio de Berna, el Artículo 10 del Tratado de la OMPI sobre Derecho de Autor y el Artículo 16 del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas.

mediante leyes concretas. Las restricciones aplicadas a las medidas tecnológicas de protección no constituyen un método necesario (ni siquiera muy eficaz) de tratar estas cuestiones. Además, las medidas tecnológicas funcionan sea cual sea el modelo económico que se aplique al contenido y a un usuario concreto. Así pues, las bibliotecas, por ejemplo, podrán obtener licencias para acceder al contenido a un precio reducido o incluso gratuitas en los casos en los que, de hecho, las medidas tecnológicas ayudan a dar cabida a dichas licencias al permitir que la biblioteca use el contenido pero impidiendo las copias no autorizadas y la redistribución de aquél. Tercero, es improbable que se apliquen las medidas tecnológicas de protección a todos los formatos. Por último, las medidas tecnológicas en realidad pueden facilitar determinadas excepciones y limitaciones a los derechos de los propietarios del contenido mediante, por ejemplo, una tecnología que permita realizar sólo una copia de la obra. No parece insensato aplicar ciertas limitaciones en lo referente a permitir excepciones a la elusión de las medidas tecnológicas hasta que el mercado de estas medidas esté más avanzado y si no surge ningún problema concreto.

Los Tratados de la OMPI no prevén de forma específica ninguna excepción a la obligación de proporcionar una protección legal adecuada contra la elusión. Cualquier excepción posible a la legislación contra elusión debe redactarse de forma restringida y limitarla a los casos especiales que no impidan el funcionamiento normal y la aplicación de las tecnologías de protección, y que no perjudiquen injustificadamente los intereses legítimos de los propietarios del contenido cuando utilicen estas tecnologías. Puesto que, por su naturaleza, los dispositivos y los servicios no se pueden limitar a usos particulares, las excepciones a las leyes contra la elusión no parecen muy adecuadas para estos dispositivos y servicios. Es mejor considerarlas en relación con determinados tipos de comportamiento individual y sujetas a una serie de condiciones razonables. Los legisladores deberían hacer muestra de cautela y servirse de parámetros como: i) la disponibilidad general de las obras (no de los formatos individuales); ii) las repercusiones que cualquier posible excepción a las normas contra elusión pueda tener sobre el valor de las obras y la eficacia de las tecnologías de protección; y iii) la existencia de acuerdos de licencia entre los titulares de derecho y las bibliotecas públicas o los archivos al considerar excepciones posibles. Por último, los legisladores deberían también examinar las posibilidades de hacer copias que, en la práctica, se están incorporando a las estructuras en estudio de protección de ejemplares. Las medidas tecnológicas pueden resultar útiles al facilitar el establecimiento de ciertas excepciones y limitaciones a los derechos de los propietarios del contenido. Si en la práctica esto funciona, no habrá mucha necesidad de establecer excepciones a la norma general contra la elusión de dichas medidas.

La DMCA prevé algunas limitaciones restringidas de la prohibición general de elusión, así como algunas excepciones a la misma. Primero, la prohibición del comportamiento elusivo individual sólo se aplica con respecto a las tecnologías de protección del acceso y no a las que impiden copiar. También se prevén otras limitaciones y excepciones: i) la observancia de la ley y otras actividades gubernamentales; ii) las bibliotecas, archivos e instituciones educativas sin ánimo de lucro, con el único objeto de decidir si desean obtener un acceso autorizado a las obras; iii) invertir la técnica únicamente para conseguir interoperabilidad; iv) la investigación en materia de codificación y las pruebas de seguridad; y v) la protección de la intimidad y de los menores. Las excepciones mencionadas están confeccionadas de forma restringida y contienen condiciones cuyo objeto es mantener un equilibrio e impedir que las excepciones anulen las normas generales contra la elusión.

Cada país tiene sus inquietudes particulares en lo que se refiere a las excepciones y las limitaciones. En nuestra opinión, debe prestarse una atención especial a dichas inquietudes. Las medidas tecnológicas y los dispositivos de elusión no pueden distinguir si el fin de carácter elusivo es legal o no. Toda excepción o limitación posible de la norma contra elusión debería aplicarse a determinados tipos de comportamiento individual y claramente definido. La prohibición de dispositivos y servicios de elusión debe seguir siendo firme y no puede verse debilitada. Hasta la fecha, las medidas tecnológicas de protección no han impedido el uso lícito o la práctica lícita con respecto a las obras y no ha habido muestra alguna de que dichas medidas tengan este efecto en el futuro. Nuestro trabajo en el ámbito de las protecciones tecnológicas nos ha llevado a la conclusión de que las legislaciones contra elusión deben disuadir de forma efectiva contra la elusión y proporcionar recursos suficientes para corregirla. Unas leyes firmes y efectivas en este ámbito son fundamentales, porque las medidas tecnológicas sólo sirven de obstáculo al uso no autorizado y siempre se podrán eludir.

Las estructuras de protección de ejemplares descritas más adelante dependen de las tecnologías y de los acuerdos de licencia. Unas leyes contra elusión efectivas son fundamentales para asegurar que estas estructuras y estos acuerdos no queden debilitados por quienes deciden no participar en los acuerdos o incumplirlos. Las leyes deberían estimular la participación y la adhesión a dichos acuerdos y estructuras e impedir que quienes han decidido no formar parte puedan competir de forma desleal anulando las medidas tecnológicas de protección. Puesto que las obras y las tecnologías de protección atraviesan las fronteras con mayor frecuencia cada vez, es fundamental que tantos países como sea posible pongan en práctica correcta y velozmente las disposiciones contra la elusión de la OMPI.[8]

TERCER ASPECTO: NEGOCIACIONES Y LICENCIAS EN EL SECTOR EMPRESARIAL: EL DESARROLLO DE LAS ESTRUCTURAS DE PROTECCIÓN DE EJEMPLARES

Las medidas tecnológicas de protección constituyen el primer aspecto de las estructuras de protección de ejemplares, aunque hemos descrito el modo en que toda una serie de limitaciones del mundo real impiden que estas medidas tecnológicas proporcionen una solución global. A continuación examinamos el segundo aspecto de la protección de ejemplares, a saber, las medidas legales y, en particular, las leyes contra la elusión. Explicamos por qué son necesarias unas leyes firmes y efectivas contra la elusión que contribuyan a la eficacia de las medidas tecnológicas. Ahora nos fijaremos en el tercer aspecto de la protección de ejemplares: los acuerdos y estructuras en el sector empresarial en virtud de los cuales se ponen en práctica las medidas tecnológicas de protección y se establecen normas para el tratamiento adecuado del contenido mediante el uso de acuerdos comerciales de licencia.

[8] Un ejemplo reciente justifica la urgencia. Hace poco, en Noruega, se pirateó el sistema de codificación que protege los DVD y se publicó en un sitio Web a partir de un servidor situado en este país, el cual, al igual que muchos otros, aún no ha promulgado ninguna ley contra la elusión como lo prescriben los Tratados de la OMPI.

Primeros intentos

Los primeros intentos de aplicar unas medidas de protección de ejemplares tuvieron un alcance algo limitado. Un ejemplo de ello es el sistema SMCS[9] creado para la música en formato digital, que permite hacer una primera generación de copias grabaciones en formato digital en un número ilimitado, pero impide la realización de una segunda generación de copias o las copias en serie (es decir, se permite hacer un número ilimitado de copias a partir del original, pero no se puede hacer ninguna a partir de esas copias). La aplicación a escala mundial del SCMS fue el resultado de las negociaciones y el acuerdo posterior entre las compañías discográficas y los fabricantes de productos electrónicos para el consumidor en 1989. En algunos países, como los Estados Unidos, se acabaron promulgando algunas leyes que exigían que los dispositivos electrónicos para el consumidor respondiesen al SCMS. No obstante, los acuerdos y las leyes relativos al SCMS no incluyeron al sector de la informática. En consecuencia, los ordenadores personales que actualmente pueden leer y grabar música en formato digital no están obligados a adherirse al SCMS.

La codificación de ciertas emisiones televisivas, en particular las que se hacen por satélite o por cable, constituye otro ejemplo. La codificación se creó con el objeto de asegurar que sólo los consumidores que están autorizados (es decir, que han pagado para estar suscritos) pueden descodificar las emisiones y ver los programas. Según la están aplicando las empresas de la industria del cable y del satélite, la tecnología de la codificación sólo protege la programación hasta que llega a la caja de conexión del consumidor autorizado. Cuando se ha descodificado la señal, el consumidor tiene a su disposición el contenido sin más protecciones tecnológicas que impidan la copia o la redistribución sin autorización.

Acciones actuales y principios generales

El objetivo de los intentos actuales de idear y aplicar unas estructuras de protección de ejemplares es sanar algunas de estas deficiencias. Los propietarios del contenido son conscientes de la importancia de establecer algún tipo de medida de protección en los distintos entornos: medios físicos, emisiones, Internet, etc. También entienden la necesidad de trabajar con las empresas de productos electrónicos para el consumidor, las informáticas y quizás las de las telecomunicaciones, para crear y aplicar unas tecnologías de protección y unas normas de utilización del contenido. La toma de conciencia de estos hechos ha llevado a fijar los siguientes objetivos y principios generales que orientan los esfuerzos actuales de protección de ejemplares:

Participación voluntaria en la estructura de protección de la ejemplares. No debería exigirse a los proveedores del contenido que usen una tecnología de protección de ejemplares. En general, los fabricantes de dispositivos deberían ser libres de decidir si desean participar en una estructura de protección de ejemplares. Si, a pesar de todo, deciden no hacerlo, entonces sus productos no deben eludir ni interferir con la tecnología de protección de ejemplares.

