S

OMPI

WCT-WPPT/IMP/2
ORIGINAL: Francés
FECHA: 23 de noviembre 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

LA PROTECCIÓN LEGAL DE LOS SISTEMAS TECNOLÓGICOS

Estudio presentado por el Profesor Alain Strowel y la Sra. Séverine Dussolier

ÍNDICE

Introducción y ámbito del estudio

En diciembre de 1996, la comunidad internacional negoció y adoptó, en el seno de la Organización Mundial de la Propiedad Intelectual, dos importantes tratados cuyo objetivo principal era adaptar el marco jurídico del derecho de autor y los derechos conexos a las nuevas tecnologías.[1] Dos de las disposiciones de estos Tratados establecieron un nuevo tipo de protección relacionado con las medidas tecnológicas mediante las cuales se protegen las obras. Varios Estados ya han incorporado estas disposiciones particulares a sus legislaciones nacionales, y otros finalizarán este proceso próximamente.

El objeto del presente estudio es, por un lado, analizar de forma comparativa estas disposiciones nacionales o regionales distintas, su alcance y su ámbito de aplicación y, por otro, presentar otros textos que ofrecen una protección similar para las medidas tecnológicas.

Se tratará con especial atención la cuestión de la interacción de las limitaciones del derecho de autor y de la protección jurídica de estas tecnologías, así como la definición de los elementos necesarios para ofrecer una protección adecuada y eficaz contra su elusión.

A. TIPOLOGÍA DE LAS MEDIDAS TECNOLÓGICAS DE PROTECCIÓN

Las tecnologías que los autores y otros titulares de derecho pueden utilizar para proteger sus obras y prestaciones[2] en la sociedad de la información son sumamente diversas. Algunas de ellas se concibieron especialmente para responder a la amenaza que el entorno digital representaba para el derecho de autor; otras se crearon para proteger indiferentemente cualquier tipo de contenido digital, estuviese o no sujeto al derecho de autor.

Resulta difícil confeccionar una lista exhaustiva de las medidas tecnológicas existentes o en desarrollo, del mismo modo que es imposible predecir el futuro de estas tecnologías en la esfera de la protección de las obras sujetas al derecho de autor.[3]

Por esta razón, hemos decidido presentar y agrupar las medidas tecnológicas de protección del derecho de autor y los derechos conexos en cuatro grandes categorías, según el tipo de función que tienen principalmente estos dispositivos. Así pues, podemos distinguir las medidas que protegen efectivamente un acto sujeto al derecho exclusivo del autor, los sistemas de acceso condicionado, los dispositivos de marcado e identificación y los sistemas de gestión electrónica de los derechos. Para cada categoría se presentarán brevemente ejemplos puntuales de tecnologías.

I. Las medidas tecnológicas que protegen los derechos de los autores

---

[1] REINBOTHE, J., MARTIN-PRATT, M., VON LEWINSKI, S.: *The new WIPO Treaties: a First Résumé*, *E.I.P.R.* 1997/4, pág. 173; LUCAS, A.: *Droit d'auteur et numérique*, Droit@Litec, 1998, pág. 270 y siguientes.

[2] En adelante, por razones de comodidad, hablaremos únicamente de la protección del derecho de autor en cuanto a las obras, sin mencionar necesariamente la protección de diversas prestaciones u objetos que se realiza por medio de los derechos conexos.

[3] GERVAIS, D.: *Gestion Électronique des Droits et Systèmes d'Identificateurs Numériques*, Comité Asesor de la OMPI sobre la gestión del derecho de autor y los derechos conexos en las redes mundiales de información, primera sesión, Ginebra, 14 y 15 de diciembre de 1998.

Se trata de los dispositivos tecnológicos que impiden que se lleve a cabo cualquier acto o uso sujeto a los derechos exclusivos de los derechohabientes, como la impresión, la comunicación al público, la copia digital, la alteración de la obra, etc. Hacemos referencia sobre todo a los sistemas anticopia, cuya función principal es impedir que se haga una copia de la obra o del objeto protegido, ya sea únicamente digital o analógica. Por ejemplo, el **dongle**, que se usa principalmente en el ámbito de los programas informáticos, es generalmente un elemento del equipo físico (*hardware*)[4], una especie de llave que se conecta al puerto de serie del ordenador. En ese momento, cualquier programa protegido por este sistema se conecta a esta llave para comprobar cuáles son los derechos del usuario. Se considera que el principio de los*dongles* es un precursor de la tecnología de las **tarjetas inteligentes** o ***smart cards*** que autorizan el almacenamiento de una cantidad mayor de información. Además, estas tarjetas pueden contener unidades de pago previamente abonadas. A diferencia de los *dongles*, cuyo uso, hasta la fecha, se limita a los programas de ordenador de coste elevado, no cabe duda de que las tarjetas inteligentes se usarán cada vez más con los programas de ordenador, así como con otras obras ofrecidas al público en general. Estas dos tecnologías tienen dos objetivos a la vez: el acceso a la utilización y el control de ésta, en particular de la copia.

El ***Serial Copy Management System*** es un sistema que se usa principalmente en los Estados Unidos de América (EE.UU.) en los dispositivos digitales de grabación sonora como las DAT y los minidiscos. Esta tecnología permite que el dispositivo descodifique las señales sonoras integradas en el soporte y, en particular, los datos relativos a las protección de éste. El sistema autoriza la realización de una sola copia digital a partir del original, e impide cualquier copia posterior. Un sistema similar, el *Content Scrambling System*[5], basado en la técnica de la criptografía, ha sido introducido en el *videodisco digital* (*DVD*) para evitar toda reproducción.

2. Los sistemas de acceso

Uno de los mayores problemas de las redes digitales es la seguridad de los accesos a la información y al contenido protegidos, ya que existe el doble objetivo de garantizar una remuneración y proteger el derecho de autor de la obra de este modo protegida. En consecuencia, se han creado varios sistemas para garantizar y proteger el acceso a una obra, a un conjunto de obras, o incluso a un servicio que incluya, entre otras cosas, obras protegidas. El modo de desactivar el mecanismo de control del acceso es abonando un importe, o cuando se han cumplido las otras condiciones de la licencia acordada con los titulares de derecho. El dispositivo de acceso sólo puede controlar el acceso inicial y a continuación dejar libre la obra a todo uso que de ella se haga, o bien comprobar, cada vez que se accede a ella, que las condiciones establecidas se respetan. Asimismo, se pueden establecer fácilmente accesos distintos en función del tipo de usuario, lo cual constituye una de las grandes ventajas de estos sistemas. Por ejemplo, una universidad puede haber obtenido acceso a una obra o a una colección de obras para un número determinado de estudiantes durante el plazo de un año a cambio de un precio global anual. En este caso, el sistema comprobará la existencia de la clave de descodificación en los ordenadores de la universidad o el uso de una contraseña

[4] También puede ser un disquete que se introduce en el ordenador cuando el usuario desea utilizar el programa. Éste sólo funcionará a condición de que el usuario esté en posesión de dicho disquete.

[5] MCCULLAGH, D.: *Blame US Regs for DVD Hack, Wired News*, 11 de noviembre de 1999.

acordada por contrato, e incluso la identidad del estudiante. Al contrario, la misma tecnología puede conceder el acceso repetidas veces a un particular a cambio de un nuevo pago cada vez, que será proporcional a la frecuencia de utilización.

Son muchas las tecnologías que desempeñan esta función: la criptografía, las contraseñas de *cajas de conexión* (*set-top-boxes*), las cajas negras (*black boxes*), las firmas digitales o los sobres digitales.[6] El procedimiento de la **criptografía** es muy conocido. Se puede definir, siguiendo la ley francesa sobre la regulación de las telecomunicaciones, como "*la transformación, con la ayuda de convenciones secretas, de información o señales claras en información o señales ininteligibles para terceros, o a realizar la operación inversa gracias a medios concebidos a tal efecto*".[7] En el mundo digital, la codificación y la descodificación se llevan a cabo mediante algoritmos cuyo grado de complejidad es variable. Las **firmas digitales** son una aplicación particular de la criptografía utilizada para certificar e identificar un documento.[8] Dentro del marco de la protección del derecho de autor, esta tecnología se usa principalmente para proteger las transmisiones de las obras a través de las redes y para impedir el acceso a la obra a toda persona no autorizada. La clave de descodificación se proporciona previo pago del importe o en función de otras condiciones a las que está sujeto el uso de la obra.

El **sobre digital** o **contenedor digital** es una aplicación de la criptografía en virtud de la cual se "introduce" una obra en un sobre digital que contiene información relativa a la obra y las condiciones de uso de ésta. El sobre se abre y el usuario puede acceder a la obra sólo si estas condiciones (como el pago de un importe establecido, el uso de una contraseña, etc.) se cumplen.

3. Los dispositivos de marcado y de impresión con filigrana (*watermarking*)

Existe una gran cantidad de técnicas que pueden desempeñar la función de identificación y marcado de las obras.[9] Son varios los objetivos de estas técnicas: el principal es servir de soporte, de forma visible o invisible, para la inserción de datos relativos a la obra, ya sea el título de la obra, la identidad de su creador y del titular de los derechos, o las condiciones de utilización. Esta función queda en particular protegida por el Artículo 12 del Tratado de la OMPI sobre Derecho de Autor, que hace referencia a la protección de la información sobre la gestión de derechos. Nos referimos aquí, sobre todo, al procedimiento de **impresión con filigrana** que permite insertar cierta información en el código digital de la obra. El marcado es en general invisible e inaudible. Esta inscripción invisible se realiza mediante la técnica de la esteganografía, que se puede definir como "*el arte y la ciencia de comunicar de tal forma que la existencia misma de la comunicación queda oculta*".[10] La

---

[6] Los *dongles* y las tarjetas inteligentes (véase arriba) también pueden tener la función de control de acceso.

[7] Ley 90-1170 de 29 de diciembre de 1990, Boletín Oficial del Estado [Francia], 30 de diciembre de 1990, pág. 16439.

[8] HUBIN, J., POULLET, Y., con la colaboración de LEJEUNE, B. y VAN HOUTTE, P.: *La Sécurité informatique, entre technique et droit*, "Cahier du CRID", núm. 14, Story-Scientia, 1998.

[9] DUSOLLIER, S.: *Le droit d'auteur et son empreinte digitale, Ubiquité*, núm. 2, mayo de 1999, págs. 31-47.

[10] LEYMONERIE, R.: *Cryptage et Droit d'auteur, Les Cahiers de la Propriété Intellectuelle*, 1998, vol. 10, núm. 2, pág. 423; véase también GUINIER, D.: *La sténographie, De l'invisibilité des*

[Sigue la nota en la página siguiente]

utilización de tinta invisible es un ejemplo de esta ciencia milenaria tomada del mundo analógico. En un entorno digital, la impresión con filigrana modifica ciertos bits denominados "inútiles"[11] de una imagen o de un sonido. Con la ayuda de un programa informático adecuado, se puede extraer y descifrar este código digital. Generalmente esta forma de marcado es indeleble y se encuentra en todas y cada una de las partes de la obra, incluso después de que ésta haya sido alterada o recortada.

