TEMA 043. LA PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE ORDENADOR. LOS MEDIOS DE COMPROBACIÓN DE LA LEGALIDAD Y CONTROL DEL SOFTWARE

Actualizado a 23/01/2022

1 PROTECCIÓN JURÍDICA

Hace ya unas cuantas décadas, donde la informática irrumpió con fuerza en la sociedad, la parte principal la constituía el hardware y las máquinas de computación, siendo el software algo menos importante o relevante. El mundo cambiante de la informática ha ido progresivamente posicionando el software, tanto a nivel técnico como comercial y económico, en una posición dominante, donde la protección de sus autores y sus creaciones se convertía en una necesidad.

En España, se optó por incluir la protección de los programas de ordenador en la Ley de Propiedad Intelectual.

El Marco jurídico actual está comprendido por:

- Tratados internacionales. Ejemplo: Convenio de Berna o Tratado de la OMPI sobre Derecho de Autor, protegen de igual forma al software
- Ley 2/2011, de 4 de marzo, de Economía Sostenible. Disposición final cuadragésima tercera.
- Real Decreto 1889/2011, de 30 de diciembre, por el que se regula el funcionamiento de la Comisión de Propiedad Intelectual.
- Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de programas de ordenador.
- Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.
- Ley 23/2006, de 7 de julio, por la que se modifica el Texto Refundido de la Ley de Propiedad Intelectual. (Transpone la Directiva 2001/29 al ordenamiento jurídico español).
- **Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual (TRLPI),** modificado por la Ley 5/1998, de 6 de marzo de 1998 y la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.
- Real Decreto 114/2000, de 28 de enero, por el que se crea y regula la Comisión Interministerial para actuar contra las actividades vulneradoras de los derechos de propiedad intelectual e industrial.

1.1 REAL DECRETO LEGISLATIVO 1/1996 (TRLPI)

En este Real Decreto Legislativo, se garantiza e incluye la protección de los programas de ordenador en su artículo 10**: Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas:**

…

i) Los programas de ordenador

El TRLPI introdujo un nuevo Título, el VII, llamado “programas de ordenador”, y consta de diez artículos que regulan la protección de los programas de ordenador.

A través de su artículo 96, define un programa de ordenador como **toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuese su forma de expresión y fijación.** También es objeto de protección la documentación y manuales de usuarios anexos al programa.

Tipos de obra que aplica a los programas de ordenador:

- Títulos originales (software de nueva creación, creación intelectual propia de su autor)
- Obras derivadas (versiones de software)

Requisitos para que una obra sea susceptible de estar protegida:

- Que sea original
- Que esté plasmada en un medio material

DERECHOS CONTEMPLADOS

Titularidad de los derechos. Corresponde a la persona o grupo de personas naturales creadores

Derechos morales. Relativos a decidir sobre la divulgación de la obra, reconocimiento de autor, respeto a la integridad de la obra. Son irrenunciables.

Derechos de explotación. Relativos a los beneficios económicos que se derivan de la explotación de la obra. Pueden ser objeto de transmisión. Tienen ciertos límites.

- Reproducción (total o parcial)
- Distribución
- Comunicación Pública
- Transformación: traducción, adaptación, arreglo o cualquier otra transformación de un programa de ordenador

Otros derechos.

- Derecho de participación
- Protección registral: Registro de la Propiedad Intelectual
- Remuneración equitativa por copia privada

DURACIÓN DE LOS DERECHOS DE EXPLOTACIÓN

Los derechos de explotación duran toda la vida del autor y setenta años después de su muerte o declaración de fallecimiento.

Respecto a las obras anónimas, seudónimas o póstumas, los derechos de explotación duran setenta años desde su divulgación lícita.

Obras con coautores: durante toda la vida de todos ellos y setenta años a partir de la muerte del último.

Las obras publicadas por partes computan por separado.

El plazo de explotación empieza a computar desde el 1 de enero del año siguiente al de la muerte del autor.

1.2 DIRECTIVA 2009/24/CE: LA PROTECCIÓN JURÍDICA DE PROGRAMAS DE ORDENADOR

Tiene por objeto aclarar y suprimir las diferencias entre la protección jurídica de los programas de ordenador en los distintos países de la Unión Europea (UE) con el fin de contribuir al buen funcionamiento del mercado interior.

Puntos clave:

- Los países miembros deben proteger los programas de ordenador mediante los derechos de autor.
- Los programas de autor deben ser protegidos como obras literarias.
- La expresión "programa de ordenador" incluye tanto el código fuente como la documentación anexa.