El contenido debe estar codificado. La codificación del contenido es fundamental para distinguir claramente los usos autorizados de los no autorizados, en particular en entornos informáticos. Ninguna persona ni ningún dispositivo puede descodificar el contenido “por

[9] Véase la descripción del SCMS en el Anexo A.

casualidad". Por lo tanto, la codificación del contenido es la piedra angular de los esfuerzos actuales de la protección de ejemplares.

Las licencias de codificación/ descodificación deben imponer unas normas de protección de ejemplares. La codificación y la descodificación del contenido exige que exista una licencia de la tecnología de codificación pertinente. Esta licencia dispondrá ciertas obligaciones sobre qué normas de protección de ejemplares deben respetarse (por ejemplo, prohibido copiar, sólo se permite una copia, etc.) como condición para descodificar el contenido y para que el usuario pueda acceder a él. Estas normas deben hallar el equilibrio entre los derechos de los propietarios del contenido y unas expectativas razonables del consumidor. Cuando se ha codificado el contenido, todo dispositivo con licencia que lo descodifique asume las obligaciones contractuales que la licencia prevé para respetar las normas de protección de ejemplares. Lo ideal sería que el contenido tuviese impresas con filigrana las condiciones de utilización y las normas de protección de ejemplares. Cualquier dispositivo no autorizado puede transmitir el contenido codificado sin limitaciones, siempre y cuando dicho dispositivo no descodifique o dé acceso al contenido de cualquier otro modo. Todo dispositivo no autorizado que descodifique el contenido infringe la legislación contra elusión (así como todo derecho de propiedad de los propietarios de la tecnología de codificación).

Aplicación a dispositivos y sistemas. Una protección efectiva de los ejemplares requiere una aplicación de la tecnología y unas obligaciones de protección de dichos ejemplares válidas para todos los dispositivos y servicios que pueden leer, grabar y/o transmitir un contenido protegido. Dadas las realidades del entorno de las redes y de Internet, todos los dispositivos y "paradas en el recorrido" de los sistemas de distribución deben mantener el contenido tan seguro como lo recibieron y no eludir protecciones ni pasar el contenido al siguiente dispositivo o componente fuera de peligro. Esto significa que estos dispositivos y sistemas no pueden pasar un contenido que se haya descodificado de forma legítima a través de conexiones analógicas o digitales a otros dispositivos y sistemas sin las protecciones adecuadas.

Control de grabación y lectura. Los dispositivos y sistemas no deben leer a partir de medios con función de grabación un contenido (música o imágenes) en el que haya impresa con filigrana una prohibición de copiar.[10] Si existe una impresión de este tipo en los medios con función de grabación, esto significa en primer lugar que la grabación no estaba autorizada. Del mismo modo, no debería poder leer ningún contenido de una copia que se haya hecho a partir de un contenido que se haya copiado una vez. La solución ideal sería que los dispositivos de grabación leyesen y respondiesen a las impresiones con filigranas y que no hiciesen ninguna copia de un contenido en el que se indique que está prohibido copiarlo.

Disponibilidad de las tecnologías de forma razonable y no discriminatoria. Las medidas tecnológicas de protección tienen que estar disponibles para un público amplio de una forma justa y no discriminatoria para que todas las partes pertinentes las puedan aplicar (por ejemplo, los fabricantes de soportes físicos, los propietarios del contenido y los operadores de sistema).

[10] Véase la descripción de la impresión con filigrana en el Anexo A.

Mantener una protección útil. Los sistemas y las tecnologías de protección de ejemplares deben proteger las obras de una forma útil y continua. Por lo tanto, estos sistemas deberían permitir la revocación de dispositivos comprometidos o clonados. Además, las tecnologías incorporadas a estos sistemas deberían poderse renovar para que un solo ataque de un pirata informático no destruya la eficacia del sistema.

Si bien el enunciado de los objetivos citados es relativamente sencillo, su puesta en práctica en estructuras de protección de ejemplares reales no ha resultado nada fácil. A continuación analizamos de forma detallada la creación y la aplicación de algunas de estas estructuras, empezando por el Videodisco Digital (DVD).

La introducción del Videodisco Digital (DVD)

La introducción del DVD facilitó la situación para la aparición de algunos de los métodos actuales de aplicación de las tecnologías de control de ejemplares. El DVD proporciona imágenes de vídeo de gran calidad en un formato muy práctico de disco de 5 pulgadas que no se daña con el uso y que tiene propiedades atractivas para el usuario, como versiones en varias lenguas extranjeras. El DVD se creó y diseñó para que tanto los dispositivos electrónicos para el consumidor como los ordenadores personales pudieran leerlo. La industria de dispositivos electrónicos para el consumidor y la industria informática se impacientaban por que se introdujera este nuevo formato para las películas. Desde el punto de vista de los productos electrónicos para el consumidor, el mercado del magnetoscopio analógico estaba bastante asentado y el DVD ofrecía una nueva generación de lectores que podían obtener una amplia popularidad entre los consumidores y generar unas ventas de equipos considerables. Desde el punto de vista de la informática, el DVD suponía una oportunidad para que el ordenador personal se introdujese también en los hogares como un dispositivo de lectura de películas. No obstante, los estudios cinematográficos no estaban dispuestos a estrenar películas en este formato digital nuevo sin contar con alguna protección contra la copia y la distribución no autorizadas, en particular la copia y la distribución digitales. Puesto que el DVD era un formato nuevo, constituía la oportunidad ideal para incorporarle una tecnología de protección de ejemplares. No existía ningún soporte instalado de lectores de DVD ni ningún lector DVD para los ordenadores personales; en consecuencia, se podían diseñar e incorporar medidas de protección de ejemplares en estos nuevos dispositivos desde un principio.[11]

Orígenes del CPTWG y de la protección contra la copia de DVD

En la primavera de 1996 se hizo obvia la necesidad de un grupo que propiciase los debates sobre la protección de ejemplares entre estas tres industrias dispares, cuando la asociación mercantil que representaba a los estudios cinematográficos más importantes y la que representaba a los fabricantes de la industria electrónica para el consumidor presentaron al sector de la informática una propuesta conjunta de legislación. Según esta propuesta, todos

[11] Las limitaciones existen incluso en este estadio ideal de introducción de un nuevo formato. Por ejemplo, para tener éxito en el mercado, los lectores de DVD tenían que ser compatibles con los soportes existentes ya instalados de los televisores. Por lo tanto, la tecnología de protección de ejemplares adoptada tenía que prever que los discos DVD utilizados con lectores legítimos se pudiesen ver en los televisores existentes.

los dispositivos que pudiesen realizar grabaciones digitales de películas tendrían que buscar, leer y responder a cierta información relativa a la protección de ejemplares que debería encontrarse en el contenido, ya fuese a partir de discos DVD, de otros formatos físicos, o de transmisiones, como las emisiones. Las empresas informáticas respondieron de forma unánime, inmediata y enérgica que esta estrategia con respecto a la protección de ejemplares era contraria a su opinión acerca del papel apropiado del gobierno (es decir, que no debía implicarse en el diseño de productos informáticos), impracticable desde el punto de vista técnico sin paralizar el funcionamiento de productos informáticos, y demasiado insegura para justificar cualquier esfuerzo especial por parte de las compañías informáticas para dar cabida al sistema.

Enfrentadas al lanzamiento inminente de lectores DVD de varias compañías de productos electrónicos para el consumidor, el deseo de éstas de contar con discos DVD pregrabados con películas, la insistencia de las compañías cinematográficas de que se diese una protección adecuada a todo contenido que se encontrase en los discos DVD, y el punto muerto en el que se encontraba la propuesta legislativa, hicieron que las tres industrias formaran dos grupos de trabajo. Uno de ellos se centró en cuestiones en materia de política y el otro en cuestiones técnicas; éste último adoptó el nombre de Grupo Técnico de Trabajo sobre la Protección de Ejemplares (*Copy Protection Technical Working Group - CPTWG*). El grupo de trabajo en materia de política se reunió en algunas ocasiones, pero no logró hacer ningún progreso significativo acerca de enfoques legislativos que fuesen aceptables para el sector de la informática o suficientes con respecto a los objetivos de protección de ejemplares de la industria cinematográfica. Así pues, la acción principal se concentró en el grupo técnico.

A partir de la primera semana de mayo y hasta mediados de julio de 1996, el CPTWG y su equipo operativo sobre el DVD se reunieron casi semanalmente, y atrajeron a participantes de los Estados Unidos de América, el Japón y Europa a casi todas las reuniones. La industria informática insistió en que la codificación del contenido debía ser el punto de partida de cualquier estructura de protección de ejemplares. En un principio, el sector de productos electrónicos para el consumidor se opuso a esta concepción porque le preocupaba que la codificación exigiese demasiado de sus dispositivos, lo cual haría que fuesen más complejos y caros. No obstante, tras varias reuniones, dos compañías, *Matsuhita Electric Industrial Co., Ltd.* (“MEI”, fabricante y distribuidor de productos con las marcas Panasonic, Quasar y National) y *Toshiba Corporation*, propusieron un método de protección de ejemplares que: i) estaba concebido específicamente para el formato DVD; ii) cumplía las condiciones de diseño de la industria de productos electrónicos para el consumidor; iii) cumplía el criterio básico del sector de la informática acerca de la protección de la codificación del contenido; y iv) impondría una serie de normas, cuyo cumplimiento se podía exigir legalmente, contra la copia y la transmisión sin autorización a un nivel que la industria cinematográfica podía aceptar mediante un acuerdo comercial privado de licencia.