Sin embargo, estas tecnologías tienen otras características que permiten proteger más o menos directamente el derecho de autor. En primer lugar, en algunos casos el marcado es perfectamente visible: se inserta claramente una "marca" en la muestra de la obra, de forma similar al término "COPIA" que figura en los billetes de banco falsos o en otros documentos oficiales. Esta práctica, también denominada *fingerprinting*, está bastante generalizada entre las agencias de fotografía, que insertan de este modo su nombre o logotipo en un ejemplar de una foto para llevar a cabo campañas publicitarias, y sólo facilitan la imagen libre de esta marca previo pago del importe previsto. Lo mismo sucede con determinados museos o archivos en línea, en los que las reproducciones de las colecciones se adornan con el sello del museo.[12] La impresión con filigrana visible desempeña en este caso una función de protección contra la copia en la medida en que este marcado totalmente evidente conlleva una reducción del valor de lo que es accesible gratuitamente en la red.

También es posible introducir un número de serie digital diferente en cada ejemplar distinto de la obra distribuido a los usuarios. En este caso, si más tarde se encuentra una copia pirata en el mercado, se podrá saber cuál ha sido el ejemplar original a partir del cual se ha hecho la falsificación. Este marcado de cada imagen permite volver hasta la fuente de las copias no autorizadas de la imagen por medio de un fichero que retoma los números de serie y los usuarios a los que se ha concedido una licencia para acceder a estas imágenes marcadas. Aquí, la función básica de la técnica de protección es aportar elementos que se puedan considerar pruebas en cuanto a la falsificación. Finalmente, una última función de la impresión con filigrana es la de autentificar el contenido marcado, en particular asegurando que la obra se conserva íntegra.

4. Los sistemas de gestión electrónica

Los dispositivos de gestión electrónica son todas las tecnologías que garantizan la gestión de los derechos en las redes mediante el permiso para conceder licencias de utilización en línea y el control de la utilización de las obras. Estos dispositivos también pueden desempeñar otras funciones, como la repartición de los derechos percibidos, la recaudación de los pagos, el envío de facturas, la preparación de bases de datos sobre los perfiles de los usuarios, etc. Un ejemplo de ello son los **agentes electrónicos** que hace poco

---

[Continuación de la nota de la página anterior]

communications digitales à la protection du patrimoine multimédia, Expertises, junio de 1998, págs. 186-190.

[11] Estos bits son inútiles en el sentido de que las imágenes y los sonidos contienen un gran número de bits cuya supresión o modificación no tienen ninguna consecuencia perceptible para el oyente o el espectador. Por ejemplo, en el caso de una obra sonora, la línea de código digital que permite el marcado se inserta en los bits de frecuencia inaudibles para el oído humano.

[12] Un ejemplo de ello es la Biblioteca del Vaticano, en la que los documentos más valiosos están digitalizados y puestos en línea a disposición del público, si bien han sido cubiertos con el sello del Vaticano, lo cual impide que se vuelvan a utilizar con fines comerciales.

hicieron su aparición en el mercado.[13] Han sido creados para desempeñar muchas funciones en las redes, y algunos de ellos están programados para negociar y concertar contratos electrónicos.[14] Esta tecnología empieza a aplicarse también al derecho de autor en la medida en que estos agentes acompañan la difusión de la información protegida en Internet para mostrar las condiciones de las licencias de utilización y al mismo tiempo recibir y gestionar la aceptación o el *clic* de los usuarios. Otros agentes más potentes gestionan completamente de forma automatizada la distribución y la utilización de la obra, en particular mediante un sistema de pago electrónico integrado, la renovación de las licencias de utilización, o dan información precisa acerca de la utilización (¿qué obras se han copiado, imprimido, ampliado, descargado?; ¿cuántas veces?), con el doble objetivo de facturar de forma adecuada y proporcional al uso real y de establecer elementos de comercialización que se puedan usar posteriormente (¿qué usuario aprecia un tipo determinado de música?). También podemos imaginar una situación en la que los agentes mencionados hagan la repartición de los derechos destinados a los autores, a los artistas intérpretes y a otros titulares de derechos en línea. Cuando los agentes se contentan con controlar la utilización de las obras y gestionar la frecuencia de las consultas de las obras y de los sitios Web, e incluso elaboran perfiles precisos de los usuarios, a menudo se habla de **sistemas de medición**.

Finalmente, los ***Electronic Right Management Systems*** o ***ERMS*** (Sistemas Electrónicos de Gestión de Derechos) sin duda son las medidas de protección de las que más se habla, aunque conviene abstenerse de creer que se trata de una tecnología específica. Los ERMS (también llamados ***ECMS*** - *Electronic Copyright Management Systems*) son más bien una combinación de varios dispositivos y tecnologías cuyo objetivo es desempeñar varias funciones.[15] Así pues, incluso un usuario legítimo puede asociar un dispositivo de criptografía que bloquee el acceso a la obra con un sistema anticopia que impida la reproducción de ésta. También se pueden integrar en el mismo programa informático la técnica de la impresión con filigrana (véase más arriba) y un sistema de licencia y pago electrónicos. Por lo general, la función principal de los ERMS es gestionar las utilizaciones y las licencias de las obras en línea, y como tales consideramos que forman parte de la categoría de los dispositivos de gestión.

Asimismo, las tecnologías que actualmente se han creado y a las que los titulares de derechos podrían recurrir para proteger sus obras cumplen varias funciones más marginales, algunas de las cuales se alejan aún más del ámbito estricto de la propiedad intelectual. Éstas son, entre otras:

- la mención de condiciones de utilización de las obras;
- la transmisión segura de la información;
- la prueba de la recepción de la información y de la identidad de la persona que ha recibido legítimamente dicha información;

---

[13] JULIA-BARCELO, R.: *Electronic contracts= A new legal framework for electronic contracts: the EU electronic commerce proposal, C.L.S.R.*, 06/1999, núm. 15/3, págs. 147-158.

[14] GAUTHRONET S. Y NATHAN, F.: *On-line services and data protection and the protection of privacy*, Estudio realizado por cuenta de la Comisión Europea, DG XV, pág. 31.

[15] LEDGER, M. Y TRIAILLE, J.P.: *Dispositions contre le contournement des dispositifs techniques de protection*, en *Copyright in Cyberspace*, ALAI Study Days, Amsterdam, junio de 1996, Ed. ALAI, 1997. <http://www.droit.fundp.ac.be/espacedroit/textes>; GERVAIS, D.: *Electronic Right Management Systems (ERMS), The next logical step in the evolution of rights management*, (1997), véase http://www.copyright.com/stuff/ecms_network.htm.

- el pago;
- la grabación y el seguimiento de las utilizaciones, en particular con el objeto de un pago adecuado y con fines de comercialización.

Estas funciones son fundamentales para el buen control y remuneración de los titulares de los derechos. No obstante, las tecnologías que aseguran el buen funcionamiento de estos otros aspectos de la transacción entre un autor y un usuario no quedarán forzosamente cubiertas por las disposiciones legales que protegen las medidas tecnológicas. Será necesario, pues, encontrar una base jurídica distinta para demandar a posibles falsificadores de estos sistemas complementarios. Este aspecto queda fuera del marco del presente estudio.

B. DISPOSITIVOS LEGALES DE PROTECCIÓN DE LOS SISTEMAS TECNOLÓGICOS

Hemos visto hasta qué punto la tecnología que usarán los autores y otros titulares de derecho para proteger sus obras desempeña generalmente distintas funciones, y que puede ofrecer seguridad y gestionar electrónicamente una gran cantidad de material e información digital que pueden no estar protegidos por un derecho de propiedad intelectual. Se puede utilizar el mismo sistema de control de acceso para sitios Web que contengan música, información financiera o para la difusión por Internet de programas de televisión. Ello tiene una doble consecuencia.

Por un lado, distintos operadores utilizan actualmente y utilizarán en el futuro las tecnologías con fines distintos. Por lo tanto, se pueden proteger legalmente dichas técnicas mediante textos distintos de los que hacen referencia a la propiedad intelectual.

Por otro lado, los sistemas y mecanismos de elusión de estas tecnologías aparecen en el mercado para eludir un tipo de tecnología que se puede usar indiferentemente con distintos fines. Así pues, el objetivo principal de estos dispositivos ilícitos no es forzosamente atentar contra una información protegida por el derecho de autor o los derechos conexos. En consecuencia, el arsenal jurídico debería prever sanciones fuera del marco estricto de la propiedad intelectual. Por ejemplo, un pirata o *hacker* puede intentar anular la protección específica de información protegida por el derecho de autor (pensemos, por ejemplo, en las personas que recientemente han revelado en Internet cómo eludir la protección anticopia de los DVD), y también puede crear un dispositivo de elusión de una medida de seguridad, el cual se podría utilizar posteriormente con el fin de cometer infracciones con respecto al derecho de autor. Para prohibir estos dispositivos, los titulares de derecho podrían remitirse a textos legales distintos de los Tratados de la OMPI.

Por esta razón nos proponemos, tras haber estudiado en derecho comparado las disposiciones legales que protegen específicamente los derechos intelectuales (punto 1), dar una idea general de otras disposiciones legales mediante las cuales se podría sancionar la elusión de tecnologías que protegen el derecho de autor, como la Directiva europea relativa a la protección de los servicios de acceso condicionado (punto 2), y también ciertas disposiciones nacionales en materia de criminalidad informática (punto 3).

1. La protección específica de la propiedad intelectual

1.1. Criterios de comparación de los dispositivos legales

Durante la Conferencia Diplomática de 1996, los Estados miembros de la OMPI no llegaron a ponerse de acuerdo en un régimen de protección muy detallado de las medidas tecnológicas de protección del derecho de autor y los derechos conexos. El texto del Tratado pide que los Estados adopten una protección jurídica "*contra la acción de eludir las medidas tecnológicas efectivas que sean utilizadas por los autores en relación con el ejercicio de sus derechos [...] y que [...] restrinjan actos que no estén autorizados por los autores concernidos o permitidos por la Ley*". El Artículo 11 del Tratado de la OMPI sobre Derecho de Autor y el Artículo 18 del Tratado sobre Fonogramas no precisan en modo alguno cómo debe organizarse esta protección[16], ni cuáles son los actos específicos que deben prohibirse. Sobre este aspecto se da libertad total a los Estados, lo cual implica el riesgo de que haya poca armonización entre las disposiciones nacionales aunque, tras un análisis, parece que los modelos estadounidense y europeo han inspirado a los otros legisladores.

Varios países han comenzado, y algunos han finalizado, la incorporación en derecho interno de las obligaciones relativas a la protección legal de las medidas tecnológicas que se derivan de los Tratados de la OMPI de 1996. Estas nuevas disposiciones nacionales o estos proyectos son de gran complejidad. Analizaremos los dispositivos legales ya adoptados según los siguientes diferentes criterios:

- **el objeto de la protección y la definición de las medidas tecnológicas**: no todas las medidas tecnológicas quedan protegidas forzosamente en todos los textos. Aunque el Tratado de la OMPI habla de forma general de las "*medidas tecnológicas efectivas que sean utilizadas por los autores en relación con el ejercicio de sus derechos*", las disposiciones nacionales a menudo son más precisas y limitan la protección mediante la definición de las medidas tecnológicas en cuestión o del criterio de efectividad que justifica la protección. También veremos que a menudo los legisladores han establecido una protección doble: para los sistemas que controlan el acceso a las obras, y para los sistemas que protegen directamente los derechos exclusivos del autor.

