

Los DRM, ¿protegen los derechos de los usuarios y los derechos de los titulares de la información?

1. Introducción
2. Origen y fundamento de las herramientas de control de contenidos
3. Funciones y principales aplicaciones
4. Los drm, los derechos de autor y el “uso honrado” de la información
5. Los drm, la confidencialidad y el respeto a la vida privada
6. Conclusión
7. Bibliografía

1. Introducción

Dentro de unos años en todas las unidades de información se tendrá un conocimiento muy detallado sobre el funcionamiento de unos dispositivos que facilitan o niegan el acceso a los contenidos electrónicos, de modo que, según unas categorías predeterminadas, estos dispositivos permiten al usuario la utilización de ese conocimiento para unos casos o se lo impiden en otros. Estas herramientas, que se presentan en forma de hardware o software, se denominan sistemas de *Gestión de Derechos Digitales*, aunque son más conocidas por sus iniciales inglesas DRM (*Digital Right Management*).

2. Origen y fundamento de las herramientas de control de contenidos

Estas herramientas que sirven para controlar la difusión de contenidos electrónicos son programas o dispositivos físicos que operan en el entorno informático, protegiendo los derechos de autor y otros derechos del titular de los mismos (seguridad o regulación y control de los accesos) con objeto de autorizar bajo ciertas premisas la utilización de tales contenidos. Para el titular de esos contenidos digitales la ventaja inmediata de su aplicación es la posibilidad de interactuar y de mantener un control continuado sobre su obra.

Desde sus orígenes, los sistemas de gestión de contenidos han recibido distintas denominaciones, tales como *DRM*, *ECMS* o *ERMS*.

Los *Electronics copyright management systems* (**ECMS**) aluden a su capacidad de gestionar los derechos de autor en la red, mientras que la expresión *Electronic right management systems* (**ERMS**) tiene un sentido más amplio, ya que indica el potencial de protección tanto de los derechos de autor, los derechos afines y otros derechos contractuales. Finalmente, la expresión *Digital right management* (**DRM**) es la más simple y la que parece tener más aceptación, si bien no hay todavía una posición unánime sobre las funciones básicas de la gestiones de derechos digitales.

En una primera aproximación podemos distinguir dos grandes funciones de los sistemas DRM,

- la primera realiza una “gestión de los derechos digitales”, dedicada a identificar y describir la propiedad intelectual y poner reglas para su utilización
- una segunda consistente en una “gestión digital de los derechos” está orientada a certificar los contenidos y hacer cumplir las reglas puestas por el titular de los derechos o por los legisladores.

Cuando los DRM gestionan derechos de autor estos dispositivos deben permitir realizar a los usuarios determinados actos sin autorización y en ciertos casos sin pagar a los titulares de los derechos, en casos tales como la copia privada, operaciones de archivo en la biblioteca y determinados usos en el caso de personas con minusvalías.

Estas “medidas técnicas de protección” tienen su acomodo legal en el tratado aprobado por la comunidad internacional en el seno de la Organización Mundial de la Propiedad Intelectual (OMPI), en diciembre de 1996. El tratado insta a los países signatarios a adoptar una protección jurídica “contra la neutralización (elusión) de medidas técnicas eficaces que son aplicadas por los autores en el marco del ejercicio de sus derechos en virtud del presente tratado o del Convenio de Berna y que, respecto de sus obras, restrinjan actos que no estén autorizados por los autores concernidos o permitidos por la ley”. El tratado no señala cómo debe organizarse esta protección, ni qué actos deben ser prohibidos. Con anterioridad, la ley (L16/1993) de transposición de la directiva (91/250/CEE) sobre protección jurídica de los programas de ordenador en su artículo 8 c) consideraba infractores a “quienes pongan en circulación o pongan con fines comerciales cualquier medio cuyo único uso sea facilitar la supresión o neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger un programa de ordenador”, este texto está incorporado al derecho español en el art. 102 c) del texto refundido vigente (RDL 1/1996).

Con la incorporación del tratado OMPI de 1996 en la directiva comunitaria de 2001 lo que se ha hecho es establecer una protección legal específica para estas medidas de protección. De modo que, a la protección de los derechos de autor por normas administrativas, civiles y mercantiles, y penales se añade ahora “la protección de las medidas tecnológicas incorporadas por los titulares de los derechos para impedir que usuarios no autorizados accedan a obras protegidas”.

El art. 6.1 de la directiva 2001/29/CE de 22 de mayo, conocida como de derechos de autor en Internet, señala que “los Estados miembros establecerán una protección jurídica adecuada contra la elusión de cualquier medida tecnológica efectiva, cometida por una persona a sabiendas, o teniendo motivos razonables para saber que persigue ese objetivo”. Más adelante, el art. 6.3 de la misma directiva entiende por “medidas tecnológicas toda técnica, dispositivo o componente que, en su funcionamiento normal, esté destinado a impedir o restringir actos referidos a obras o prestaciones protegidas que no cuenten con la autorización del titular de los derechos de autor o de los derechos afines a los derechos de autor establecidos por ley”. Hemos de señalar la importancia de estos sistemas en todo intercambio electrónico de información y la neutralidad de los mismos en cuanto al contenido de la transacción. Tanto se pueden aplicar para garantizar la seguridad de una operación de comercio electrónico como para proteger la integridad del contenido de un artículo accesible en la red bajo la modalidad de acceso abierto (open access).