Los objetivos básicos que se exigían de esta tecnología de protección de ejemplares y estructura de licencias eran los siguientes:

Suficiente protección tecnológica y jurídica para que la gente “que era honesta lo siguiese siendo”, es decir, hacerle difícil a un consumidor común que utilice dispositivos que se suelen encontrar en los hogares la realización de una copia a partir de un contenido protegido;

Suficiente protección tecnológica y jurídica para impedir la creación sin dificultad de medios utilizables y disponibles de forma amplia de eludir las protecciones tecnológicas y jurídicas que proporcionan las licencias tecnológicas y otras relacionadas;

Aplicación de esta tecnología a los productos informáticos y a los productos electrónicos para el consumidor para que el efecto no sea excesivamente gravoso en complejidad y coste en ambos entornos;

Licencias tecnológicas que puedan prestar las protecciones jurídicas necesarias con respecto a los fabricantes y distribuidores de dispositivos y que les resulten poco gravosas; y

Operaciones transparentes para los consumidores, excepto en los casos en los que los consumidores intentan realizar copias sin autorización de contenido protegido usando el sistema.

Por último, un principio de partida fundamental era que una compañía cinematográfica o de dispositivos no estaba obligada a usar las licencias tecnológicas y otras conexas. Se pueden crear y lanzar al mercado, y así se ha hecho, tecnologías de protección de ejemplares alternativas para el DVD.[12]

La propuesta de tecnología de MEI y Toshiba se examinó en estrecha colaboración con otros participantes del CPTWG y se presentó en un principio al *DVD Consortium* para asegurarse de que los creadores del formato DVD apoyarían la adopción de dicha tecnología como compatible con este nuevo formato. A continuación, MEI y Toshiba presentaron la propuesta a todo el CPTWG a mediados de julio, a lo que siguieron tres meses más de intenso trabajo, durante los cuales se perfeccionó la tecnología y se debatieron las normas de uso para asegurar que la protección era adecuada desde la perspectiva de las compañías cinematográficas y razonable desde la de las empresas que incorporarían dicha tecnología en sus productos.

La mejora de la tecnología consistió, entre otras cosas, en una evaluación atenta por parte de compañías informáticas para asegurarse de que la aplicación de las funciones de codificación en los soportes lógicos era razonable en cuanto a capacidad de procesamiento necesaria. Puesto que la producción de MEI y Toshiba se orientaba a circuitos semiconductores y otros productos de soporte físico para el diseño de dispositivos, en un principio el sistema se había optimizado para aplicarlo a los soportes físicos. Las compañías informáticas principales no tardaron en ver que este sistema no era óptimo para la descodificación de soportes lógicos y que lo que entonces era un ordenador personal normal no podría llevar a cabo la descodificación en el soporte lógico sin utilizar toda o prácticamente toda la capacidad de procesamiento de ese ordenador. Varias compañías informáticas consiguieron la descripción, muy confidencial, de la tecnología mediante unos acuerdos de confidencialidad y no divulgación y se pusieron a trabajar para encontrar un modo de adaptar la tecnología para que su incorporación a los ordenadores fuese aceptable. Estas revisiones se presentaron al CPTWG para su debate. El resultado fue un acuerdo unánime de que la versión revisada presentaba suficiente protección contra las copias por parte de los consumidores. Esta versión revisada de la tecnología, llamada Sistema de Cifrado del Contenido (*Content Scramble System -CSS*), se convirtió así en el sistema a partir del cual

[12] La alternativa más evidente que se ha introducido ha sido el sistema DIVX, patrocinado por *Circuit City* y un grupo de inversores privados.

se crearía una protección para el DVD. En el Anexo B damos una descripción más detallada de la tecnología CSS y de su funcionamiento.

Tras haberse puesto de acuerdo en utilizar el CSS para codificar el contenido audiovisual de los discos DVD, las empresas debían negociar las condiciones que regirían la descripción y la lectura del contenido de los discos. Debe subrayarse que el objeto de distribuir imágenes en DVD es que los consumidores vean las películas y disfruten con ellas. Ni a los consumidores ni a las empresas les interesaría que el contenido permaneciese codificado y no se pudiese ver. Por lo tanto, las negociaciones se centraron en cómo los dispositivos de lectura (tanto los de la industria electrónica para el consumidor como los informáticos) deben tratar el contenido de los discos DVD cuando ya está descodificado. Las empresas estuvieron de acuerdo, en principio, en que el contenido audiovisual de los discos DVD no debería ser objeto de copia o transmisión no autorizadas, así como de puesta a disposición del contenido por Internet.

El examen de estos principios, junto con las normas según las cuales se puede usar el CSS, se llevó a cabo en el seno del CPTWG. El resultado de los debates fue un acuerdo general respecto a una serie de principios. El CPTWG no tenía autoridad para “adoptar” estos principios o para forzar a alguien a usarlos, pero desempeñó una función muy importante. Los debates abiertos que llevaron al acuerdo unánime entre todos los que participaron en dichos debates proporcionaron un mapa vial para MEI[13] al crear la licencia para el uso del CSS.

Antes de describir las obligaciones contractuales particulares de la licencia, es importante entender en primer lugar por qué es necesaria una licencia. El CSS, creado por MEI y Toshiba, es de propiedad; estas compañías concibieron la tecnología y tienen algunos derechos de propiedad intelectual con respecto a ella. En consecuencia, cualquiera que desee usar el CSS - ya sea para codificar un contenido o para descodificarlo -, debe obtener una licencia. Esta licencia no sólo le da a la persona el derecho a usar la tecnología, sino que también le facilita las “claves” tecnológicas pertinentes y necesarias. Puesto que para utilizar el CSS es necesaria una licencia, ésta puede imponer obligaciones en lo referente al modo en que se debe usar la tecnología y sobre cómo debe tratarse el contenido tras haber sido descodificado. Para asegurarse de que los propietarios del contenido, los fabricantes de productos electrónicos para el consumidor y los fabricantes de productos informáticos realmente usarían el CSS, era fundamental que los tres sectores alcanzasen un acuerdo unánime en cuanto a las obligaciones que la licencia iba a imponer.

Gracias al consenso del CPTWG con respecto a algunos principios, MEI estaba segura de que era razonablemente probable que todos los participantes en el nuevo mercado del DVD aceptasen una licencia para esta tecnología basada en los principios mencionados. Pocos días después de la reunión del CPTWG en la que se llegó a este acuerdo general, que se celebró pocos días después de que se acordase unánimemente que la tecnología de codificación revisada era aceptable, MEI presentó el documento de licencia inicial “provisional”, y las compañías pudieron producir discos DVD que contenían películas codificadas y dispositivos

[13] En lo referente al CSS, MEI ha actuado como agente expedidor de licencias tanto para sí misma como para Toshiba.

que pudiesen leer la película para el placer del consumidor, a la vez que protegían ese contenido de la realización de copias no autorizadas por parte del consumidor.[14]

La licencia del CSS

Hay dos características de la licencia de esta tecnología que la hicieron única: en primer lugar, se ofrece basándose en un sistema libre de regalías, con una pequeña contribución administrativa que se percibe para compensar los costes reales de la gestión del sistema de licencia; en segundo lugar, la licencia a largo plazo de la tecnología se entregará a una organización cuyos propietarios y dirigentes son los titulares de la licencia de la tecnología, incluidos los propietarios del contenido, los encargados de introducir productos informáticos, y los fabricantes de productos electrónicos para el consumidor. Aunque se ha tardado un tiempo considerable y se han efectuado no pocas negociaciones hasta completar las normas de gobierno en virtud de las cuales funcionará este organismo compuesto por varias industrias y las condiciones de la licencia final que se ofrecerá a través de esta organización, los documentos de la licencia y de las empresas ya están casi preparados, y se espera que en un futuro próximo comience la expedición de licencias de largo plazo mediante este organismo compuesto por varias empresas y propiedad de los titulares de las licencias.

Requisitos vigentes para la protección de ejemplares. La licencia del CSS expedida por MEI impone a los titulares una serie de obligaciones con respecto a cómo debe protegerse el contenido codificado con el CSS cuando ha sido descodificado. Las compañías que fabrican dispositivos de lectura licenciados, con arreglo al acuerdo referente a la licencia y a las especificaciones conexas, deben utilizar ciertas técnicas determinadas para mantener la protección del contenido como sigue:

La primera tarea es impedir que los consumidores tengan acceso al contenido descodificado durante el proceso de lectura.