- **el alcance de la prohibición (acto de elusión y/o actos preparatorios para la elusión)**: los textos de la OMPI sólo parecen referirse al acto mismo de elusión de la medida tecnológica de protección. Ahora bien, los titulares de derecho y los legistadores insisten en la necesidad de una prohibición de las llamadas actividades preparatorias para la elusión que son la fabricación y la puesta a disposición del público de dispositivos de elusión. En efecto, no cabe duda de que el perjuicio causado a los titulares de derecho será mucho mayor si hay una gran disponibilidad de tecnologías de elusión en el mercado y no hay dificultad para conseguirlas. Por lo tanto, la mayor parte de las disposiciones o proyectos nacionales establecen una doble incriminación: por un lado, con respecto a las personas que eluden la medida tecnológica; por el otro, con respecto a la comercialización de los dispositivos que pueden permitir o facilitar dicha elusión.

- **el tipo de actividades preparatorias ilícitas**: por lo general, los legisladores determinan de forma estricta las actividades que pueden implicar la responsabilidad de los fabricantes de dispositivos de elusión. Por ello se

[16] REINBOTHE, J., MARTIN-PRATT, M., VON LEWINSKI, S., op. cit., pág. 173.

enumeran las actividades ilícitas, desde la fabricación hasta todos los tipos de distribución al público de los dispositivos ilícitos. En este contexto, analizaremos si la prestación de servicios de elusión también tiene un carácter delictivo.

- **las condiciones de ilegalidad de los dispositivos**: una cuestión fundamental es determinar a partir de qué momento un dispositivo *a priori* lícito se puede considerar ilegítimo. Un gran número de dispositivos electrónicos o informáticos están concebidos específicamente para eludir la medida tecnológica y se comercializan explícitamente con este fin. A otros se los puede apartar de su función *a priori* legítima para cumplir funciones menos lícitas. Resulta fundamental, pues, trazar una línea clara entre los dispositivos lícitos y los que no lo son.[17] La definición precisa y clara de lo que es ilícito es también una de las grandes preocupaciones de la industria de los equipos electrónicos, que reclama a este respecto cierta seguridad jurídica. Por ejemplo, un magnetoscopio cuya función principal es la lectura y grabación de programas audiovisuales, pero que cuenta con una función accesoria que permite eludir la protección tecnológica con que cuentan las cintas, ¿es ilegal? ¿Y qué sucede con un soporte lógico de codificación que los usuarios utilizan sobre todo para descodificar sin autorización determinadas señales? En resumen, ¿la función de elusión debe ser principal, única, predominante o sencillamente accesoria?

- **el conocimiento de la actividad ilícita como condición de la responsabilidad**: algunos textos exigen del autor que ha cometido acciones ilegítimas cierto conocimiento del atentado al derecho de autor. En ciertas legislaciones, el autor de un acto de elusión no será responsable salvo si conocía o debía conocer que de este modo estaba cometiendo una infracción del derecho de autor.

- **el futuro de las limitaciones del derecho de autor**: una de las cuestiones más polémicas en materia de protección legal de las medidas tecnológicas es la del futuro reservado a las limitaciones y excepciones del derecho de autor y, en particular, la cuestión de saber si es admisible eludir la protección tecnológica para ejercer un acto no sujeto a la autorización del autor. En realidad, la cuestión de las excepciones tiene dos aspectos. Por un lado, ¿debe tolerarse la elusión de las medidas tecnológicas que controlan el acceso y la utilización de una obra de dominio público o cuyo uso está exento en virtud de una excepción legal? Por otro lado, ¿debemos considerar ilícitas la fabricación y la comercialización de sistemas de elusión cuyo único objetivo sea la supresión de tecnologías incluidas en elementos de dominio público o que permitan valerse de excepciones?

- **la existencia de excepciones a la prohibición de elusión**: en determinados casos, la protección legal de los sistemas tecnológicos viene acompañada de

[17] VINJE, TH.: *A brave new world of technical protection systems: Will there still be room for copyright?, EIPR,* 1996, núm. 8, pág. 431.

una serie de excepciones. En este caso, la prohibición no concierne al acto de elusión y/o a la fabricación y distribución de dispositivos ilícitos.

- **la existencia de una cláusula de no obligatoriedad**: ciertos sistemas exigen un reconocimiento por parte del dispositivo encargado de la lectura, de descargar páginas de Internet o de la reproducción. En este caso, la protección está integrada en el soporte o en el código digital de la obra que envía una señal (*control flag*) al dispositivo para evitar que realice ciertas funciones (copiar, imprimir, acceder, por ejemplo). La industria de equipos electrónicos o informáticos teme que se la obligue a incluir en estos dispositivos mecanismos que permitan la interacción con dichas señales. En consecuencia, la industria electrónica defiende la introducción clara en la Ley de una disposición que les exima de adaptar sus productos a las medidas tecnológicas. Generalmente se califica a una disposición de estas características de cláusula de "no obligatoriedad".

1.2. La protección de las medidas tecnológicas en la Unión Europea:

a) La Directiva sobre la protección de programas de ordenador y la incorporación de ésta en los Estados miembros

La Unión Europea estudió por primera vez la protección legal de las medidas tecnológicas durante la redacción de la Directiva de 19 de mayo sobre los programas informáticos. En el apartado 1 (c) del Artículo 7 se obliga a los Estados miembros a incriminar a las personas que "*pongan en circulación o tengan con fines comerciales cualquier medio cuyo único propósito sea facilitar la supresión no autorizada o la elusión de cualquier dispositivo técnico que se hubiere utilizado para proteger un programa de ordenador*". [18]

La medidas tecnológicas que en este caso se protegen no aparecen realmente definidas en el texto europeo. Sólo se tienen en cuenta de forma vaga los dispositivos técnicos que protegen los programas de ordenador. Se podría considerar, pues, que al aplicarlos a los programas informáticos, la mayor parte de los sistemas que hemos mencionado más arriba caben en esta definición, estén relacionados con la protección del acceso al programa o con la copia de éste.

En esta disposición no se considera el acto de elusión en sí. Sólo son ilícitas las llamadas actividades preparatorias; en el caso de este texto, son ilícitas la puesta en circulación y la tenencia con fines comerciales. La puesta en circulación se puede llevar a cabo mediante la venta, la oferta al público, el alquiler, etc.

Los dispositivos y sistemas cuya puesta en circulación está prohibida son *cualquier medio* cuyo *único propósito* sea facilitar la supresión o la elusión del dispositivo técnico. Este criterio es a la vez amplio y bastante limitado. Por un lado, el término "cualquier medio" parece indicar que tiene en cuenta un gran abanico de mecanismos, programas informáticos, elementos de un sistema y dispositivos. Por otro lado, el criterio del "único propósito" reduce de forma importante el ámbito de los dispositivos que se consideran ilícitos. Por ejemplo, la

[18] Directiva sobre la protección jurídica de programas de ordenador de 14 de mayo de 1991, D.O. L 122, 17.5.1991.

prohibición no se aplicará a un programa informático que tenga un propósito perfectamente lícito pero que, de forma accesoria, permita eludir la medida tecnológica, aunque resulte evidente que el éxito de este programa entre los usuarios se base sobre todo en esta función accesoria. En consecuencia, el criterio del propósito único conlleva la exención de la prohibición para una gran cantidad de sistemas.[19]

Sin embargo, Alemania ha interpretado este criterio de forma muy amplia,[20] y se consideró que el propósito único de la aplicación, y no del programa en conjunto, era suficiente para prohibir la distribución de dicho programa informático que permitía la elusión. En consecuencia, esta interpretación amplia del texto permitiría la prohibición de los programas que tenían una aplicación cuyo fin único era la elusión, independientemente de que el programa tuviese también otros fines.

Por lo demás, las incorporaciones de esta disposición en los Estados miembros no se alejan demasiado del texto de la Directiva. Por ejemplo, Alemania introdujo en su Ley sobre Derecho de Autor una disposición que prohibe los medios que facilitan la anulación o la elusión no autorizadas de las medidas tecnológicas que protegen los programas.[21] La Ley belga castiga a "*aquellos que ponen en circulación o tienen, con fines comerciales, cualquier medio cuyo único propósito sea facilitar la supresión no autorizada o la elusión de los dispositivos técnicos que protegen el programa*".[22]

La propuesta de Directiva europea relativa a los derechos de autor en la sociedad de la información, que se presentará a continuación, prevé que la protección jurídica que en ella se promulga no afecte en modo alguno las disposiciones específicas de protección previstas en la Directiva sobre la protección jurídica de programas de ordenador. Sin embargo, sería ilógico conservar este sistema que establece una protección limitada para los dispositivos cuyo único propósito es la elusión de programas de ordenador, mientras que la futura Directiva sobre Derecho de Autor introducirá una protección más amplia para todos los otros tipos de obra.

b) Propuesta de Directiva sobre el derecho de autor y los derechos conexos en la sociedad de la información

El Artículo 6 de la propuesta revisada de Directiva relativa a la armonización de determinados aspectos de los derechos de autor y derechos conexos en la sociedad de la información[23] dice:

"*17. Los Estados miembros establecerán una protección jurídica adecuada frente a la elusión sin autorización de cualquier medida tecnológica efectiva destinada a proteger el derecho de autor o los derechos conexos al derecho de autor establecidos por la ley, o el derecho sui generis contemplado en el Capítulo III de la Directiva 96/9/CE del Parlamento*

[19] VINJE, TH., op. cit., pág. 431.
[20] RAUBENHEIMER, A.: *Softwareschutz nach den Vorschriften des UWG, CR,* 1994, pág. 264.
[21] Apartado f del Artículo 69, *Gesetz über Urheberrecht und verwandte Schutzrechte.*
[22] Artículo 10 de la Ley belga de 30 de junio de 1994 mediante la cual se incorpora al derecho belga la Directiva europea de 14 de mayo de 1991.
[23] Propuesta modificada de Directiva sobre la armonización de determinados aspectos de derecho de autor y derechos conexos en la sociedad de la información, COM (1999) 250 final de 21 de mayo de 1999.

Europeo y del Consejo [Directiva relativa a las bases de datos] que la persona ejecute con conocimiento o con motivos razonables para pensar que persigue este objetivo.

2. Los Estados miembros establecerán una protección jurídica adecuada frente a todas aquellas actividades, incluida la fabricación o distribución de cualquier dispositivo, producto o elemento o la prestación de servicios, no autorizadas, que:

a) sean objeto de una promoción, de una publicidad o de una comercialización con el fin de eludir la protección o

b) tengan como principal razón para su comercio o su uso limitado eludir la protección o

c) estén principalmente concebidos, producidos, adaptados o realizados ante todo para permitir o facilitar la elusión de la protección,

de cualquier medida tecnológica efectiva destinada a proteger el derecho de autor o los derechos conexos (...) o el derecho sui generis (...)”.

Actos prohibidos

En el texto de la propuesta de Directiva, tras haber pasado por el Parlamento Europeo, se decidió incriminar a la vez el acto de elusión y las actividades preparatorias. La propuesta inicial era algo vaga a este respecto en la medida en que se tenían en cuenta “todas las actividades”. En este punto, el artículo se subdivide en dos apartados distintos: en uno se incrimina el acto de elusión sin autorización, y en el otro las actividades de fabricación y distribución de dispositivos no autorizados.