No obstante, conviene precisar que en el ámbito de los derechos de autor la protección otorgada por los DRM a las obras desencadena un nuevo proceso de acceso a las mismas. Los DRM impiden el acceso electrónico a las obras, *de facto*, es decir, otorgan al titular la prerrogativa de autorizar o no el acceso a las mismas. A diferencia de un libro impreso que se puede hojear antes de ser comprado (y comprarse o no), ese mero acceso a las obras otorga un nuevo derecho al titular y “puede llegar a ser el más importante derecho respecto a los trabajos digitales”.

3. Funciones y principales aplicaciones

La gestión de derechos digitales abarca las siguientes funciones:

- Protección de contenidos digitales, al mantener la integridad de los mismos se asegura que el documento no se modifica durante su almacenamiento.
- Seguridad en la distribución, al registrar, por ejemplo, a los diferentes actores que intervienen en el proceso: autores, editores, productores, entidades de gestión colectiva...
- Autenticación de los contenidos, al integrar la identidad digital de las obras, de los titulares y de sus representantes
- Control de transacciones, al facilitar los pagos electrónicos
- Identificación de los participantes en el mercado, lo que lleva consigo el deber de protección de los datos personales y la confidencialidad.

En definitiva, los DRM protegen los contenidos e incluyen mecanismos para comprobar y validar los derechos de los usuarios sobre cada acceso.

Principales sistemas DRM:

- **SCMS (Serial copy management system)**
Uno de los dispositivos técnicos más antiguos, data de los años ochenta y se emplea para proteger la música en los CD's.
- **Macrovisión**
Sistema anticuado como el anterior y se utiliza para proteger las copias de video.
- **CSS (Content scrambling system)**
Sistema de codificación que usa una clase de encriptación 40 bit, lo cual se considera una protección débil, el sistema fue craqueado y su código fuente dado a conocer en 1999. Sigue siendo el estándar en la protección de DVD. El sistema DeCSS es el equivalente en el entorno Linux.
- **Watermarking, marca de agua o tatuaje**
Es una técnica de identificación de contenidos digitales, muy difícil de eliminar según los expertos. En los DVD, actualmente el sistema introduce una calcomanía en la película y otra marca en el plástico del soporte y para que el disco funcione las dos marcas tienen que coincidir. El sistema también puede permitir la realización de una copia privada pero bloquear todas las demás.

Algunas empresas suministradoras de DRM para contenidos:

SDMI: especializada en música digital.

DAS: Sistema de Microsoft, utilizado en libros digitales (MS Reader).

Inter Trust: Es un DRM de propósito general para proveedores de información y comercio electrónico.

Content Guard: Una empresa participada por Xerox y Microsoft, suministra contenidos encriptados en los cuales se almacena el contenido, uno de sus productos es un lenguaje XML específico para gestionar derechos de autor (XrML).

4. Los drm, los derechos de autor y el “uso honrado” de la información

Como ya se ha mencionado, los DRM son un conjunto de tecnologías electrónicas que ejercen varias funciones con el objetivo de bloquear y proteger la obra y gestionar el acceso a las mismas mediante un sistema de licencias, a partir de las cuales generalmente se obtiene una retribución por las distintas variantes de utilización de las mismas (leer, copiar, imprimir...). Estos mecanismo además de proteger los derechos de autor realizan otras funciones más amplias de ese campo, tales como:

- Términos y condiciones de utilización de la obra;
- Transmisión segura de los contenidos;
- Prueba de recepción del contenido y de la identidad de la persona autorizada a realizar el contenido;
- El pago;
- Registro y secuencia de utilización, con el objetivo principal de conseguir un pago adecuado o las metas de marketing.

Dado que la función ejercida por los DRM es, por tanto, más diversa que la protección de la autoría de las obras, van a ser utilizados por muchos actores del mercado para proteger sus intereses comerciales y el acceso a las obras, tal es el caso, por ejemplo, de los canales de televisión de pago. Sin embargo, es preciso adentrarse en cómo estos mecanismo van a respetar el derecho de acceso de los usuarios en el conjunto de las excepciones a los derechos de autor, aspecto que en el ámbito estadounidense se conoce como uso honrado (fair use) de la información.