Aplica a:

- Cualquier programa de ordenador, pero **NO las ideas o principios en los que se basa.**
- Cuando el programa es original.

Descompilación. Se puede hacer siempre y cuando sea indispensable para obtener la información necesaria para la interoperabilidad de un programa de ordenador nuevo con otros programas.

Medidas de protección. Los estados miembros deben adoptar medidas contra los actos de puesta en circulación, tenencia de copias ilegítimas o puesta en circulación o tenencia de cualquier medio cuyo fin sea la supresión o elusión no autorizada de cualquier dispositivo técnico de protección.

2 CONTROL DEL SOFTWARE ILEGAL

La infracción de los derechos está regulada dentro del Título VII, artículo 102 del TRLPI.

2.1 GESTIÓN DE ACTIVOS SOFTWARE -SAM (SOFTWARE ASSET MANAGEMENT)

La Gestión de Activos de Software (SAM por sus siglas inglesas) es una metodología de gestión de software que ayuda a definir e implementar procesos para optimizar la inversión en software cumpliendo con la legislación aplicable.

Las principales **ventajas** de implementar SAM son:

- Reducción de costes del software y de su mantenimiento, gracias a poder realizar una gestión más eficiente del licenciamiento del software en la organización.
- Fomento del cumplimiento de las políticas de seguridad en la organización.
- Mejora de la productividad del trabajador, al disponer de las herramientas software adecuadas a su puesto de trabajo.

- Mayor conocimiento del retorno de las inversiones realizadas en software en la organización.
- Facilidad y control en la detección de necesidades de adquisición de software.

SAM constituye un **estándar internacional** de gestión de los sistemas de información, soportado por su correspondiente Norma: **UNE-ISO/IEC 19770-1:2012**

2.2 DRM (DIGITAL RIGHTS MANAGEMENT)

La gestión de derechos digitales o DRM es un término que engloba varias técnicas que permiten al dueño de los derechos o distribuidor de un contenido en formato digital controlar cómo puede emplearse el material por los usuarios en cualquier tipo de dispositivo electrónico.

Las técnicas de DRM se basan en la encriptación, la cual permite a los dueños del contenido controlar el modo en que podrá accederse al mismo por los distintos usuarios, incluyendo la cuestión de licencias y la desencriptación en el dispositivo cliente.

La protección técnica para combatir las infracciones de los derechos de autor y copyright tienen dos posibilidades: la **protección a priori o activas y la protección a posteriori o pasivas**. La primera consiste en impedir que el cliente (comprador) pueda realizar una copia del material, mientras que la segunda consiste en detectar dichas copias. Dentro de la comunidad científica hay quien cree que la protección a priori, a la larga, es vulnerable ya que se puede dar con el algoritmo de protección y por tanto anularlo, de forma que en los últimos años se ha desarrollado la protección a posteriori como una herramienta eficiente para combatir la piratería.

ELEMENTOS DE UN DRM

- El propio contenido digital, puede ser, por ejemplo, un fichero de música, un libro electrónico, una aplicación de software, etc
- La fuente de dicho contenido, La fuente es la que proporciona el contenido digital encriptado y la licencia asociada (que puede estar integrada con el propio contenido)
- El destino del mismo, el que los utiliza. Ambos, fuente y destino, pueden ser tanto un usuario como un dispositivo digital
- La licencia define lo que el destino puede hacer con el contenido digital y en qué condiciones.
- El modelo de confianza entre fuente y destino., El modelo asegura que todas las partes y componentes pueden confiar entre sí: que la fuente está autorizada a expedir la licencia, que nadie puede acceder de forma no controlada a la misma y que el destinatario cumple las condiciones de la licencia. La encriptación, autorización y otras tecnologías de seguridad son los medios necesarios para llevar a cabo este modelo de confianza.

TÉCNICAS DE CONTROL

- **Marca de agua digital (watermarking).** es una técnica de ocultación de información que forma parte de las conocidas como esteganografías.
    - Concretamente, esta técnica consiste en insertar un mensaje (oculto o no) en el interior de un objeto digital, como podrían ser imágenes, audio, video, texto, software, etc. Dicho mensaje es un grupo de bits que contiene información sobre el autor o propietario intelectual del objeto digital tratado (copyright).