Objeto de la protección

Ya se trate de la elusión o de la distribución de dispositivos de elusión, las medidas tecnológicas protegidas se definen como “toda técnica, dispositivo o componente que, en su funcionamiento normal, esté destinado a prevenir o impedir la violación del derecho de autor o los derechos conexos (...) o el derecho sui generis (...)”. A primera vista, esta definición parece sólo referirse a las medidas que constituyen una protección directa del derecho de autor, como los sistemas anticopia.

Sin embargo, y siguiendo en este aspecto a los Tratados de la OMPI, las medidas tecnológicas deberán ser efectivas para poder disfrutar de la protección. La Unión Europea introdujo una definición de este criterio de efectividad: “*Las medidas tecnológicas sólo se considerarán “efectivas” cuando el acceso a la obra o su uso o el de otro trabajo protegido esté controlado por mediante de la aplicación de un código de acceso o de cualquier otro tipo de procedimiento de protección destinado a realizar este objetivo de protección de manera operativa y fiable, con la autorización de los derechohabientes. Estas medidas incluyen la descodificación, la desaleatorización u otra transformación de la obra”*.

Esta definición de la efectividad de las medidas tecnológicas requiere varios comentarios. En primer lugar, los criterios de efectividad son que el acceso a la obra esté controlado tecnológicamente o que lo esté la utilización de ésta. Ahora bien, el acceso a una

obra o a cualquier otro objeto protegido, *a priori*, no es en sí mismo un acto sujeto a los derechos exclusivos del autor o del titular de los derechos conexos.

Asimismo, el texto inicial de la Comisión limitaba la definición de la efectividad al acceso.[24] El Parlamento Europeo, en su intervención, añadió el criterio de la utilización, lo cual permite cubrir de forma más amplia los actos realizados por el usuario, incluidos los de reproducción y comunicación al público, sujetos a las autorizaciones de los titulares de derecho. Esta modificación está vinculada al primer apartado, en el que se insiste más claramente en que la protección se refiere a las medidas tecnológicas que protegen cualquier derecho de autor o derecho conexo. Así pues, si bajo el efecto del primer texto no estaba claro que se pudiesen proteger los sistemas anticopia, ahora parece que la nueva definición permite establecer su protección con mayor facilidad. No obstante, la protección que finalmente se ha instaurado es sorprendentemente amplia, ya que permite englobar cualquier acto que el usuario haya llevado a cabo (desde el acceso inicial a la obra hasta todos los actos de utilización posteriores). Volveremos a este aspecto en la última parte del estudio.

La definición también especifica que las medidas tecnológicas tienen que haberse aplicado a la obra u objeto protegido con el consentimiento de los titulares de derecho, ya sean éstos los autores, los artistas intérpretes, los productores o los distribuidores/vendedores. Sin embargo, no está claro el alcance de esta autorización. ¿ El distribuidor/vendedor que desee distribuir obras de forma segura mediante un sistema tecnológico de protección deberá obtener la autorización de todos los titulares de derecho? Imaginemos una biblioteca que desee que las grabaciones que presta o alquila, con la autorización de los derechohabientes o con el permiso de la ley, sean prestadas o alquiladas de una forma más segura: ¿deberá obtener una autorización específica de cada titular de derecho? Si no la consigue, ¿significa que no podrá demandar a las personas que eludan la protección? ¿ Se implica, con ello, de forma general, que sólo estarán protegidas las tecnologías que utilicen los titulares de derecho? Ello significaría dar muestras de una protección algo incompleta en la medida en que habría obras en ciertas redes de distribución legales, debidamente protegidas por tecnologías, que se podrían copiar y utilizar a pesar de esta protección. Sin embargo, debemos señalar que, en este caso, existen otros textos mediante los cuales se podría proteger estos sistemas, como la Directiva relativa al acceso condicionado, si bien veremos que, en ese caso, el acto de elusión no será sancionable en sí mismo.

Finalmente, se especifica que los procedimientos de protección incluyen la descodificación, la desaleatorización[25] o cualquier otra transformación de la obra. A nuestro juicio, la transformación de la obra podría incluir las técnicas de impresión con filigrana de la obra que, con todo, no son más que un mecanismo de protección indirecta de la obra, como vimos más arriba. Estos tres tipos de procedimientos se citan sólo a modo de ejemplo, lo cual no excluye que se puedan tomar en consideración sistemas como los *dongles* u otros que impidan la reproducción de la obra.

Tipos de actividades ilegales y responsabilidad

[24] DUSOLLIER, S.: *Electrifying the Fence: The legal protection of technological measures for protecting copyright, E.I.P.R.*, 1999, núm. 21/6, págs. 285-297.

[25] Lo cual demuestra que este texto considera principalmente los sistemas de codificación y acceso.

Hemos visto que el primer apartado del Artículo 6 ya incluye de forma explícita el acto mismo de elusión de las medidas tecnológicas en el ámbito de las actividades ilícitas. Sin embargo, en este caso, se ha añadido un elemento moral con el objeto de demandar sólo a las personas que han llevado a cabo dicha elusión del mecanismo tecnológico con conocimiento de causa. El texto habla de "*con conocimiento o con motivos razonables para pensar que [la persona] persigue este objetivo [la elusión sin autorización]*". Estamos ante una condición de conocimiento que no aparece en la infracción paralela de fabricación de dispositivos de elusión.

En el caso de las actividades preparatorias, el texto europeo es muy amplio ya que se refiere de forma bastante vaga a "las actividades". La fabricación, la distribución de dispositivos ilícitos y la prestación de servicios se citan sólo a modo de ejemplo. En consecuencia, parece que queda cubierta cualquier actividad de comercialización de dichos dispositivos no autorizados. Del mismo modo, parece que también se consideran las actividades no comerciales de oferta de sistemas de elusión. Así pues, la distribución de claves de descodificación por Internet, incluso sin fin lucrativo, también se consideraría ilícita, a la manera de lo que sucede actualmente con la descodificación de la protección tecnológica del DVD.

Dispositivos ilegales

Existen tres criterios alternativos que condicionan la ilegalidad de los dispositivos y de los servicios: puede darse que el sistema o servicio sea objeto de promoción, publicidad o comercialización con el fin de eludir la protección técnica; o bien que la finalidad comercial o la utilización de dichos dispositivos sea principalmente la elusión; o que el sistema o servicio haya sido ideado, producido, adaptado o creado principalmente para permitir o facilitar la elusión.

En cierto modo, los servicios y dispositivos que se consideran son los que tienen claramente una función de elusión de las medidas tecnológicas correspondientes, independientemente de que ésta aparezca en el momento de la creación del producto, mediante la publicidad que de éste se hace, cuál sea su función principal o el modo en que se utilicen estos servicios y dispositivos.

También en este caso, como es natural, la frontera entre los sistemas legales e ilegales es borrosa y está sujeta a la estimación de los tribunales. Por ejemplo, se prohibirá el programa informático de descodificación que más se utiliza para descodificar obras protegidas. En cuanto al magnetoscopio, aunque la función de elusión sea sólo accesoria, el hecho de promocionar el instrumento con este fin será suficiente para que sea ilegal.

Límites y protección del derecho de autor

En el texto revisado de la propuesta, la Comisión Europea reitera que se deben determinar las protecciones tecnológicas con el fin de proteger un derecho de autor o un derecho conexo y, por lo tanto, aquéllas deben quedar dentro de los límites de éstos.

Además, un considerando expresa claramente que, para que la elusión se considere ilegal, no puede existir autorización de los derechohabientes, ni puede estar permitida por la ley.[26] No obstante, esto no resuelve en absoluto qué sucederá con los actos de elusión realizados valiéndose de una excepción. Los sistemas tecnológicos impiden que se efectúen actos sujetos al derecho de autor (por ejemplo, la reproducción, la comunicación o la modificación de la obra) sin ser capaces de determinar si el acto que la protección técnica impide resulta del recurso legítimo a una excepción. Además, las mismas medidas tecnológicas protegen de forma equivalente las obras protegidas por el derecho de autor y las que forman parte del dominio público.

Asimismo, el Considerando 30 no establece que la elusión sea legal si se realiza en calidad de excepción. Sería necesario que el texto precisase que el autor debe haber autorizado el acto de reproducción o de utilización posterior a la elusión, o que la ley lo permite.

La copia privada es la única que aparece regulada, por un lado en el Artículo 5, párrafo 2, b) *bis*, en el que se autoriza únicamente la copia privada digital en caso de que no existan medidas tecnológicas que la impidan y, por otro lado, en virtud del Considerando 27, que añade a este primer principio que la excepción de la copia privada no puede justificar un acto de elusión no autorizado. En consecuencia, está prohibido eludir una protección anticopia para hacer una copia privada de una obra.

El hecho de que la Comisión haya hecho caso omiso de las modificaciones del Parlamento con respecto a este punto, que proponía generalizar esta solución y aplicarla a la totalidad de las excepciones, podría querer decir que, en el estado actual del texto, las otras excepciones no desaparecen ante las protecciones técnicas, e incluso que la elusión de éstas estaría autorizada dentro de este marco.

Aunque la Comisión ha especificado en la Exposición de Motivos que la cuestión del recurso a las excepciones está reglamentada mediante el texto mismo del Artículo 6 sobre las medidas tecnológicas -en particular mediante la definición de éstas-, el cual exige una violación del derecho de autor, la cuestión dista de estar resuelta definitivamente.

Excepciones a la prohibición de elusión

A la inversa del texto estadounidense, la propuesta de Directiva no enumera una serie de excepciones a la prohibición de la elusión. Sin embargo, los Considerandos de la Directiva nos dicen que esta protección no deberá suponer un obstáculo para la investigación en criptografía, [27] ni impedir la descompilación de programas informáticos autorizada por la Directiva de 1991 que trata de la cuestión.[28] Así pues, seguirán estando permitidos los actos de elusión de las medidas tecnológicas que sirven para probar la eficacia del algoritmo de codificación, al igual que el hecho de eludir una medida de protección para descompilar el programa informático. Sin embargo, en este último caso, será necesario que la descompilación se lleve a cabo respetando las condiciones estrictas impuestas en la Directiva acerca de la protección de programas de ordenador, en particular el hecho de que la persona sea un usuario

[26] Considerando 30, al final.
[27] Considerando 30 *bis*, al final.
[28] Considerando 31, al final.

legítimo del programa y que no se pueda disponer de otra forma de la información necesaria referente a la interoperabilidad. Por último, esta descompilación sólo se podrá efectuar, al igual que la elusión de la medida tecnológica creada a tal efecto, con el único fin de conseguir la interoperabilidad del programa.

Cláusula de no obligatoriedad

Tras los debates del Parlamento Europeo, la propuesta revisada incluye actualmente en los Considerandos una cláusula de *no obligatoriedad*. En el Considerando 30 figura que la protección no puede "*impedir el funcionamiento normal de los equipos electrónicos y su desarrollo técnico; que dicha protección jurídica no debe suponer una obligación de conformar los dispositivos, productos, elementos o servicios con dichas medidas tecnológicas*". El objetivo principal de la Comisión en este caso es fomentar las negociaciones entre los titulares de derecho y la industria electrónica para conseguir incorporar las medidas tecnológicas en los equipos electrónicos e informáticos.