La mencionada directiva sobre derechos de autor en Internet, señala en el art. 6.4 que cuando los titulares de derechos no adopten medidas voluntarias, los Estados tomarán las medidas pertinentes para que los titulares faciliten el acceso a los beneficiarios de la excepción (reproducciones en papel, grabaciones efímeras de carácter documental excepcional, fines educativos...). Si bien en el mismo apartado se abre la vía contractual, en cuyo caso si el acceso ha sido convenido entre el usuario y el titular la excepción queda sin efecto. En principio, la legislación comunitaria es más favorable a la posición del usuario que la estadounidense y la australiana al exigir la nuestra que los titulares de los derechos implementen las excepciones, mientras que aquellas se limitan a sancionar la violación de la protección. Sin embargo, la libertad de pactos puede dejar en inferioridad de condiciones a los usuarios y se corre el peligro de que las excepciones

perezcan por esta migración del derecho de autor desde la órbita de las normas de derecho necesario a la de libertad de pactos.

5. Los drm, la confidencialidad y el respeto a la vida privada

Los sistemas de protección y gestión de derechos (DRM) imponen en su operatividad el control de quiénes pueden utilizar las obras que administran, así como los usos que cada individuo efectúa de dichas obras.

En efecto, los DRM, imponen en primer lugar restricciones a la utilización de las obras, pero en un segundo nivel de control informan al titular de los derechos de las actividades individuales de cada usuario (los usos realizados como guardar el archivo pdf e imprimirlo; el terminal de conexión, ...)

La información suministrada por los DRM puede ser utilizada para construir perfiles sobre las preferencias informativas de los usuarios y venderlos con propósitos comerciales.

Hay que recordar en este punto los dictados de la Ley Orgánica de Protección de datos de carácter personal (LOPD, 15/1999), en virtud de la cual los operadores de sistemas de protección de derechos digitales que manejen obras protegidas deberán respetar, principalmente, las obligaciones siguientes:

- Garantizar la seguridad y exactitud de los datos (art. 9)
- Deber de secreto (art. 10)
- Comunicación de los datos, sólo debe hacerse para el cumplimiento de los fines y con el consentimiento del afectado. Esto es especialmente importante en el caso de que los contenidos digitales a los que accede el usuario estén fuera de la biblioteca, a este supuesto se refiere el apartado 2c) del art. 10.
- Derecho de rectificación y cancelación (art. 16)

Por otro lado no hay que olvidar la amenaza que para el dominio público suponen los DRM, ya que aunque pueden negar la realización de copias ilegales de trabajos protegidos, pueden impedir fácilmente la realización la copia y distribución de obras de dominio público como si fueran trabajos protegidos.

Los DRM ejercen una grave amenaza tanto sobre la libertad de acceso a la información como sobre el acceso al dominio público.

6. Conclusión

Si los DRM fueran unos dispositivos neutrales para regular el acceso de los usuarios y respetar los derechos de los titulares, la respuesta a si los DRM protegen los derechos de los usuarios y los derechos de los titulares de la información sería que sí. Pero si matizamos algunas cuestiones, la respuesta global será que no. Así, se puede cuestionar que estas arquitecturas puedan ayudar a proteger las limitaciones sobre los derechos exclusivos del titular de los derechos de autor, preservando la flexible doctrina del “fair use”.

Por otro lado, no menos importante, es que el uso honrado y los límites a la titularidad de los derechos de autor se han gestionado en ese contexto social de equilibrio entre los intereses de los titulares de los derechos y de los usuarios, mientras que los DRM están sustituyendo esa práctica social por reglas privadas que establecen unilateralmente los titulares de los derechos y los fabricantes de software.

Si trazamos un balance de ventajas y desventajas de los sistemas de gestión de derechos digitales, podemos encontrar las siguientes ventajas:

- Para el titular de los derechos la principal ventaja está en su interactividad y en la posibilidad de controlar la explotación sucesiva de una obra.
- Facilita al autor una estadística de lecturas y búsqueda para su trabajo en tiempo real y le ayuda a determinar el valor del trabajo realizado
- En su caso, le facilita al autor una fuente de ingresos, complementarios a la publicación impresa
- Control de acceso, todos los sistemas DRM incorporan un sistema de seguridad y de control de acceso, lo que limita los usos no autorizados y reduce la posibilidad de copias ilegales.
- Más y mejores contenidos, al incentivar la creación se producirían contenidos de mayor calidad.
- Control editorial de la calidad, al ser la mayoría de la información producida en estos sistemas de pago, se aseguraría la calidad mediante la evaluación de los contenidos por árbitros.

Por otro lado hay una serie de desventajas que reseñamos también:

- Los sistemas DRM no se consideran seguros y hay una sensación general de que son fácilmente vulnerados y craqueados.
- Restricciones del acceso a la información, al ser de pago muchos usuarios no acceden.
- Costes del sistema de gestión, costes de hardware y de software, además de del personal de mantenimiento del sistema y de los árbitros de la publicaciones.
- Sistemas de pago no seguro, todavía el sistema de liquidación no se considera completamente fiable.
- Elevada complejidad del sistema de control de acceso, lo que provoca incompatibilidades entre sistemas y que muchos usuarios no los usen o lo hagan incorrectamente.
- Falta de privacidad, la mayoría de los sistemas incluyen un control de la conducta del usuario, sobre qué adquieren, preferencias, tasas de uso; al ser los datos transmitidos por el sistema supone una total pérdida de la privacidad del usuario.