      2 técnicas

- **Técnicas espaciales**: implican la modificación de alguna componente en el dominio espacial, son fáciles de implementar y son frágiles frente a ataques. (Ejemplo: substitución de bits de menor peso).
- **Técnicas espectrales**: implican la modificación de alguna componente en el dominio transformado frecuencial, son complicadas de implementar y robustas frente a modificaciones. (Ejemplos: modificación de los coeficientes DCT, ensanchamiento de espectro,…).
- Pueden sufrir tres tipos de ataques: robustez, presentación y la interpretación

- **Huella digital (fingerprinting)**
  - consiste en introducir una serie de bits imperceptibles sobre un producto de soporte electrónico (CD-ROM, DVD.) de forma que se puedan detectar las copias ilegales. Si dichas marcas contienen información del comprador, esto nos permite identificarlo y por tanto detectar el responsable de la copia ilegal.
  - Simétrica: solo interviene el vendedor en el proceso de marcado
  - Asimétrica: intervienen comprador y vendedor
  - Anónima: ha intervenido una tercera parte de confianza
- **Protección de copia**
  - medida técnica diseñada para prevenir la duplicación de información
- **Distribución y protección basada en llaves**
  - **Hardware:** (también conocida como dongle). Se trata de un dispositivo que cuando se acopla al ordenador o dispositivo electrónico bloquea la funcionalidad del software o codifica el contenido. De este modo, para poder ejecutar el software protegido se necesita una llave USB conectada al ordenador que protege la aplicación de la piratería y el uso ilegal.
  - **Software**: el usuario transmite la clave de producto a un servidor de activación remoto y recibe una llave con términos de licencia, que se instala en su equipo. La activación de producto está protegida con un canal de comunicación basado en SSL (Secure Socket Layer) entre el equipo del usuario y el servidor de activación.
- **Windows Media Rights Manager System** Este sistema permite a cualquier distribuidor de contenidos limitar el uso que se le da a dichos contenidos cuando estos se reproducen por la aplicación Media Player de Windows
- **Búsqueda por comparación.** Existen herramientas que permiten realizar detección de copias de código fuente, permitiendo al propietario comprobar si el código fuente de un programa de ordenador ha sido plagiado. Existen numerosas herramientas en el mercado que permiten detectar copias de código fuente, algunas de ellas comparan con ficheros locales y otras permiten comparar con ficheros en Internet. Algunos ejemplos son Jplag y MOSS (Measure of Software Similarity).

Las **iniciativas del OMA**, Open Mobile Alliance, que especifican la gestión de derechos digitales en el entorno móvil.

Conceptos relacionados con la tecnología DRM, como son:

- El contenido. Es un recurso digital, puede ser, por ejemplo, una imagen, un conjunto de sonidos, etc.
- Los derechos de uso. Son permisos y restricciones que definen el acceso a un contenido.

- Los permisos. Definen los tipos de operaciones que pueden realizarse sobre el contenido protegido (la visualización, la impresión, etc.).
- Las restricciones. Controlan el consumo de los contenidos (mediante restricciones puede expresarse, por ejemplo, que una imagen sólo pueda ser visualizada un determinado número de veces).
- El contenido DRM. Es un contenido que se consume de acuerdo con un conjunto de derechos (los derechos de uso pueden estar incluidos en el propio contenido o se pueden descargar de forma independiente). Un contenido DRM puede estar cifrado o no.
- El mensaje DRM. Es un mensaje que contiene un contenido DRM y, opcionalmente, sus correspondientes derechos.
- El agente DRM. Es una entidad residente en el dispositivo consumidor que se encarga de aplicar los derechos de uso y consumir el contenido protegido.

LENGUAJES DE EXPRESIÓN DE DERECHOS

Uno de los componentes más importantes, especialmente para sistemas DRM complejos, se conoce como **REL (*Rigths Expression Language*)**. Los derechos dentro de una determinada licencia tienen que expresarse en un lenguaje entendible por las máquinas, de modo que el software DRM pueda leer y actuar sobre ellos; éste es precisamente el papel de los REL. La mayoría de los REL se basan actualmente en XML

Rights Expression Language (REL)

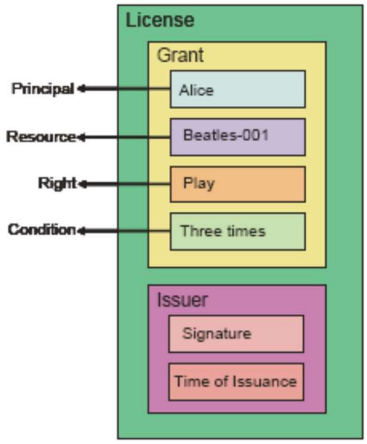
El lenguaje REL (Rights Expression Language) de MPEG-21 es un lenguaje de propósito general para especificar expresiones de derechos y condiciones asociadas con la utilización y gestión de contenido digital y servicios en la red. El REL está basado en el lenguaje **XrML (eXtensible rights Markup Language)** es un lenguaje para la especificación de derechos y condiciones para el control del acceso a contenidos y servicios digitales, desarrollado por la empresa más importante de la industria del DRM, ContentGuard.