En el entorno de la lectura informática, no debe colocarse el contenido descodificado en buses accesibles al usuario mientras aquél esté en el sistema codificado con MPEG. En el futuro, no se permitirá ningún contenido en los buses accesibles al usuario, incluso tras la descodificación del MPEG, debido a la fácil disponibilidad de codificadores MPEG para aplicaciones de consumo. A corto plazo, la idea es que un contenido codificado con MPEG se podría manipular desde el ordenador de un consumidor de tal modo que se pueda hacer una copia del contenido - de ahí la exigencia de que el contenido codificado mediante MPEG no esté disponible fácilmente en los buses a los que normalmente tienen acceso los consumidores. Los datos descodificados mediante MPEG son lo suficientemente extensos y complejos para que un usuario común los manipule por lo que en el momento en que se negoció la licencia no había necesidad de prohibir un acceso normal del usuario a dichos datos. A partir del momento, cada vez más cercano, en que los codificadores MPEG estén disponibles más fácilmente para los consumidores, y a éstos les cueste menos usarlos, y cuando no resulte complicado mantener alejado el contenido descodificado dentro del entorno informático de los buses accesibles para el usuario, el pliego de condiciones exige que los

[14] Aunque la licencia provisional inicial se presentó con gran rapidez, la licencia provisional a largo plazo tomó muchos meses de negociaciones antes de que se alcanzase un acuerdo entre las partes interesadas basado en una serie definitiva de normas de uso y protección de ejemplares.

fabricantes de productos informáticos mantengan este contenido alejado de los buses accesibles al usuario.

En un principio no se pusieron condiciones equivalentes en el ámbito de los productos electrónicos para el consumidor, debido a que los consumidores no suelen alterar el funcionamiento que el fabricante ha establecido para los dispositivos electrónicos. Sin embargo, para impedir cualquier cambio posible, en un futuro cercano se modificarán las condiciones, y se exigirá que incluso los productos electrónicos para el consumidor tengan contenido codificado y descodificado con MPEG en los buses accesibles al usuario que puedan existir en dichos dispositivos, y se prohibirá que dichos productos electrónicos se fabriquen de tal forma que los consumidores que utilicen instrumentos fácilmente disponibles puedan acceder al contenido codificado y descodificado con MPEG.

La licencia también regula atentamente las conexiones entre los dispositivos de lectura y otros dispositivos. Sólo se permiten, como indicamos a continuación, algunas conexiones específicas:

Las conexiones con productos electrónicos para el consumidor normales deben incluir tecnologías de protección de ejemplares analógicas específicas: los sistemas de propiedad Macrovision cuando sea pertinente, y la versión analógica de los indicadores de información sobre protección de ejemplares del Sistema de Gestión de Generación de Ejemplares (*Copy Generation Management System*) en el caso de determinadas conexiones;

Se han prohibido totalmente las conexiones digitales debido a la falta de un sistema de protección de ejemplares que se haya acordado de forma unánime. Se espera que esta situación cambie en un futuro cercano, con la aprobación general de los acuerdos sobre la tecnología de Protección de Ejemplares por Transmisión Digital (*Digital Transmission Copy Protection*) y la licencia conexa.

Puesto que las conexiones con monitores de ordenador ya estaban muy extendidas en el mercado basado en la tecnología general RGB, el acuerdo referente a la licencia permite estas conexiones a pesar de la falta de una protección de ejemplares aceptada.

Condiciones de funcionamiento conexas

Control de lectura a escala regional. Se estuvo de acuerdo en que se podría aplicar el control de lectura a escala regional al entorno DVD, y la licencia CSS ha servido de vehículo para esta condición particular. En el Anexo C se presenta un examen más detallado del control de lectura a escala regional.

Control de lectura de medios que permiten grabar. La licencia CSS, como apoyo a las condiciones relativas al hecho de impedir el acceso de los consumidores a flujos de datos en un entorno en el que se puedan hacer copias, prohibe que se lleven a cabo las funciones de lectura del CSS (descodificación, etc.) con respecto a todo contenido que se encuentre en medios que permiten grabar. En otras palabras, el CSS es una tecnología que debe usarse únicamente en relación con contenido pregrabado en medios fabricados sólo para la lectura (DVD-ROM).

Control de lectura aplicable al contenido no codificado. Aunque los proveedores del contenido son libres de colocar su contenido sin codificar en discos DVD de cualquier tipo, la licencia CSS también impide que el contenido que en un principio se codificó usando el CSS

se grabe sin codificar en cualquier tipo de disco. Así pues, si un consumidor consigue acceder a la información tras la descodificación y graba el contenido en un disco DVD, la licencia exige que el sistema de lectura reconozca que este contenido se había codificado inicialmente usando el CSS y que no se puede presentar sin codificar, independientemente del tipo de medios implicados. La tecnología inicial para realizar lo descrito depende de la existencia y la colocación de un único bit en la información de formato del DVD, y se considera muy poco fiable. El sistema a largo plazo que sirva para impedir la reproducción de este contenido se basará en una tecnología de impresión con filigrana que los propietarios del contenido podrán utilizar para marcar el contenido y que los titulares de licencias de dispositivos de lectura deberán buscar en cualquier contenido que se presente en forma no codificada.

Solidez contra el ataque. Para asegurar que los consumidores no anulen fácilmente las puestas en ejecución, ya sea mediante sus propios instrumentos y métodos, o mediante programas o dispositivos creados con el objeto de anular la protección de ejemplares prevista en las condiciones de la tecnología y la licencia, la licencia del CSS también exige que la aplicación de las funciones de descodificación y las relacionadas con la protección de ejemplares sean difíciles de anular. La definición exacta de esta condición ha sido algo polémica, y algunos titulares de las licencias han fracasado en su puesta en ejecución. Resultaba tan sencillo anular algunas de las puestas en ejecución de los lectores DVD del sistema de control de lectura a escala regional que este sistema fue objeto de desacato generalizado en 1998 y principios de 1999. Un interés renovado de los titulares de la licencia con respecto a esta condición, junto con la disponibilidad de más películas pregrabadas en DVD codificadas para su reproducción fuera de la región del América del Norte, ha conducido a un mejor cumplimiento de ésta. Recientemente, una aplicación poco segura de las funciones de descodificación en un programa informático de lectura concluyó en un “acto de piratería”, que recibió mucha publicidad, de la propia tecnología de codificación, situación que supondrá un problema para esta tecnología concreta durante los próximos meses.

Observancia y otras condiciones de la licencia. Como se indicó anteriormente, en la actualidad MEI es quien expide las licencias de la tecnología del CSS de forma “provisional” y pronto cederá esta responsabilidad a la Administración de Control de Ejemplares de DVD (*DVD Copy Control Administration -“DVD CCA”),* un organismo formado por varias empresas y controlado por los titulares de las licencias. En calidad de expedidor de licencias, MEI tiene, y DVD CCA tendrá después, unos derechos directos para asegurar el cumplimiento de la licencia y de las condiciones de especificación conexas. También se han concedido unos derechos especiales a los proveedores de contenido que son titulares de una licencia para hacerla respetar en calidad de “terceros beneficiarios”, como reconocimiento de que el objeto de la licencia es la protección del contenido, de que la tecnología está libre de regalías y de que hace que aumente el valor de los productos únicamente en relación con la disponibilidad de contenido que, de otro modo, no se hubiese presentado en este formato. Este derecho se ha limitado al desagravio por mandato judicial y a otros desagravios de equidad (con el objeto principal de mantener alejadas del mercado las puestas en práctica que no cumplan las condiciones), pero se ha considerado que la amenaza de litigios desde estas compañías añade un factor disuasivo verosímil contra el incumplimiento por parte de los titulares de licencias.

Otros trabajos del CPTWG

Cuando el trabajo inicial sobre el CSS para DVD hubo finalizado, el CPTWG se centró en otros problemas. Una de las cuestiones es la protección del contenido que circula por

conexiones digitales entre los dispositivos que se encuentran en los hogares de los consumidores. Una segunda cuestión guarda relación con el marcado del contenido con información de protección de ejemplares de tal modo que sobreviva sin complicaciones a transformaciones habituales del contenido (por ejemplo, transformándolo de formato digital a analógico y de nuevo a formato digital).

Actualmente, el CPTWG es un foro abierto a presentaciones sobre tecnologías relativas a la protección de contenido digital sonoro y de vídeo contra la copia sin autorización por parte del consumidor. Este grupo se reúne mensualmente en Burbank, California, y atrae aproximadamente a 125-150 personas a sus reuniones. Aunque se presentan informes de forma regular acerca de determinados hechos acaecidos en foros conexos, el orden del día está abierto, y cualquiera que desee exponer algo no tiene más que presentarse y hacerlo. Por su naturaleza, no es ésta una organización en la que se tomen decisiones, sino más bien en la que se plantean y se debaten cuestiones. Cuando los miembros así lo deciden, el CPTWG ha creado, y probablemente volverá a hacerlo en el futuro, grupos de trabajo o de debate especiales para ocuparse de temas particulares. La regularidad de las reuniones del CPTWG también sirve para facilitar la programación de otras reuniones relacionadas con la protección de ejemplares durante la semana en que se reúne el CPTWG. Los participantes en este grupo proceden de todo el mundo, y entre ellos se cuentan muchas pequeñas empresas y no pocos inventores, así como las empresas más importantes a escala mundial de las industrias cinematográfica, musical, informática, y de productos electrónicos para el consumidor.[15]

El objetivo declarado de los esfuerzos de las distintas empresas ha sido proponer unos medios legales y tecnológicos de “hacer que la gente honesta lo siga siendo”. Esos esfuerzos no tenían como objetivo explícito impedir que los piratas profesionales obtuviesen acceso al contenido protegido por el derecho de autor o que hiciesen copias ilegales de las obras, sino que, más bien, el objetivo ha sido idear unos medios para dificultar a los consumidores corrientes la realización de copias o transmisiones sin autorización de obras protegidas.