1.3. La protección de las medidas tecnológicas en los Estados Unidos:

a) Artículo 1002 de la Ley sobre Derecho de Autor (*Copyright Act*): la protección de los Sistemas de Gestión de Copias en serie (*Serial Copy Management Systems*)

Cuando aparecieron los primeros dispositivos que permitían la grabación y la copia de ficheros sonoros digitales, comúnmente denominados*Cinta Sonora Digital* o *DAT* (*Digital Audio Tape*), la industria discográfica estadounidense y los titulares de derecho se inquietaron al ver que aquellos sistemas permitían hacer innumerables copias de obras musicales sin que se produjera ninguna pérdida en cuanto a la calidad y con un coste mínimo.

Se adoptó entonces una modificación de la Ley sobre Derecho de Autor para imponer la inserción en las DAT de un mecanismo anticopia que impidiese hacer más de una copia digital de la obra (se trata de los *Serial Copy Management Systems - SCMS*). En aquel caso, la industria se vio obligada a ajustar su producción a los sistemas técnicos en curso en aquel momento, por lo que tenemos aquí una disposición que no respeta la condición de *no obligatoriedad*.

Esta modificación legislativa incluye también la prohibición de importar, fabricar, distribuir, ofrecer o prestar un servicio cuyo efecto o fin principal sea eludir la medida tecnológica anticopia.[29] Conviene señalar que en una decisión reciente,[30] un juez estadounidense consideró que estas disposiciones debían interpretarse de forma estricta y que, en consecuencia, no podían aplicarse a sistemas distintos de las DAT. La industria discográfica intentaba forzar a los fabricantes de lectores de ficheros MP3, como la empresa Diamond, a introducir en sus dispositivos un sistema que impidiese la copia de ficheros y la lectura de ficheros pirata.

[29] Artículo 1002 (c): "*No person shall import, manufacture, or distribute any device,or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent any program or circuit which implements, in whole or in part, a system described in subsection (a)*".

[30] *RIAA contra Diamond Multimedia System, Inc.*, núm. 98-56727 (9th Cir., junio de 1999).

b) Ley sobre Derecho de Autor en el Milenio Digital (*Digital Millenium Copyright Act*)

En octubre de 1998, el Congreso estadounidense votó la *Digital Millenium Copyright Act*, un largo texto legislativo en el que se revisa la Ley sobre Derecho de Autor. Esta reforma legislativa, concebida a la vez para incorporar los Tratados de la OMPI y regular algunos aspectos incluidos en el programa digital estadounidense,[31] trata sobre la protección de las medidas tecnológicas.

El nuevo Artículo 1201 de la Ley estadounidense de Derecho de Autor prevé lo siguiente:

(a) VIOLATIONS REGARDING CIRCUMVENTION OF TECHNOLOGICAL MEASURES

> *(1) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2 -year period beginning on the date of the enactment of this chapter. (...)*
>
> *(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that:*
>
> > *(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;*
> >
> > *(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or*
> >
> > *(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.*

(b) ADDITIONAL VIOLATIONS-

> *(1) No person shall manufacture, import, offer to the public, provide or otherwise traffic in any technology, product, service, device, component, or part thereof that*
>
> > *(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;*

[31] GINSBURG, J.: *Chronique des États-Unis, R.I.D.A.*, enero de 1999, pág. 147 y siguientes.

> *(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or*
>
> *(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.*

De este modo se establece una doble protección, una con respecto a los sistemas técnicos que controlan el acceso a las obras protegidas, y otra con respecto a medidas tecnológicas que protegen efectivamente un derecho exclusivo del autor. En realidad, el texto estadounidense establece tres infracciones: 1) *la elusión de medidas tecnológicas* de protección que *controlan el acceso* a las obras protegidas; 2) *la fabricación y la difusión* de medidas de dispositivos o la *prestación de servicios* que apuntan a la elusión de los sistemas de *control de acceso* y, finalmente, 3) la *fabricación y difusión* de dispositivos o la *prestación de servicios* que permitan la elusión de *medidas tecnológicas de protección de los derechos* de los autores. Estos tres aspectos merecen comentarios separados.

i) La protección de los sistemas de control de acceso

Objeto de la protección

Las medidas tecnológicas en cuestión son las que "*en el curso normal de su funcionamiento,requieren la aplicación de información, de un proceso o de un tratamiento, con la autorización de los titulares de derecho, para tener acceso a la obra*" [32] Por supuesto, esto incluye mecanismos como la codificación, el sobre digital, el *dongle* y las palabras clave.

El objetivo y la función principal de las tecnologías de que se trata es controlar el acceso a una obra, no a un ejemplar o a una copia de ésta.[33] En consecuencia, los mecanismos que permiten someter a la autorización del titular de derecho, en particular mediante el pago de un importe, cada nuevo acceso o nuevo uso de una obra que se encuentra en un soporte adquirido legalmente (por ejemplo, un programa informático en CD-ROM), estarán protegidos por este artículo. En tal caso, el usuario no podrá eludir la protección técnica unida a la obra, so pena de sanciones penales, aunque haya pagado para tener acceso. Esta ampliación de la protección más allá de los derechos tradicionales del autor ya ha suscitado comentarios en los Estados Unidos.[34] En la última parte volveremos a esta polémica, cuyas condiciones y dificultades no difieren de forma substancial de la situación europea que hemos esbozado antes.

---

[32] Traducción no oficial de "*if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work*".

[33] GINSBURG, J. op. cit., pág. 159.

[34] LITMAN, J.: *New Copyright Paradigms*, http://www.msen.com/~litman/paradigm/htm; NIMMER, D.: *Brains and other paraphernalia of the digital age, Harvard Journal of Law and Technology*, vol. 10, núm. 1, 1996, págs. 1-46; GINSBURG, J. op. cit.

Tipo de actividades ilegales

Estas nuevas disposiciones prevén sanciones para la elusión de la medida tecnológica así como para la fabricación y comercialización de dispositivos que eludan esta protección.

En lo que se refiere a la elusión, el texto no será aplicable hasta el término de un período de dos años a partir de la entrada en vigor de las nuevas disposiciones. Durante estos dos años, el *Register of Copyright* y el *Librarian of Congress* analizarán hasta qué punto esta prohibición de elusión de las medidas de protección tecnológicas puede causar un perjuicio a los usuarios de obras protegidas, así como a las excepciones al derecho de autor admitidas generalmente como utilización lícita (*fair use*), como la cita, la enseñanza, la investigación, las reseñas de actualidad, etc. Al cabo de estos dos años, ciertos tipos de obras podrán quedar exentos de la prohibición de elusión de los sistemas de acceso que los protegen para permitir un uso legítimo. Este sería el caso, por ejemplo, de los artículos científicos si se considerase que, debido a su uso frecuente en investigación, es preciso que los usuarios puedan consultarlos, incluso a pesar de las medidas tecnológicas de protección con que contarían.

Este proceso de evaluación del efecto de la prohibición se repetirá cada dos años.

La otra rama de protección de los sistemas de acceso es efectiva inmediatamente. Su objeto son la fabricación, la importación, la oferta al público, el suministro o cualquier otro tipo de comercialización de tecnologías, productos, servicios, dispositivos o elementos ilegales. Por lo tanto, tanto la prestación de servicios como la oferta de productos están cubiertos.

En cambio, ningún elemento cognitivo puede condicionar la responsabilidad de la persona que comete un acto de elusión, ni la de la que fabrica y distribuye dispositivos ilegales.

Dispositivos ilegales

Se considerarán ilegales los productos o servicios cuando hayan sido concebidos o fabricados con el fin de eludir una medida tecnológica, ya sea un control de acceso o la protección de un derecho exclusivo, cuando no tengan una finalidad comercial o un uso limitado distinto de la elusión, o cuando hayan sido objeto de una comercialización centrada en la idea de la elusión.

Excepciones a la prohibición de elusión de los sistemas de acceso y de la fabricación de dispositivos

El texto estadounidense fue objeto de grandes presiones por parte de diversas industrias y círculos interesados, así como por parte de la industria informática y electrónica en las bibliotecas. Por ello, se han establecido algunas excepciones, cuyo funcionamiento resulta a veces complejo, a la prohibición de elusión de los sistemas tecnológicos de control de acceso. Nos limitaremos aquí a señalar las principales:

- ***excepción a favor de las bibliotecas sin ánimo de lucro***: el Artículo 1201 d) prevé una excepción a la prohibición de elusión en beneficio no sólo de las bibliotecas, sino también de los archivos e instituciones de educación sin ánimo de lucro. Esta excepción se limita a la posibilidad de infringir una medida de protección tecnológica con el único fin de informarse sobre el interés de la posible adquisición de la obra protegida. También es preciso que no haya ninguna copia de esta obra disponible de ningún otro modo y que la biblioteca se deshaga del ejemplar de la obra a la que ha accedido tras haber tomado una decisión;

- ***excepción para las autoridades y los controles de seguridad***: las autoridades oficiales o policiales que eluden las medidas de protección tecnológicas con fines de investigación no estarán sujetas al régimen de la infracción. Esto resulta bastante obvio, al igual que la excepción en el marco de la comprobación de seguridad de un sistema realizada con la autorización del propietario del sistema o de la red informática;

- ***descompilación***: a semejanza de la Directiva europea sobre la protección de los programas informáticos, el derecho estadounidense renonoce al usuario legítimo de una copia de un programa la posibilidad de proceder a la descompilación del programa con el objeto de garantizar la interoperabilidad. Ahora bien, los sistemas de control de acceso podrían suprimir *de facto* esta posibilidad. En consecuencia, la ley prevé una excepción al carácter delictivo de la elusión de estas medidas tecnológicas en este contexto;

- ***actividades de investigación en materia de codificación***: el Artículo 1201 g) introduce una excepción estricta cuando la elusión es necesaria para que la investigación en materia de codificación avance, en especial mediante la identificación y la comprobación de los puntos débiles de la tecnología. Dentro de esta excepción están exentas la elusión de medidas de acceso y la creación de dispositivos ilegales;

- ***excepciones en el caso de menores***: los Estados Unidos sienten gran preocupación por el hecho de que menores de edad puedan tener acceso a material pornográfico o violento en Internet. Por esta razón la industria ha creado muchos sistemas de filtración, como los PICS,[35] para responder a estas preocupaciones. Durante los debates de la DMCA, pareció claro que estos sistemas podrían contener elementos capaces de eludir las medidas de protección tecnológicas de acceso, precisamente para comprobar la naturaleza del contenido del sitio visitado. El Artículo 1201 h) prevé que no se puede prohibir la comercialización de sistemas de este tipo por esta sola razón;

- ***protección de los datos de carácter personal***: en la medida en que la tecnología de acceso o el contenido por ella protegido contiene datos personales relativos al usuario (pensemos en las *cookies*, por ejemplo), éste

[35] LIVORY, A.: *CEE, contrôle du contenu circulant sur Internet: une approche particulière, le contrôle par l'usager et le système PICS, D.I.T.*, 06/1997, núm. 97/2, págs. 52-54; POULLET, Y.: *Quelques considérations sur le droit du cyberspace*, FUNDP, Facultad de Derecho, 1997, 27 págs.

puede eludir estas medidas tecnológicas para revelar y borrar el elemento que reúne toda esta información personal sin que lo sepa la persona concernida. Sin embargo, la excepción se limita a este único fin y no se aplicará si el operador del sistema tecnológico informa al usuario de la recopilación de datos.