MPEG-21REL (Moving Picture Experts Group REL). Estándar ISO/IEC desde 2004, conocido oficialmente por **ISO/IEC 21000-5:2004**. Se basa en XrML 2.0.

Una licencia es un contenedor de cesiones de derechos o grants. Un grant expresa una cesión de un derecho (Right) asociado a un recurso (Resource) que una entidad (Principal) puede ejercer posiblemente bajo ciertas condiciones (Condition).

Un grant es una estructura XML que expresa una cesión de derechos utilizando los siguientes elementos del lenguaje REL:

- Principal: identifica una entidad como una persona, una organización o un dispositivo al que se le ceden los derechos.
- Right: especifica la actividad o acción que el Principal puede realizar. Algunos ejemplos de derechos pueden ser: escuchar una canción, imprimir una imagen, visualizar un vídeo, etc.
- Resource: identifica el objeto que el Principal puede utilizar cuando ejerce un determinado derecho. Por ejemplo se puede utilizar un URI para identificar un fichero que contienen un vídeo que un Principal puede visualizar.
- Condition: especifica una o más condiciones que se deben cumplir antes de que el Principal pueda ejercer un derecho sobre un determinado recurso. Por ejemplo el Principal debe pagar una tasa antes de poder ejercer un derecho sobre un recurso
- La entidad que expide una licencia puede firmar digitalmente la licencia mediante el elemento Issuer.



ODRL (Open Digital Rights Language)

La iniciativa ODRL (Open Digital Rights Language) está compuesta por una serie de empresas del sector audiovisual lideradas inicialmente por IPRSystems. La especificación ODRL se ha copublicado como estándar internacional por W3C (World Wide Web Consortium) y OMA (Open Mobile Alliance) ha definido un lenguaje de expresión de derechos estándar para móviles basado en ODRL.

ODRL es un vocabulario para la expresión de términos y condiciones sobre el contenido digital, que incluye permisos, restricciones, obligaciones, condiciones y acuerdos con los poseedores de los derechos

Los elementos más importantes definidos en el modelo ODRL son los siguientes:

- **Assets:** identifica de forma única el contenido digital a proteger. Puede contener información asociada de seguridad como encriptación para la entrega segura.
- **Rights:** la información relacionada con los derechos digitales asociados con un Asset consiste en:
    - **Permissions:** acciones permitidas sobre un Asset. Por ejemplo, visualizar un vídeo.
    - **Constraints:** limitaciones asociadas a las acciones permitidas sobre un Asset. Por ejemplo, visualizar un vídeo un máximo de 5 veces.
    - **Requeriments:** obligaciones necesarias para ejercer una determinada acción permitida sobre un Asset. Por ejemplo, pagar 5 Euros cada vez que se visualiza un vídeo.
    - **Conditions**: especifican excepciones bajo las cuales las acciones permitidas expiran y es necesario renegociarlas. Por ejemplo, si la tarjeta de crédito caduca, entonces se anula el permiso para visualizar el vídeo.
- **Parties**: entidades que incluye usuarios finales y propietarios de derechos

Lenguaje XMCL

Lenguaje XMCL (Extensible Media Commerce Language), desarrollado por RealNetworks. Esta soportado por 27 compañías (por ejemplo, Adobe, America Online, IBM, Intertrust Technologies…etc). Este lenguaje describe un formato de intercambio que describe las reglas de uso que aplican al contenido multimedia. XMCL permite que el

contenido sea gestionado de un modo independiente de códecs, sistemas de gestión de derechos y sistemas de comercio electrónico.

XMCL maneja tres etiquetas principales:

- **clientInfo,** con información relacionada con el cliente
- **licence**, en donde se incluye información relacionada con el contenido que se adquiere, período de utilización, derechos de uso, etc.
- **auth,** con información sobre la autenticación

Whistleblowing: se trata de la práctica de alertas o revelación de secretos por parte de un ciudadano, que, en un momento dado, al darse cuenta de la existencia de un hecho que puede constituir un delito, peligro o fraude, y que está siendo silenciado, decide alertar o denunciarlo públicamente.

BSA (Business Software Alliance): es una asociación comercial sin ánimo de lucro creada para defender los objetivos del sector de software y de sus socios de hardware. Es la organización más destacada dedicada a fomentar un mundo digital seguro y legítimo.