En respuesta a las dos cuestiones de la protección del contenido en las conexiones digitales y el marcado del contenido con información de protección de ejemplares que no se deteriore, el CPTWG creó dos grupos de trabajo -el Grupo de Debate sobre la Transmisión Digital (*Digital Transmission Discussion Group - DTDG*) y el Subgrupo de Ocultación de Datos (*Data Hiding Subgroup - DHSG*)-, para buscar propuestas tecnológicas de distintas procedencias y realizar algunas pruebas y análisis de las propuestas recibidas. Ambos grupos debatieron, con las partes interesadas, los métodos que ellos utilizarían para evaluar las propuestas, redactaron peticiones de propuestas y las difundieron, y probaron y examinaron las propuestas recibidas. Ningún grupo contaba con la capacidad jurídica para hacer ningún tipo de “selección” de las tecnologías propuestas, pero ambos contaban con el suficiente prestigio y las capacidades tecnológicas para que las pruebas, los exámenes y los procesos de evaluación fuesen objeto de un interés considerable y obtuviesen el apoyo de varias empresas y compañías que ofrecían soluciones.

---

[15] La industria musical ha participado menos que las otras y, como se describe con mayor detalle en este estudio, ha intentado basarse en su propia organización, la Iniciativa para una Música Digital Segura (*Secure Digital Music Initiative*), para abordar las cuestiones de protección de ejemplares relacionadas específicamente con la música.

La Protección de Ejemplares por Transmisión Digital

El sistema de Protección de Ejemplares por Transmisión Digital (DTCP), formado por la fusión de dos sistemas tecnológicos propuestos inicialmente al DTDG del CPTWG, está diseñado para proteger el contenido durante la transmisión digital de un dispositivo de consumo a otro. El sistema se basa en una combinación de autenticación -comunicación de un dispositivo a otro en una interfaz digital de dos direcciones para determinar que cada dispositivo es un "miembro" aceptable en la "familia" DTCP- y de codificación del contenido para protegerlo de cualquier interceptación no autorizada mientras viaja por la interfaz.

La licencia de este sistema está controlada por una sociedad de responsabilidad limitada constituida por las cinco compañías que crearon la tecnologías: Hitachi, Intel, Matsushita, Sony y Toshiba. La licencia tiene muchas de las características de la licencia del CSS: en ambas la licencia básica autoriza el uso de la propiedad intelectual en el algoritmo, las claves y otras tecnologías que son propiedad de la sociedad de responsabilidad limitada. Las regalías y las contribuciones corresponden a las cantidades necesarias para recuperar los costes de funcionamiento del sistema. Por último, la protección básica de ejemplares efectuada mediante las normas de conformidad exige que el contenido esté protegido de forma segura a lo largo del proceso de transmisión.

Dos aspectos de la licencia de esta tecnología son algo distintos y han sido causa de cierta polémica: las normas de uso que deben aplicarse a los propietarios del contenido que deseen utilizar la tecnología para proteger su contenido, y qué medios seguros se deben usar para proteger las copias autorizadas cuyo contenido ha sido protegido usando el DTCP.

Con respecto a las normas de uso, el DTLA propuso un pliego de normas con el objeto de asegurar que los consumidores pueden seguir haciendo copias de algunos tipos de emisiones, como la televisión gratuita y la programación básica por cable. Los posibles propietarios del contenido, titulares de la licencia de la tecnología, están negociando con el DTLA para resolver las cuestiones relativas al número de copias que se deberían permitir, las normas que deben aplicarse para pagar y otras emisiones de acceso condicionado. El DTLA y los propietarios del contenido están de acuerdo en que se puede usar el DTCP para impedir que los consumidores hagan copias del contenido en medios físicos (como el DVD), las emisiones que deben pagarse para poderlas ver y el vídeo por encargo. Se espera que pronto se tome una decisión final con respecto a la cuestión de las normas de uso.

Puesto que el sistema DTCP permite una cantidad determinada de copias, se reconoce que toda copia autorizada debe estar protegida de ser objeto de copias posteriores. De no ser así, de poco habría servido proteger el contenido hasta el momento de hacer una copia autorizada. Por consiguiente, con arreglo a las normas del DTCP, toda copia autorizada debe estar codificada o debe formar parte de un "sistema cerrado" para asegurar que las condiciones de la licencia adicional aplicable a la lectura de la copia pueden limitar cualquier copia posterior.

Si bien aún quedan algunas cuestiones que no han sido resueltas, entre ellas hasta qué punto se puede hacer uso del DTCP para impedir que se carguen sin autorización contenidos en Internet, parece probable que las empresas lleguen a un acuerdo. La licencia del sistema DTCP ha estado en el mercado durante más de un año y cada vez son más los productos en los que se incorpora. También se ha aceptado como una norma de la UIT (Unión Internacional de Telecomunicaciones) y se está incluyendo en la norma Open Cable para las

cajas de conexiones. La confirmación final de la tecnología y las condiciones de licencia tendrán un efecto positivo importante en el uso real que se hace del sistema en el mercado.

La transmisión de información sobre la protección de ejemplares: Información Digital Segura (*Secure Digital Information*) y las tecnologías de impresión con filigrana

Puesto que la copia de una parte limitada del contenido está autorizada, es muy importante que la información relativa a la situación de protección de ejemplares de un contenido específico se transmita de forma precisa, segura y cómoda.

Las primeras propuestas de transmisión de la información relativa a la protección de ejemplares como “información adjunta” (es decir, información que se adjunta a un contenido específico pero que no es parte de dicho contenido ni es necesaria para poder verlo o escucharlo) no es segura frente a la modificación sin autorización (y, por lo tanto, puede ser inexacta en cualquier momento) y su búsqueda resulta poco práctica para algunos dispositivos. Por consiguiente, ha habido una oposición considerable, en especial por parte de algunas empresas del mundo de la informática, a esta forma de transmitir la información relativa a la protección de ejemplares.

Para resolver estos problemas, se han concebido dos métodos de transmisión de información sobre la protección de ejemplares.

Datos Digitales Seguros (*Secure Digital Data*). Una característica de la tecnología DTCP es que la información sobre protección de ejemplares relativa a cada parte de contenido que se manda mediante la interfaz protegida por el DTCP se transmite como parte del propio sistema de codificación. Es decir, si alguien intenta manipular la información sobre protección de ejemplares, se modificarán las claves del contenido, y éste será inaccesible para el dispositivo receptor. Este método tiene en cuenta los tres factores: la información está segura ante el ataque de alguien que desee modificarla, es fiable tras haberla recibido (siempre y cuando no se haya falsificado), y es pertinente, ya que forma parte del propio sistema de seguridad. Un contenido que no utilice el DTCP sencillamente no lleva esta información sobre protección de ejemplares, y un ordenador puede no buscarla en dicho contenido. Los ordenadores deben tratar de forma especial el contenido protegido con el DTCP en cualquier caso, debido a la necesidad de descodificarlo, y la información sobre la protección de ejemplares no es más gravosa que el propio sistema de protección.

Impresión con filigrana. El segundo método de transmisión de información sobre protección de ejemplares resuelve los problemas de seguridad y fiabilidad, pero no puede resolver por sí mismo el de la pertinencia. Las tecnologías de impresión con filigrana transmiten la información escondiendo determinados códigos dentro del propio contenido. Aquellos que saben dónde mirar y cómo interpretar los códigos pueden extraer la información y dar una respuesta. No obstante, también es fundamental que la información no moleste la visualización o audición normal del consumidor. Por lo tanto, debe ser invisible excepto para un detector especialmente diseñado. Esto significa que la detección de la información es “poco práctica” en el sentido de que el producto a través del cual circula el contenido, o con el que se esta viendo o escuchando, debe saber buscar la impresión con filigrana en esta parte especial del contenido. Puesto que muchos dispositivos no distinguen entre distintos tipos de contenido, este método no da ninguna protección cuando se trata de sistemas no participantes.

Hasta ahora, la idea central de nuestros análisis ha sido principalmente la protección del contenido visual (es decir, las obras audiovisuales). Ahora nos centraremos en la música grabada. Ha habido dos iniciativas importantes en este ámbito: la protección de ejemplares de discos sonoros DVD, y la Iniciativa para una Música Digital Segura (*Secure Digital Music Initiative*).

La protección de ejemplares de discos sonoros DVD

Aunque los videodiscos DVD y los productos de lectura relacionados llevan casi tres años en el mercado, el formato sonoro DVD aún no se ha comercializado. La entidad 4C, LLC, una sociedad de responsabilidad limitada constituida para ofrecer y administrar licencias de tecnologías de protección de ejemplares creadas por cuatro compañías (IBM, Intel, Matsushita y Toshiba), está ofreciendo la protección de ejemplares para este formato. Si bien en un principio se había propuesto que se ofrecería una variante menor del sistema de codificación vídeo CSS como codificación base para el contenido grabado en los discos sonoros DVD, el reciente acto de piratería en la tecnología del vídeo ha hecho que se considere de nuevo esta propuesta. Actualmente, es probable que el sistema de codificación de los discos sonoros DVD se base en una tecnología de codificación totalmente nueva que no sea susceptible de ser víctima del mismo acto de piratería o incluso del mismo tipo de acto que tuvo lugar con relación al CSS para el DVD vídeo.