Límites y protección del derecho de autor

La DMCA no regula el régimen jurídico de los actos de elusión efectuados valiéndose de una excepción permitida dentro de los límites del *fair use* pero, como ya hemos señalado, los legisladores previeron un procedimiento de evaluación del efecto de la prohibición en cuanto a las excepciones y los límites del derecho de autor. Además, la posible exención de la protección en el caso de algunas excepciones determinadas sólo se aplicará a las medidas técnológicas que controlan el acceso, y no a las medidas de protección de los derechos exclusivos. No obstante, puesto que la elusión de las medidas tecnológicas no está prohibida en el marco de las protecciones de los derechos exclusivos, la repercusión de esta diferencia de régimen es mínima.

ii) La protección de las medidas tecnológicas que protegen los derechos del autor

Objeto de la protección

El párrafo b) del artículo 1201, cuyo texto hemos citado antes, tiene como objetivo más directo la incorporación de los Tratados de la OMPI en la medida en que las medidas tecnológicas que se han tomado en cuenta son precisamente las que protegen los derechos reconocidos en virtud del derecho de autor estadounidense, es decir, los derechos de reproducción, adaptación, distribución, representación (*public performance*) o presentación pública (*public display*) de la obra. En este contexto, la protección establecida es única y tiene como objeto los fabricantes y proveedores de dispositivos de elusión. El acto de elusión en sí mismo no es, pues, reprensible, pero los actos que el usuario realice con posterioridad constituirán un atentado contra el derecho de autor. No cabe duda de que, en este caso, se estimó que una sanción adicional no se justificaba.

Las tecnologías objeto de interés son las que protegen efectivamente un derecho que el derecho de autor estadounidense reconoce al titular del derecho de autor. En particular se trata de los SCMS y de otros dispositivos anticopia.

Los actos de comercialización ilegales son los mismos que los relativos a los dispositivos de control de acceso, es decir, la fabricación, importación, oferta al público, suministro o cualquier otro tipo de comercialización de tecnologías, productos, servicios, dispositivos o elementos ilegales. Lo mismo sucede con respecto a la definición de los dispositivos ilegales, que se aplica *mutatis mutandis* a los dos tipos de tecnología (de acceso y de protección de los derechos). El criterio fundamental es también la finalidad comercial o un uso limitado distinto de la elusión.

Excepciones y medidas tecnológicas de protección de los derechos

Puesto que la elusión en sí no está prohibida, los usuarios podrán anular la protección tecnológica al realizar un acto de *fair use*. Además, nada indica que se haya autorizado la producción y distribución de los dispositivos de elusión con el único fin de eludir una protección para utilizar una obra en el marco de una excepción.

Excepciones a la fabricación de dispositivos ilegales

Únicamente la excepción en el caso de las acciones de la autoridad y de los servicios policiales se aplica también en el marco de las medidas tecnológicas de protección de los derechos.

Cláusula de no obligatoriedad

La DMCA prevé que las industrias electrónica, de telecomunicaciones e informática no deban adaptar sus productos de tal forma que puedan interactuar con las medidas tecnológicas de protección o de control de acceso.[36]

1.4. Australia: Proyecto de Modificación de la Ley sobre Derecho de Autor (*Copyright Amendment (Digital Agenda) Bill*) de 1999

También en Australia está en curso un proyecto de ley con un doble objetivo: adaptar la ley australiana sobre derecho de autor al desarrollo tecnológico e incorporar los Tratados de la OMPI. En materia de protección legal de las medidas tecnológicas, el proyecto declara:

(5B) A person must not provide a circumvention service if the person knows, or is reckless as to whether, the service will be used to circumvent, or facilitate the circumvention of, an effective technological protection measure.

(5C) A person must not:
(a) make a circumvention device; or

(b) sell, let for hire, or by way of trade offer or expose for sale or hire, a circumvention device; or

(c) distribute a circumvention device with the intention of trading, or engaging in any other activity that will affect prejudicially an owner of copyright; or

(d) by way of trade exhibit a circumvention device in public; or

(e) import a circumvention device into Australia with the intention of:

[36] Apartado c) 3) del Artículo 1201.

(i) selling, letting for hire, or by way of trade offereing or exposing for sale or hire, the device; or

(ii) distributing the device for trading, or for engaging in any other activity that will affect prejudicially an owner of copyright; or

(iii) exhibiting the device in public by way of trade; or

(f) make a circumvention device available online to an extent that will affect prejudicially an owner of copyright;

if the person knows, or is reckless as to whether, the device will be used to circumvent, or facilitate the circumvention of, an effective technological protection measure.

Objeto de la protección

Las medidas tecnológicas efectivas que son objeto de esta protección están definidas como "*a device or product, or a component incorporated into a process, that is designed to prevent or inhibit the infrigement of copyright subsisting in a work or other subject-matter if, in the ordinary course of its operation access to the work or other subject matter protected by the measure is available solely by use of an access code or process (including decryption, unscrambling or other transformation of the work or other subject-matter) with the authority of the owner or licensee of the copyright in the work or other subject-matter*".

También en este caso el elemento esencial de la definición es el acceso a la obra y no la protección de un derecho específico del autor. Al contrario que el derecho estadounidense, e incluso el europeo, no se prevé ninguna protección en paralelo para las medidas de protección tecnológicas que impiden la reproducción o cualquier otro acto de explotación sujeto al derecho de autor. Así pues, se plantea de nuevo la cuestión de la posible aplicación de este texto a los sistemas anticopia o a otras tecnologías cuya función principal no sea aumentar la seguridad y el control del acceso a la obra.

Actos prohibidos y dispositivos ilegales

Únicamente se sancionarían los actos preparatorios para la elusión, y no el acto mismo de elusión por parte del usuario. En concepto de actos preparatorios, se prohibirían la prestación del servicio de elusión, la fabricación, la venta, el alquiler, la exposición con miras a la venta, la comercialización, la distribución, la importación o la puesta a disposición en línea de un dispositivo de elusión, definido éste como "*a device (including a computer program) having only a limited commercially significant purpose or use, or no such purpose or use, other than circumvention, or facilitating the circumvention of an effective technological measure*".

El criterio es similar a los criterios europeo y estadounidense.

Sin embargo, se prevé una condición adicional de responsabilidad en la medida en que una persona que haya cometido una infracción debía saber cómo utilizar el dispositivo con fines de elusión.

Límites del derecho de autor y excepciones

El proyecto de ley australiano regula de forma totalmente nueva la delicada cuestión de cómo tratar las excepciones al derecho de autor. Efectivamente, está previsto que la prohibición de los actos de fabricación y distribución de los dispositivos de elusión o la prestación de servicio no se aplique si la persona a quien se proporciona el servicio o dispositivo firma una declaración según la cual esta persona se compromete a usarlos únicamente con un fin que permita la ley, el cual también debe figurar expresamente en la mencionada declaración. El fin permitido por la ley se define como la utilización del dispositivo o servicio para realizar un acto que se deriva de una excepción al derecho de autor o que se ha efectuado con la autorización del titular del derecho. En este contexto, a nuestro parecer, una persona podría reivindicar el uso de un dispositivo de elusión con el fin de llevar a cabo actos fuera del ámbito del derecho de autor y, así, incluso exonerar al proveedor de toda responsabilidad a este respecto. Sin embargo, existe el riesgo de que una declaración similar se convierta en moneda corriente en los contratos de suministro de estos dispositivos electrónicos y que, en consecuencia, la responsabilidad de los fabricantes acabe siendo prácticamente inexistente.

Además, en materia de fabricación y de importación de estos dispositivos, no se podrá considerar responsable al fabricante o al importador si la utilización que se haga de dichos dispositivos se limita a un fin que la ley permite.

Excepciones a la prohibición del acto de elusión

Además de la excepción general prevista cuando se trata de eludir la medida tecnológica para recurrir a una excepción al derecho de autor, el proyecto de ley prevé una excepción general a la prohibición para las autoridades o los servicios policiales.

1.5. Otros países

Según nuestra información, el Japón[37], Singapur, Hungría e Irlanda ya han incorporado los Tratados de la OMPI en materia de protección de las medidas tecnológicas o se preparan para hacerlo. No obstante, en el momento de finalizar este informe no disponemos de los textos de estos Estados.

Alemania también había introducido un proyecto de ley con el mismo objetivo, en el que se preveían sanciones para el acto de elusión, la supresión y la destrucción de los dispositivos y las medidas tecnológicas, incluidos los programas de ordenador, que protegen los derechos de los autores.[38] Al parecer, el nuevo gobierno alemán ha abandonado este proyecto.

[37] Ley de 15 de junio de 1999.

[38] Propuesta de introducción de una 5ª enmienda a la Ley alemana sobre Derecho de Autor, de 7 de julio de 1998, artículo 96a.

2. Protección de las medidas tecnológicas que controlan el acceso a servicios

Existen legislaciones fuera del ámbito estricto de la propiedad intelectual que, en ciertos casos, prestan cierta protección a los sistemas tecnológicos que los titulares de derechos podrían invocar, entre otras cosas, para proteger sus obras, en particular para controlar el acceso a ellas.

Por lo general, el objetivo de estas disposiciones es proteger los sistemas tecnológicos impidiendo y controlando el acceso a determinados servicios. Otras disposiciones similares, previstas en el pasado para los servicios analógicos en ciertos países,[39] se podrían retomar y ampliar al entorno digital y los servicios en línea debido a la convergencia de los medios audiovisuales, la informática y las telecomunicaciones.

Nos limitaremos al análisis de una Directiva europea que, a nuestro juicio, establece una protección adicional para las medidas tecnológicas que protegen el acceso a obras protegidas. Se trata de la Directiva 98/84/CE del Parlamento Europeo y del Consejo, de 20 de noviembre de 1998, relativa a la protección jurídica de los servicios de acceso condicionado o basados en dicho acceso.

El objetivo de la Directiva es proteger los servicios cuyo acceso está sujeto a ciertas condiciones, entre ellas el pago de un importe, y sancionar la comercialización de mecanismos que facilitan la acción de elusión de los sistemas de acceso condicionado. Los servicios protegidos son principalmente la radio y la televisión, así como los servicios de la sociedad de la información.

Esto podría incluir los servicios visuales o sonoros por encargo, la edición electrónica, el acceso a una base de datos en línea, un sitio con ficheros musicales, etc. En cambio, los soportes autónomos (*offline*), cuyo acceso estaría controlado por un sistema tecnológico, no quedarían protegidos por este texto.

Así pues, los titulares de derecho podrían impedir la comercialización de dispositivos que permiten la elusión de las medidas de acceso a las que dichos titulares recurren. Conviene precisar desde este momento que, a pesar de todo, el objetivo de esta Directiva no es la protección de información sujeta a la propiedad intelectual. De hecho, la propuesta inicial excluía de forma expresa las medidas tecnológicas aplicadas a las obras protegidas por el derecho de autor.[40] En su versión final, la Directiva prevé que su aplicación no perjudicará las disposiciones comunitarias en materia de propiedad intelectual que figuran en la Directiva sobre Derecho de Autor en la Sociedad de la Información (véase más arriba), lo cual no basta para olvidar todas las cuestiones sobre el posible doble uso y sobre la articulación de los dos textos y la existencia de una protección doble. Las dos directivas tienen, en principio, objetivos distintos: en uno de los casos, el objeto de la protección será la obra y, en el otro, el servicio, esté o no compuesto de obras protegidas.