Las normas de protección de ejemplares también serán algo distintas en el caso del DVD sonoro. Puesto que es un hecho que los consumidores utilizan el material sonoro de forma distinta del visual, se permitirá que se realicen algunas copias como una cuestión de rutina. La naturaleza y el alcance de las copias que se permitirán fue el tema de un atento debate entre las compañías de 4C y las cinco compañías de grabación más importantes. La estrategia que iban a adoptar se anunció en febrero de 1999 en la reunión del CPTWG y cuenta con las siguientes normas básicas:

Se permitirán tres tipos de salidas en los equipos de lectura de DVD: dos salidas *Legacy* (analógica y IEC 958) y salidas digitales protegidas (probablemente en configuradas un principio como salidas IEEE 1394).

En cuanto a las salidas *Legacy*, la protección de ejemplares quedará cubierta por una combinación de impresiones con filigrana que contendrán información sobre esta protección y, para las salidas IEC 958, el Sistema de Gestión de Copias en Serie (*Serial Copy Management System* -exigido en los Estados Unidos en virtud de la Ley sobre Grabaciones Sonoras en el Hogar de 1992 y parte de la norma de la Comisión Electrotécnica Internacional que se observa en la Unión Europea, el Japón y otros países). En estas salidas, por lo general debe entregarse el contenido en “tiempo real” (es decir, debe transmitirse a la velocidad normal de audición del contenido).

En cuanto a otras formas de salida digitales, se exigirá la aplicación de protección de ejemplares, y la tecnología DTCP será una forma posible de protección. Sea cual sea la tecnología que se utilice, ésta debe: 1) limitar el contenido a la “calidad CD” o reducir las frecuencias de muestreo o las extensiones de los bits del contenido; 2) transmitir toda la información sobre protección de ejemplares necesaria para las opciones del “menú” completo de las opciones del proveedor del contenido (véase abajo); y 3) asegurar la protección del contenido de forma adecuada tanto en la transmisión como en la copia autorizada que se hace. La interfaz digital protegida puede transmitir el contenido sea cual sea la velocidad que

admita la interfaz (es decir, puede ser a velocidades mayores que la del tiempo real y, por ello, puede admitir capacidades de grabación a velocidades muy elevadas).

Al iniciar la lectura de un disco sin codificación, el dispositivo de lectura debe buscar la impresión con filigrana para decidir si la copia que se está haciendo está autorizada. Si encuentra una impresión con filigrana que indica que el contenido, en un principio, había sido codificado mediante el sistema 4C, el dispositivo de lectura debe negarse a leer cualquier disco cuyo contenido no esté codificado.

Los dispositivos de grabación tendrán una licencia para grabar utilizando un sistema de codificación autorizado para proteger el contenido de un ejemplar autorizado. Una condición de esta licencia es que el dispositivo de grabación lea y responda a la información sobre la protección de ejemplares en forma de impresión con filigrana en cualquier interfaz *Legacy* y a la información digital contenida en cualquier interfaz digital protegida contra la copia. Para "responder" como es debido, el dispositivo de grabación debe decidir si la señal de entrada procede del original de la grabación o de una copia del contenido que ya se había hecho utilizando el sistema de protección de ejemplares (en cuyo caso así lo indicaría la información de protección de ejemplares);

debe negarse a hacer una copia de todo contenido en el que la señal o la información de entrada proceda de una fuente que ya era una copia del material;

debe negarse a hacer una copia de cualquier contenido recibido mediante una interfaz digital protegida contra la copia cuando el dispositivo de grabación ya había hecho una copia del material (es decir, la norma fundamental es que, en el supuesto de que el contenido se envíe mediante la interfaz digital protegida contra la copia, se puede hacer una copia por dispositivo de grabación); y

en los casos en que se permite hacer una copia del material de entrada, debe poner al día la información sobre protección de ejemplares en forma digital (si existe) y de impresión con filigrana, para señalar que la copia que se está haciendo es realmente una copia y no la grabación original del material.

Al permitir que los consumidores hagan copias con arreglo a estas normas, el grupo 4C tiene la intención de establecer ciertos límites a las copias respetando unas condiciones razonables según las expectativas y la experiencia del consumidor normal en relación con otros entornos sonoros. El grupo, así como las compañías de grabación que le aconsejaron, reconocieron que los consumidores están acostumbrados a hacer al menos una copia "de comodidad" del material sonoro para distintos lugares; es decir, se puede hacer una copia adicional para tenerla en el automóvil, o para ir a correr, o para las otras habitaciones de la casa, o para otros lugares en los que pueda encontrarse el consumidor en un momento determinado. Cualquier sistema que no permitiese hacer esa copia se encontraría con una oposición considerable por parte de los consumidores como una cuestión de mercado y con la amenaza constante de la elusión. El grupo y los consultores de las compañías de grabación, más que enfrentarse a esos problemas, convinieron permitir este tipo de copias de comodidad pero también utilizar distintas tecnologías de formas diferentes para evitar que se hiciesen más copias.

Además, el grupo comprendió la necesidad de admitir los productos y sistemas *Legacy* como forma de hacer sus productos más atractivos en el mercado. De este modo, los consumidores llegarían antes a contar con productos "conformes" que proporcionen cierta

protección de ejemplares dentro de las normas sobreentendidas descritas anteriormente, más que seguir confiando en unos sistemas no conformes y *Legacy* que no proporcionan ninguna protección de ejemplares.

Iniciativa para una Música Digital Segura (*Secure Digital Music Initiative - SDMI*)

La SDMI fue creada por las asociaciones comerciales de la industria de grabación y las compañías discográficas más importantes. Se trataba, en gran medida, de una respuesta al "fenómeno" del MP3 que se extendió por todo el mundo en 1998. El MP3 - una tecnología de compresión que permitía comprimir el contenido sonoro en ficheros informáticos que son lo suficientemente pequeños para poderlos transmitir fácilmente por Internet - permitía que los consumidores se convirtiesen en sus propios distribuidores de música grabada. Esta tecnología, que carecía de sistemas de protección (ni de acceso ni de copias) fue la causa de la "peor pesadilla" de las compañías discográficas: un álbum se vendía una vez y a continuación los consumidores individuales lo redistribuirían a todo aquel que desease ese álbum, sin que la compañía discográfica vendiese más que el primero.

A modo de respuesta, las discográficas presentaron una demanda judicial, que resultó infructuosa, contra la distribución del producto que permitía que los consumidores almacenasen ficheros MP3 portátiles. Incluso mientras se esperaba una decisión con respecto a la demanda, las compañías discográficas intentaron reclutar a las industrias de la electrónica y la informática para el consumidor para llevar a cabo un proceso voluntario de creación de unas normas y unas tecnologías mediante las cuales se pudiera limitar la distribución no autorizada de música por Internet, al mismo tiempo que permitían la distribución autorizada. Se invitó a las compañías a formar parte de la SDMI por 10.000 dólares estadounidenses cada una, a cambio de los cuales las compañías que se adherían al grupo obtenían voz en el proceso de creación de las normas y de selección de las tecnologías. A finales de 1999, unas 150 compañías habían pasado a formar parte de la SDMI, y muchas de ellas enviaban a representantes a la mayor parte de las reuniones.

Aunque el "Plenario" - el órgano compuesto por la totalidad de miembros de la SDMI- está abierto a todas las compañías que deseen pagar la contribución y firmar el acuerdo con respecto a las condiciones de participación, la Fundación SDMI es la que administra la organización, y está formada por una Junta Directiva compuesta por representantes de las compañías discográficas (la mayor parte de ellas, si bien no todas, son las compañías discográficas más importantes). Sin embargo, el poder de la Fundación es limitado y no puede anular las decisiones tomadas en el Plenario con respecto a la sustancia de la norma o las condiciones de cualquier licencia que ofrezca la SDMI.

La prioridad del grupo era crear una norma provisional para iniciar el proceso de regulación del contenido sonoro que llega a los dispositivos portátiles. Para hacerlo, la SDMI estableció el Grupo de Trabajo sobre dispositivos portátiles (*Portable Device Working Group – PDWG*) cuya misión era formular una norma inicial que debía estar lista para el 30 de junio de 1999. El PDWG se reunió una media de dos veces al mes desde febrero hasta principios de julio y, en julio de 1999, presentó la versión 1.0 de la fase I de su norma sobre dispositivos portátiles.

En la norma se mencionan tres tipos principales de protección. Primero se exige que los sistemas de conformidad estén provistos de la tecnología necesaria para detectar tres tipos de señales impresas con filigrana:

una señal que comunica que se ha completado la fase I y que se necesita pasar a la fase II para que el sistema reciba el contenido destinado a esta fase. No será necesario un ascenso del sistema siempre y cuando el consumidor no desease recibir el contenido de la fase II;

información sobre protección de ejemplares que figura en la impresión con filigrana indicando que no se permite hacer copias del contenido del cual la impresión forma parte; y

una indicación de que el contenido forma parte de la fase II, y que se permitirá el acceso al sistema sólo si éste ha sido ascendido a la fase II.