---

[39] En materia de codificación de las emisiones de televisión, citemos los artículos 79-1 a 79-6 de la Ley francesa de 30 de septiembre de 1986 relativa a la libertad de comunicación, los artículos 297 a 299 de la Ley inglesa sobre Derecho de Autor, y el artículo 605 de la Ley sobre Comunicación (*Communications Act*) en los Estados Unidos.

[40] Considerando 15 de la propuesta de Directiva.

La Directiva relativa al acceso condicionado tienen como objetivo la protección de los servicios de acceso condicionado así como las tecnologías que garantizan y controlan dicho acceso. En la medida en que la propuesta de Directiva sobre Derecho de Autor define las medidas tecnológicas como las que controlan el acceso a las obras, los dos textos pueden proteger las mismas tecnologías, así como sancionar los mismos tipos de sistemas pirata. Se debe admitir que la gran mayoría de los servicios de la sociedad de la información incluirá obras protegidas por el derecho de autor o los derechos conexos y bases de datos protegidas. Una base de datos con un acceso seguro gracias a una medidad tecnológica será a la vez una obra (o un objeto protegido) y un servicio de acceso condicionado. Así pues, la protección será doble.[41]

El criterio de la remuneración por el servicio también parece fundamental para la aplicación de la Directiva relativa al acceso condicionado. No obstante, esto no significa que la remuneración deba ser anterior a la provisión del servicio, ni ser global. Así pues, un servicio de acceso condicionado que consista en una colección de fotografías en línea, y que tenga incorporado un mecanismo de medición, podría estar protegido, incluso aunque la factura en la que figure un pago en función de la utilización exacta de la fototeca se envie a intervalos regulares después de haber accedido por primera vez.

La Directiva relativa al acceso condicionado impone a los Estados miembros que prohiban la fabricación, la importación, la venta, la distribución, el alquiler, la retención con un fin no comercial, la instalación, el mantenimiento o la substitución de un dispositivo que permita el acceso no autorizado a un servicio protegido, así como la promoción de dichos dispositivos. El criterio de ilegalidad de los dispositivos de acceso no autorizado a los servicios protegidos es más estricto que en el caso de las medidas tecnológicas en materia de derecho de autor. Sólo se prohibirán los equipos o programas informáticos concebidos o adaptados con miras a permitir dicho acceso.

Es obvio que el hecho de que la protección de los servicios de acceso condicionado sea ajena al derecho de autor y a los derechos conexos impide que se puedan invocar las excepciones y limitaciones del derecho de autor para anular la protección tecnológica. Así pues, un mecanismo de criptografía podría proteger un servicio de acceso condicionado en el que hubiese obras de dominio público. Los administradores de este servicio podrían prohibir la fabricación de claves pirata de descodificación, basándose probablemente en la incorporación de la Directiva relativa al acceso condicionado y no en la futura Directiva sobre Derecho de Autor. Después de todo, el hecho de que las obras en cuestión no recibiesen protección mediante el derecho de autor no sería demasiado importante.

En consecuencia, a veces a los titulares de derecho les convendrá invocar este texto para impedir la venta de sistemas de elusión: no se les podrán objetar las excepciones y los límites del derecho de autor. Además, en el marco de la Directiva relativa al acceso condicionado, ciertas actividades como el mantenimiento, la instalación o la substitución de un dispositivo de estas características están sancionadas explícitamente, lo cual no está previsto en la propuesta de Directiva sobre Derecho de Autor.

[41] DUSSOLIER, S.: *Electrifying the fence...*, op. cit., pág. 290.

3. Disposiciones en materia de criminalidad informática

El acceso sin autorización a obras u otros objetos protegidos puede asimilarse en determinadas situaciones a una infracción que perjudica a los sistemas informáticos. Estas infracciones se recogen en el Código Penal de varios países debido a la represión de la criminalidad informática, sobre todo tras las preocupaciones que surgieron en los años 80 frente a los *hackers* y otros piratas de la informática.

El Consejo de Europa recomendaba la represión penal, mediante disposiciones específicas, de una serie de acciones que iban en contra de los sistemas y los datos informáticos.

En esta lista figuraban, entre otros, los actos siguientes:

- el fraude informático, definido como *la entrada, la alteración o la supresión de datos o de programas informáticos, o cualquier otra injerencia en un tratamiento informático, que influya en el resultado causando así un perjuicio económico o material a otra persona con la intención de obtener un beneficio económico ilegítimo para sí mismo o para un tercero o con la intención de privar ilegalmente a dicha persona de su patrimonio*;

- la falsificación en informática, que consiste en la infracción tradicional de la falsificación mediante la injerencia en un sistema informático;

- los daños que afectan a los datos o a los programas consistentes en *el daño, el deterioro o la supresión sin derecho de datos o programas informáticos*, de los que el más extendido es, por supuesto, el virus u otras bombas informáticas;

- el sabotaje informático que constituye la entrada o la injerencia en sistemas informáticos con la intención de obstaculizar el funcionamiento;

- el acceso sin autorización a sistemas informáticos que se lleva a cabo violando las normas de seguridad;

- la interceptación no autorizada de comunicaciones informáticas;

- la reproducción no autorizada de programas de ordenador o de topografías;

- la alteración ilegal de datos o programas de ordenador;

- el espionaje informático;

- el uso sin autorización de un ordenador, de un sistema o de una red informática, cuyo carácter delictivo sólo se da en ciertos casos;

- el uso ilegal de un programa informático.

Aunque algunas de estas infracciones son totalmente ajenas a la hipótesis de la protección tecnológica de las obras, otras podrían servir de base, de forma secundaria, a una acción contra actos de elusión de la barrera tecnológica.

Por ejemplo, una persona que infrinja el sistema de criptografía que guarda el acceso a una base de datos de obras protegidas podría ser demandada por fraude informático (el perjuicio causado a los titulares de derecho por la entrada en su sistema consistiría en la pérdida del pago que se les debe, aunque debe probarse la intención fraudulenta), y por la infracción que supone el acceso sin autorización a la base de datos.

La acción de elusión de un mecanismo de *watermarking* que impide la modificación de la obra también se podría reprimir como alteración no autorizada de datos. Por último, la elusión de una medida tecnológica que guarde el acceso y la utilización de un programa informático constituiría la base de la infracción de utilización no autorizada de un programa informático. Sin embargo, los legisladores nacionales han incluido generalmente esta infracción particular en el marco de la protección jurídica de los programas informáticosy no en los textos penales específicamente relativos a la criminalidad informática.

Los países que han seguido las recomendaciones del Consejo de Europa han introducido de forma mayoritaria en su arsenal legal represivo una infracción de intrusión no autorizada y una infracción por alteración de datos. En materia de acceso sin autorización, citemos el Artículo 321-1, párrafo 1 del Código Penal francés que reprime el acceso y la permanencia fraudulenta en un sistema informático; el Artículo 202a del Código Penal alemán que prohibe la obtención de datos especialmente guardados contra el acceso no autorizado. Noruega[42] y Finlandia también exigen que haya violación de las normas de seguridad. En cambio, la Ley federal estadounidense[43] referente al tema require que haya, además del acceso ilegal, obtención, modificación o destrucción de información.

En la legislación francesa se encuentra el elemento de permanencia indebida, lo cual permitiría, entre otras cosas, cubrir la elusión de las medidas tecnológicas relativas a la utilización de las obras protegidas incluso cuando el titular del derecho ha autorizado el acceso. Imaginemos pues a una persona que se subscribe a un servicio de video por encargo y a la que cada utilización se le factura posteriormente. Esta persona consigue eludir las medidas tecnológicas que graban y facturan estas utilizaciones. A nuestro parecer, no hay nada que pueda impedir que consideremos que estas utilizaciones fuera del sistema tecnológico constituyen una permanencia indebida en el sistema de tratamiento de datos que la ley francesa puede castigar.

En cuanto a la alteración de datos, en particular mediante la anulación del marcado digital de la obra, se tratará de un delito en virtud del Artículo 303a del Código Penal alemán y del Artículo 323-3 del Código Penal francés.

[42] Artículo 145 del Código Penal noruego.

[43] Ley Federal sobre los Dispositivos de Acceso Falsificado y Fraude y Abuso Informáticos de 1984 (*Federal counterfeit access device and computer fraud and abuse Act of 1984*), USC título 18, capítulo 47, Artículo 1030.

C. CONSIDERACIONES FINALES

Desde la adopción de los Tratados de la OMPI hace tres años, algunos países han incorporado las normas en materia de protección jurídica de las medidas tecnológicas o, al menos, se disponen a hacerlo. Esto muestra suficientemente cuán necesaria era esta nueva protección.

Además, hemos podido comprobar que, a pesar de ciertas divergencias en cuanto al alcance y las condiciones de la protección, las disposiciones nacionales o regionales están de acuerdo en lo referente a los elementos fundamentales de una protección adecuada, como la definición del objeto de la protección, la delimitación de los actos ilegales (el acto de elusión y la puesta a disposición de mecanismos de elusión), así como la definición de ilegalidad de dichos mecanismos (puntos 1.1, 1.2 y 1.3 a continuación, respectivamente).

Sin embargo, hay una serie de preguntas que quedan abiertas; la más delicada, sin duda, es la de la existencia de un posible conflicto entre la protección jurídica de la medida tecnológica, las excepciones a los derechos del autor y las limitaciones de estos (punto 2 a continuación).

1. Elementos de una protección adecuada y efectiva

1.1. En cuanto al objeto de la protección

La definición de las medidas tecnológicas, la elusión de las cuales debería prohibirse, se ha dejado a la discreción de los Estados que incorporan los Tratados de la OMPI. La única indicación fue que el fin y la función de estas medidas era proteger los derechos que se reconocen al autor o a cualquier otro titular de derechos. A primera vista, pues, se trataba de proteger principalmente las técnicas que impiden la reproducción o la comunicación al público de obras o prestaciones protegidas. Ahora bien, en general, los Estados o las organizaciones regionales, como la Unión Europea, han introducido o adoptado textos cuyo objetivo no eran sólo las tecnologías que protegían estrictamente los derechos de autor, sino también las que condicionan y controlan el acceso a las obras. Ello es evidente en los textos estadounidense y australiano; asimismo, es algo que se puede deducir de la definición de las medidas tecnológicas retomada en la propuesta comunitaria.

En consecuencia, la protección tecnológica del acceso a una obra queda protegida en la medida en que su elusión está prohibida, lo cual establece una protección *de facto* del acceso a la obra, el control del cual se convertiría así en una prerrogativa del titular de derecho aunque ésta no esté prevista por la ley. Es cierto que una gran mayoría de los sistemas tecnológicos que actualmente se utilizan para proteger obras son medidas que se basan en la criptografía, la cual, principalmente, impide el acceso no autorizado al contenido codificado. La simple acción de acceder a una obra para la que haya sido necesario desactivar una barrera técnica, sin que por ello se haya realizado un acto sujeto al derecho de autor tras haber accedido a dicha obra, sería sancionable.

Esta extensión es muestra suficiente de hasta qué punto el acceso a una obra es fundamental para los titulares de derecho. Jane Ginsburg escribió, en particular, que “*access probably will become the most important right regarding digitally expressed works, and its*

recognition, whether by the detour of prohibitions on circumvention of access controls, or by express addition to the list of exclusive rights under copyright, may be inevitable".[44] Sin embargo, esto ocasiona cierta confusión en las incorporaciones de los Tratados de la OMPI a este respecto y, en determinados casos, se vuelve borroso el límite de un híbrido entre la protección de los derechos y la protección del acceso a las obras. En todo caso, esta protección de los sistemas de control de acceso parece exceder el alcance de las disposiciones de los Tratados de la OMPI.

La preocupación por proteger las tecnologías relativas al acceso no es difícil de entender. Sin embargo, depende más de la protección del acceso al servicio en el que se encuentran las obras y, sobre todo, de la protección del pago por el servicio. Así pues, se trata más de una preocupación del vendedor o del distribuidor de las obras que de una protección directa de los derechohabientes. El interés protegido mediante la protección legal de las medidas tecnológicas está relacionado con la distribución de las obras en las redes. No cabe duda de que este interés merece una protección como, por ejemplo, la que supone la Directiva europea sobre el acceso condicionado. Pero debe reconocerse que esta protección ya no se puede justificar exclusivamente mediante consideraciones relacionadas con la propiedad intelectual. Este cambio de la razón de ser de la protección tecnológica y jurídica debería, como mínimo, ser objeto de una reflexión más detenida.

1.2. En cuanto al tipo de actos ilegales

Aunque a primera vista los Tratados de la OMPI sólo se centran en el acto de elusión mismo de las medidas tecnológicas de protección, las disposiciones nacionales que hemos tratado han completado unánimemente la prohibición del acto de elusión mediante una prohibición general de fabricación y distribución de dispositivos que permiten o facilitan dicho acto. En efecto, parece obvio que una difusión a gran escala de mecanimos que permitan anular las protecciones tecnológicas supondrá un perjuicio mayor para los titulares de derechos que los actos de elusión aislados. En determinados casos, la protección que los países han establecido de este modo se limita, además, a la incriminación de los llamados actos preparatorios, excluyendo las actividades de elusión mismasEste es el caso, en particular, en Australia y en los Estados Unidos en lo referente a las medidas tecnológicas que protegen los derechos de los autores.

Por otro lado, podemos lamentar que la mayoría de los textos no sean más claros en cuanto a las actividades de distribución de los dispositivos de elusión. Así pues, no se apunta explícitamente a la oferta en un sitio Web de sistemas de este tipo, del mismo modo que tampoco son objetivos la puesta a disposición gratuita y sin ánimo de lucro de sistemas de desbloqueo. En efecto, en la mayoría de casos en los que los piratas han "desmontado" la protección tecnológica, pocas horas después han comunicado sus ardides por Internet sin el menor fin lucrativo. No obstante, la protección que se ha establecido en los Estados Unidos y en Europa parece ser lo suficientemente amplia para englobar los actos de distribución distintos de los realizados en el marco de una comercialización.

1.3. En cuanto al tipo de dispositivos ilegales

[44] GINSBURG, J., op.cit., pág. 171.

Es difícil determinar el momento a partir del cual un dispositivo que permita la elusión de medidas tecnológicas es ilegal. Sin duda, es necesario tener en cuenta los intereses de la industria electrónica e informática, que desearía que no se prohibiesen algunos de los dispositivos que crea por la simple razón de que algunos usuarios los utilizan para anular la protección tecnológica. Es difícil encontrar el equilibrio. Hemos visto que la mayor parte de las disposiciones existentes hacen referencia al criterio de la finalidad comercial o de la utilización limitada. Los dispositivos prohibidos son los que sólo tienen una finalidad comercial o una utilización limitada distinta de la elusión de la protección, lo que deja un margen de acción razonable para los jueces que deberán poner en práctica estas disposiciones. Por supuesto, la promoción y la comercialización de dispositivos con el objetivo explícito de la elusión también se han tenido en cuenta. En conclusión, el límite así establecido entre dispositivos legales e ilegales se basa de forma lógica en la evidencia del fin del dispositivo de este modo concebido, producido, promocionado o vendido.

Por supuesto, los límites de este criterio aún están sujetos a múltiples interpretaciones cuya aclaración será tarea de la jurisprudencia. De todos modos, es importante hacer hincapié en la conveniencia de definir la ilegalidad de los dispositivos de elusión de forma idéntica en varios países.

2. Limitaciones del derecho de autor y excepciones

La cuestión de la interferencia de las excepciones al derecho de autor y sus limitaciones, así como de la protección jurídica de las medidas tecnológicas, es uno de los aspectos más complejos del tema. Está claro que una medida tecnológica puede, por definición, restringir de forma importante la capacidad del usuario de llevar a cabo los actos permitidos en virtud de una excepción legal bloqueando el acceso a una obra o impidiendo la realización de un acto sujeto a la autorización del autor. Si, como consecuencia del uso de una medida tecnológica de protección, el usuario no puede citar la obra, hacer una copia privada de ella, utilizarla con fines educativos o informativos, existe el riesgo de que el alcance de estas excepciones en el mundo digital se reduzca en gran medida.

En el marco de la protección de las medidas tecnológicas, la cuestión se plantea de dos formas. Puesto que, por lo general, los Estados han establecido una protección doble de las medidas tecnológicas, a la vez con respecto a la elusión y a la puesta a disposición de mecanismos ilegales, se debe prever la incidencia de las excepciones en las dos ramas de esta protección.

Por un lado, nos podemos preguntar si el acto de elusión de la medida tecnológica también está prohibido si se lleva a cabo para obtener acceso a una obra no protegida o para realizar actos que quedan cubiertos por una excepción.

Por otro lado, algunos fabricantes o distribuidores de sistemas que permiten la elusión de las medidas tecnológicas a veces están tentados a invocar el hecho de que sus dispositivos sólo tienen un fin perfectamente legal: permitir que los usuarios puedan eludir la barrera tecnológica para obtener acceso a obras de dominio público. Comenzaremos analizando esta segunda rama de la cuestión antes de hacer frente la otra, más peligrosa, sobre el futuro de las excepciones frente a la prohibición del acto de elusión.

2.1. Excepciones y fabricación de dispositivos de elusión

En lo que se refiere a la prohibición de los llamados actos preparatorios de un acto de elusión, la cuestión de las excepciones se resume a la de la eventual aceptación con respecto a sistemas que sólo permiten la elusión con el fin de tener acceso a información sin protección o con el fin de valerse de una excepción permitida por la ley.

Puesto que las medidas tecnológicas de protección se aplican indiferentemente a las obras protegidas y las que están libres de derechos, los dispositivos que deben eludirlas tampoco harán ninguna diferencia. Es difícil imaginar que un dispositivo se conciba con el único propósito de hacer copias privadas o copias de una obra no protegida. Resulta obvio que los mismos sistemas permitirán la elusión de los mecanismos de protección con fines ilegales. Además, autorizar la puesta en circulación de sistemas utilizados únicamente con fines legítimos permitiría que sus fabricantes se viesen libres sistemáticamente de toda responsabilidad.

Así pues, la respuesta nos parece relativamente sencilla. Los diseñadores y los distribuidores de dispositivos que permiten eludir las obras protegidas no podrían librarse de la prohibición basándose sólo en el hecho de que posiblemente su uso se limite a desbloquear el acceso a las obras no protegidas. Sin embargo, nada impide que estos diseñadores negocien con los titulares de derecho la autorización de sistemas de desbloqueo específicos, por ejemplo para controles de seguridad o en beneficio de las bibliotecas que desearan, en los casos permitidos por la ley, hacer una copia de seguridad o de archivo.

2.2. Excepciones y acto de elusión

El usuario que desee valerse de una excepción a veces se verá obligado a desbloquear la protección tecnológica que le impediría hacerlo. Si consideramos ilegal este tipo de elusión, se sancionará al usuario aunque quede fuera del derecho de autor y no se le pueda demandar por ello. Esto demostraría que el objeto de la protección es más la técnica en sí, en concepto de la inversión en la fabricación y en la utilización de ésta, que el derecho de autor. Si, por el contrario, se considera legal esta elusión, no se demandará al usuario por violación del derecho de autor ni por violación de la protección de la medida tecnológica, lo cual plantea la cuestión de la determinación del fin que el usuario persigue al llevar a cabo la elusión. En efecto, ¿cómo se podría demostrar que la elusión de la tecnología protectora se ha llevado a cabo sólo recurriendo a una excepción?

La solución que a menudo se presenta para este problema es dar a las excepciones un carácter imperativo que los contratos y las medidas tecnológicas no puedan derogar.[45]

No obstante, esta solución es imperfecta. Es cierto que la tecnología es ciega y reacciona sólo en función de la demanda de actos tecnológicos como son una copia, una impresión, un envío, una lectura o un acceso, pero no puede reconocer el marco en el que se efectúa dicho acto. Unas medidas tecnológicas similares son incapaces de analizar y reconocer las condiciones, a menudo subjetivas, que plantea el ejercicio de una excepción. Un ejemplo de ello es el carácter imperativo que concede la Directiva europea sobre las bases de

[45] HUGENHOLTZ, B.: *Rights, Limitations and Exceptions: Striking a Proper Balance*, Discurso de apertura del Imprimatur Consensus Forum, 30-31 de octubre de 1997, Amsterdam; GUIBAULT, L.: *Contracts and Copyrights Exemptions*, Amsterdam, Instituto de Derecho de la Información, 1997.

datos a la excepción en virtud de la cual se permite que el usuario legítimo lleve a cabo los actos necesarios para una utilización normal. ¿Cómo podría determinar la medida tecnológica que protege la base de datos que se trata de una utilización normal?

Asimismo, se reconoce una excepción también imperativa al usuario de una base de datos protegida por un derecho sui generis para extraer partes no esenciales. El sistema que protege la base no podría definir qué es una parte no esencial a menos que el titular del derecho lo haya programado para ello, lo cual quitaría a la excepción una parte de su sentido.

En el marco de las relaciones contractuales entre los titulares de derecho y los usuarios se puede hallar otra solución. Los autores podrían hacer dos cosas: proporcionar a determinados tipos de usuarios que hayan adquirido la obra de forma legítima, una copia de ésta desprovista de las protecciones tecnológicas, o proporcionar una copia en la que la protección tecnológica tendría en cuenta el tipo particular de excepciones a que dicho usuario puede recurrir. En todo caso, esta solución sólo concernería a las grandes categorías de usuarios, como bibliotecas, periodistas, investigadores, profesores, con los que se relacionan determinadas excepciones. Estos mismos usuarios podrían beneficiarse de una especie de presunción que los eximiría de la prohibición. Los titulares de derecho deberían derribar esta presunción en el caso de que los usuarios hayan eludido la protección tecnológica fuera del marco de la limitación del derecho de autor del cual gozan generalmente. No obstante, estas distintas alternativas impondrían un castigo a los usuarios individuales a quienes no se reconociese una posibilidad similar. El sistema de las excepciones se convertiría en un simple asunto de negociación contractual entre los derechohabientes y algunos usuarios que podríamos denominar colectivos.

En todo caso, estas soluciones pueden servir de pista para una reflexión sobre esta cuestión, especialmente delicada, de las excepciones.

[Fin de documento]