Segundo, aunque todos los tipos de contenido (por ejemplo, los ficheros MP-3), incluidas las copias no autorizadas de las obras, pueden entrar en un sistema conforme a la SDMI durante la fase I, cuando el contenido ha entrado en dicho sistema, se deben mantener algunas protecciones. Tras la elección inicial del consumidor de que el contenido debe conservarse dentro del entorno conforme a la SDMI, toda copia debe realizarse de forma protegida (codificada de algún modo seguro) y la lectura del contenido está limitada a determinadas salidas autorizadas, que básicamente impiden que el consumidor cargue el contenido en Internet o que lo envíe a dispositivos mediante una conexión digital. El tercer tipo de protección es la promesa de un régimen de protección más elaborado en la fase II.

La SDMI ha funcionado en general como un organismo de creación de normas para la industria, tomando como modelo las técnicas utilizadas para crear normas como MPEG pero sin seguir completamente los procedimientos de creación de normas. Las decisiones se toman cuando hay un “acuerdo unánime sustancial” a favor de esa decisión concreta entre cada grupo de industrias implicado. La existencia de dicho acuerdo unánime queda determinada en última instancia por el director ejecutivo de la SDMI, al cual nombra la Fundación SDMI.

Por lo general, la norma SDMI es similar a muchas otras que las industrias utilizan para fomentar la explotación de determinados productos y sistemas. La única parte de la norma SDMI que exige una licencia tecnológica específica es la impresión con filigrana. La razón que explica la existencia de una única tecnología con este fin y, por lo tanto, una licencia obligatoria para una tecnología concreta asociada con la norma, es que introducir varias impresiones con filigrana en el contenido probablemente tendrá como consecuencia una degradación importante de la calidad de la música, y la detección de más de una impresión con filigrana se considera demasiado gravosa para los productos y sus fabricantes. Así pues, las empresas de contenido y de productos tienen un fuerte incentivo para limitar la impresión con filigrana a una sola tecnología que las empresas de contenido utilizan uniformemente y que los productos que reciben el contenido detectan, también, uniformemente. Estos hechos llevaron al PDWG de la SDMI a decidirse a escoger una sola tecnología de impresión con filigrana para transmitir información sobre ejemplares en la fase I y transmitir la señal de que esta fase ha finalizado y de que un producto debe ascender a la fase II para poder recibir el contenido de la fase II. El proceso de selección comportaba una petición de propuestas, un examen inicial de las tecnologías presentadas, y las condiciones, la creación y la aplicación de la licencia de un régimen de prueba para decidir qué impresiones con filigrana se detectaban de forma más sencilla y fiable y cuáles tenían menos consecuencias en la calidad de la música que iba a oír el consumidor.

El resultado fue un proceso considerablemente más largo de lo previsto. No obstante, la finalización de la selección de impresiones con filigrana y la disponibilidad de una norma final significan que los productos conformes a la SDMI estarán en los mercados de todo el

mundo poco después del inicio del año 2000, y las compañías discográficas esperan que, a partir de este momento, proliferen este tipo de productos y que, básicamente, desplacen durante el proceso a los productos no conformes.

Actualmente, la SDMI está realizando una labor a más largo plazo encaminada a definir una norma para la fase II (es decir, todo lo que sigue a la fase I). Su finalización está prevista para abril del 2000, aunque visto el proceso de la fase I, quizá sea esto algo optimista. El objetivo fundamental de la fase II es escoger un medio a largo plazo para determinar qué contenido es conforme a la SDMI y hacerlo sobre una base cuya aplicación sea fiable, segura y razonable. La tecnología de impresión con filigrana de la fase I no se aplicará automáticamente a la fase II, si bien se considera necesario cierto uso continuo de esta tecnología, aunque sólo sea para indicar a los consumidores que deben pasar a la fase II.

La tecnología de impresión con filigrana de la fase I es propiedad de una empresa particular, que es quien la creó y quien concede las licencias, mediante la entidad 4C, LLC como su organismo autorizador. Los gastos relacionados con esta licencia son una combinación de las contribuciones necesarias para cubrir los gastos administrativos similares a los de los otros sistemas principales de protección de ejemplares antes descritos y las regalías comerciales habituales asociadas a un dispositivo tecnológico comercial. La propia licencia impone también algunas restricciones en cuanto a la utilización de la tecnología, ideadas básicamente para mantener las prácticas habituales de los consumidores de mandar la música de un dispositivo a otro descritas anteriormente en relación con los métodos de protección de copias sonoras DVD. En la práctica, esto significa que la música comercial pregrabada para venderla a los consumidores no puede estar codificada como material del que no se permite hacer ninguna copia, sino que los consumidores deben poder hacer al menos una.

Conclusiones

Como se ha intentado explicar en este trabajo, la creación y la aplicación de medidas tecnológicas para la protección de ejemplares no es una tarea fácil. La innovación de tecnologías de protección es un proceso continuo que requiere una inversión importante de investigación y perfeccionamiento. La puesta en práctica de medidas tecnológicas requiere que exista cierta colaboración entre las industrias. La expedición de licencias de medidas tecnológicas de protección para el uso de propietarios del contenido y de fabricantes de equipos implica que han de llevarse a cabo negociaciones para llegar a un consenso acerca de las normas apropiadas de control de copias y de utilización del contenido que usan estas medidas. Las descripciones que hemos hecho de algunas de las estructuras actuales de protección de ejemplares han demostrado que las medidas tecnológicas se pueden aplicar, y se están aplicando, de forma que satisfagan las expectativas razonables de los consumidores y que permitan a los consumidores realizar ciertas copias. El objetivo de las medidas tecnológicas no es oponerse a todas las posibilidades de valerse de las excepciones legítimas a los derechos exclusivos de los propietarios del contenido, sino que en realidad pueden ayudar a facilitar el uso adecuado de estas excepciones y limitaciones. Sin embargo, la creación de las medidas tecnológicas de protección y su puesta en práctica mediante acuerdos comerciales referentes a licencias son sólo dos elementos de la ecuación de la protección de ejemplares. Es necesaria una protección legal firme, tanto en lo referente a las legislaciones de derecho de autor y derechos conexos como a las leyes contra la acción de elusión de las medidas tecnológicas de protección.

Sin una protección legal adecuada contra la acción de elusión de las medidas de protección de ejemplares, los que “siguen las reglas del juego” tienen una desventaja competitiva injusta. Por ejemplo, los fabricantes de dispositivos de lectura de DVD que quieren que sus productos puedan leer discos DVD codificados con el CSS deben disponer de un acuerdo de licencia que permita la descodificación. Como se explicó anteriormente, este acuerdo de licencia impone ciertas obligaciones acerca del modo en que los dispositivos deben funcionar para proteger el contenido después de haberlo descodificado. No obstante, si las partes tienen la libertad de piratear y anular el CSS, entonces se pueden fabricar productos sin una licencia que descodifique este sistema y que no cumplan las obligaciones relativas a la protección de ejemplares. A menos que este tipo de actividad elusiva sea claramente ilegal, los fabricantes de equipos legítimos no tendrán mucho aliciente para solicitar la licencia para una tecnología, y se derrumbará toda la estructura de protección de ejemplares. El papel fundamental que han desempeñado unas leyes contra la elusión firmes y efectivas demuestra claramente la necesidad de que todos los países incorporen a sus legislaciones nacionales los dos tratados de la OMPI y establezcan unas disposiciones efectivas contra la elusión.

[Siguen los Anexos]

ANEXO A

DESCRIPCIONES SUCINTAS DE ALGUNOS MÉTODOS Y TECNOLOGÍAS DE PROTECCIÓN EXISTENTES

Indicadores de control de copias: Son bits digitales que preceden inmediatamente al contenido o que están incrustados en él y que indican si se pueden hacer copias. Estos indicadores pueden ser muy detallados al definir el número de copias o el tiempo de visualización, etc. Para que sean eficaces, los fabricantes de equipos deben buscar y responder a estos indicadores. Los piratas del contenido pueden identificarlos, desarmarlos o no tenerlos en cuenta fácilmente. Hasta la fecha, no se ha exigido a las empresas informáticas (al menos en los Estados Unidos) que busquen los indicadores, y éstas se han resistido a hacerlo.

SCMS (Sistema de Gestión de Copias en serie): Se trata de un método específico de utilización de los indicadores de control de copias, que permite hacer copias digitales a partir de un original, pero no a partir de una copia de ese original. De este modo, la segunda generación de copias o las posteriores quedan descartadas. Esto se consigue gracias a una serie de indicadores de control que se encuentran en el original y que el dispositivo de copia modifica durante el proceso de copia. Si el ejemplar copiado se utiliza para hacer otra copia, los indicadores de control son incorrectos y el dispositivo lo rechazará como original. Este sistema se utiliza principalmente en los discos compactos de música.
No se ha obligado a los sistemas informáticos a ajustarse al SCMS. Además, se ha visto que el uso de indicadores de control se puede comprometer fácilmente.

Macrovision: Es una señal dentro de una señal de vídeo analógica que perturba la capacidad de grabación de los magnetoscopios de los consumidores. El Tipo I de Macrovision perturba el sistema de circuitos de grabación de los magnetoscopios analógicos, y es compatible con las señales de vídeo NTSC y PAL. Los tipos II y III de Macrovision (pulso de sincronización de la subportadora de color de dos y cuatro líneas respectivamente) se introdujeron con el DVD. Estas señales degradan más la señal de vídeo. Los tipos II y III de Macrovision sólo son compatibles con los magnetoscopios normales NTSC.

Codificación: Es lacodificación digital de los bits que configuran el contenido para impedir que éste se vea con claridad hasta que está descodificado. Las claves necesarias para descifrarlo se entregan sólo a los usuarios y/o a los equipos autorizados. Esta tecnología se utiliza ampliamente en todas las emisiones por satélite, incluidos los canales de acceso condicionado. Los primeros sistemas se basaban en un método de codificación repetible que, una vez comprometido, ya lo estaba para siempre. Los sistemas posteriores utilizaban claves con métodos de codificación renovables y cambiantes. Se facilitaron tarjetas inteligentes a los consumidores para identificar quién había pagado por el servicio y quién no. La codificación protege el contenido hasta que se descodifica (normalmente en una caja de conexión). En este momento, el contenido se puede copiar en otros medios digitales (por ejemplo, el disco de un ordenador) o analógicos (por ejemplo, en un magnetoscopio) que puede estar conectado a la caja de conexión directa o indirectamente pasando por otro dispositivo, como un televisor.

Identificación: Es una forma única de identificar dispositivos y clases de dispositivos para facilitar la autenticación y la revocación.

Autenticación: Es el acto de comprobar un dispositivo para decidir si se ajusta a una tecnología/ estructura de protección de ejemplares concreta y si debería recibir contenido protegido. Cuando se ha verificado el dispositivo, la autenticación permite transferir los datos (el contenido) del dispositivo de partida al dispositivo receptor verificado por un canal seguro. Normalmente esto se realiza mediante el uso de varias técnicas criptográficas.

Autorización: Son los derechos de acceso que se conceden a un dispositivo cuando ha sido identificado y autentificado satisfactoriamente.

Revocación: Cuando la manipulación o la clonación ilegal ha comprometido un dispositivo o un tipo de dispositivos, la revocación digital anula cualquier otro derecho de acceso a ese dispositivo. Los dispositivos conformes a las normas no autentificarán ni autorizarán los dispositivos revocados. Esta lista se actualiza electrónicamente, pasando por las redes y los medios físicos hasta llegar a los dispositivos seguros y no requiere ninguna modificación física.

Impresión con filigrana: Son bits incrustados en el contenido que no se pueden detectar con la vista ni con el oído, pero que un dispositivo de detección puede leer para saber si el contenido que se ve u oye es auténtico y cuál es la fuente de dicho contenido. Este tipo de información puede ser sobre el autor, los derechos, la distribución, etc. También puede contener información e instrucciones de control. La impresión con filigrana sólo puede ser efectiva si los detectores conformes a las normas que leen y responden a la impresión están incorporados en los dispositivos de lectura y grabación; si no es así, la impresión no será detectada. Una de las dificultades de este sistema es que debe conservarse después de que el contenido haya sido comprimido sin pasar a ser visible o audible una vez descomprimido.

[Sigue el Anexo B]

ANEXO B

DESCRIPCIÓN DE LA TECNOLOGÍA CSS Y SU APLICACIÓN AL VIDEODISCO DIGITAL (DVD)

La tecnología CSS es la combinación de un algoritmo privado y una serie de claves relacionadas con la obra individual objeto de protección, el disco en el cual se encuentra la obra, y el fabricante de un dispositivo de descodificación. En su aplicación a la informática, la relación entre el lector de DVD y el sistema de descodificación del ordenador anfitrión está regulada por un protocolo de autenticación y una codificación adicional de las claves durante el proceso de pasar del disco al módulo lector de descodificación. La información sobre protección de ejemplares se introduce en los datos utilizando posiciones definidas por el libro de formato DVD y que después utiliza el programa de codificación.

Desde el punto de vista de la codificación, cuando una compañía cinematográfica desea que una de sus obras quede protegida por este sistema, dicha compañía manda a una de las compañías que preparan el contenido para el formato DVD que codifique la obra. En el caso de que una compañía cinematográfica cuente con una unidad que efectúe el formato del contenido y a continuación la codificación, la propia compañía debe ser titular de una licencia, pero si esta compañía contrata a otra para llevar a cabo la codificación, entonces la compañía no necesita ser titular de una licencia. La compañía cinematográfica o a quien ésta haya designado pueden escoger unas claves para el disco y el título que sean únicas, y pueden cambiarlas tanto o tan poco como lo deseen. La clave del título se utiliza para codificar el contenido, y la del disco para codificar la del título. MEI aún tiene el módulo ox” que codifica la clave del disco. El propietario del contenido o a quien éste haya designado manda las dos claves a MEI para codificar el “conjunto” de claves que usa el módulo. El intercambio se realiza utilizando medios seguros, y la información resultante se coloca en una parte del disco a la que una unidad sin licencia para este sistema no suele tener acceso.

Desde el punto de vista del dispositivo lector, cualquier empresa que utilice la información confidencial o muy confidencial para fabricar su producto debe ser titular de una licencia y debe obtener una licencia para cada categoría de la especificación CSS que exige para su producto. A las compañías que están fabricando el producto de descodificación en sí se les asignan unas claves para dicho producto. Estas claves son las que utiliza MEI durante el proceso de codificación del conjunto de claves.

[Sigue el Anexo C]

ANEXO C

CONTROL DE LECTURA A ESCALA REGIONAL PARA EL DISCOVIDEO DIGITAL (DVD)

Si bien la introducción del DVD era una perspectiva muy emocionante, el efecto fue que los sistemas de distribución de las compañías cinematográficas se podían ver totalmente desorganizados. La tecnología del DVD era verdaderamente mundial, con un formato que no cambiaba según las diferentes normas locales de televisión y que permitía ver fácilmente películas en televisores y monitores de ordenador en varias lenguas según la elección del consumidor. Por lo tanto, una película en un disco DVD estrenada en un lugar se podría ver inmediatamente, sin suponer grandes dificultades para el consumidor, en todas las partes del mundo. Los problemas de esta tecnología eran: primero, que a menudo empresas distintas controlaban los derechos pertinentes para la distribución de la película en distintos países y, segundo, que las compañías cinematográficas con frecuencia calculaban que los estrenos de la misma película se hiciese en momentos distintos en distintas partes del mundo. Es decir, una película que iba a ser “la película del verano” se estrenaría en el hemisferio norte en julio pero se esperaría hasta enero siguiente antes de estrenarla en el hemisferio sur. Sin embargo, para cuando se estrenase la película en las salas del hemisferio sur, era probable que ya se hubiese estrenado en DVD para venderla o alquilarla a los consumidores del hemisferio norte. Las compañías cinematográficas estaban muy preocupadas de que la consecuencia fuese que los discos puestos a la venta en el hemisferio norte se mandasen al hemisferio sur y que el estreno en las salas del sur se viese menoscabado de forma importante por el influjo de discos DVD que los consumidores podían ver en sus hogares.

Por estas dos razones (la cuestión jurídica de control de los derechos de distribución y la estructura de los estrenos del comercio cinematográfico), las compañías cinematográficas insistieron en que el DVD adoptase de algún modo un sistema de lectura a escala regional, para que así un disco puesto a la venta en una región no funcionase con los sistemas de reproducción utilizados en otras regiones. Una vez más, esta estructura tenía como objetivo hacer que la gente honesta lo siguiese siendo, más que crear un sistema infalible de impedir la utilización de un disco codificado para una región con productos de lectura vendidos en otras regiones. La situación se complicó aún más debido a los mecanismos de distribución que utilizaban las empresas de dispositivos, es decir, el fabricante de un lector DVD para un ordenador o la UPC de un ordenador no podían saber en el momento de la fabricación de dicho producto dónde se acabarían vendiendo el lector o la UPC. Muchas compañías informáticas distribuyen a escala mundial y suelen enviar sus productos de un mercado a otro en función de la demanda. Sostuvieron que no se les podía exigir que designaran de forma inalterable un lector o una unidad UPC determinados para una región dada en el momento de la fabricación. Así pues, el sistema debía ser lo bastante flexible para ajustarse a este problema. Una vez más, el CPTWG se reunió durante varias semanas para debatir acerca de varias formas de cumplir los objetivos de las industrias cinematográfica e informática.

El resultado final fue un compromiso que, a continuación, se recomendó a los encargados de idear un régimen jurídico mediante el cual se pudiese exigir el cumplimiento de varias normas. Dicho compromiso era que los consumidores podían reinicializar los ordenadores hasta 25 veces por consumidor. No obstante, iba a resultar algo complejo diseñar y poner en práctica este sistema, por lo que debía permitirse un sistema alternativo en la primera fase de los sistemas informáticos de lectura DVD. En la primera fase, los ordenadores

podían estar inicializados para una región determinada mediante un dispositivo de soporte lógico que se podía programar en el momento en que el consumidor instalaba el ordenador, resolviendo así las preocupaciones de distribución de las empresas informáticas. Una vez más, el CPTWG carecía de los medios necesarios para poner en práctica o exigir la aplicación de este sistema. Por lo tanto, la licencia CSS permitió poner en práctica los requisitos para llevar un control a escala regional de la lectura. Los fabricantes de equipos que solicitan una licencia para que sus productos puedan leer discos DVD codificados con el CSS está obligados por esa licencia a prever un control de lectura a escala regional en sus productos.

[Fin del Anexo C y del documento]