Les Mesures Techniques de Protection... autrement dit les DRM

Teddy Furon

▶ **To cite this version:**

Teddy Furon. Les Mesures Techniques de Protection... autrement dit les DRM. Colloque PRIAM, Nov 2008, Grenoble, France. ⟨inria-00505909⟩

HAL Id: inria-00505909

https://inria.hal.science/inria-00505909v1

Submitted on 26 Jul 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

HAL Authorization

Les Mesures Techniques de Protection… autrement dit les DRM.

Teddy Furon, Thomson Security Lab

Les MTP sont les Mesures Techniques de Protection défendant une œuvre (film, musique, …) contre la redistribution illégale. Elles sont plus connues sous le terme anglais *DRM*, *Digital Right Management system*.

Les MTP sont au cœur d'un décor socio-économique et juridique assez dense. Beaucoup d'acteurs sont présents : fournisseurs de contenu, distributeurs, fournisseur de technologie et consommateurs. Les modes d'expression sont normatifs (normes de fait ou standards internationaux). Les scénarios types envisagés sont le stockage, la consommation, la transmission ou la production des œuvres.

I. Les aspects juridiques

Commençons par un avertissement : je ne suis pas juriste, ce qui suit est l'interprétation par un technicien du cadre juridique autour des MTP.

Les œuvres sont protégées par les lois sur la propriété littéraire et artistique incluse dans le Code de la Propriété Intellectuelle, CPI. Très schématiquement, deux concepts fondamentaux y sont décrits : le droit d'auteur et les droits voisins. Le droit d'auteur est un droit moral, c'est-à-dire un droit de l'homme, qui est ici l'auteur. Ce droit défend la paternité de l'œuvre et son contrôle par l'auteur. Ce droit est incessible et imprescriptible (*i.e.* sans fin). Les droits voisins sont des droits patrimoniaux, c'est-à-dire des droits des biens défendant les intérêts financiers de l'auteur mais aussi des producteurs, promoteurs, éditeurs (*i.e.* les voisins) de l'œuvre. Les MTP visent surtout à restreindre la distribution illégale, ils sont donc relatifs aux droits voisins.

Ces lois sont en fait élaborées au niveau international pour homogénéiser le code de la propriété intellectuelle à travers le monde. Ceci est le but du WIPO, *World Intellectual Property Organization*, regroupant 184 pays membres. Le dernier traité WIPO date de 1996. Il a été traduit et ou adapté aux Etats-Unis dans le DMCA, *Digital Millennium Copyright Act* (1998), en Europe dans l' EUCD, *European Union Copyright Directive* (2001), puis en France dans la loi DADVSI (Droit d'Auteur, Droit Voisin et Système d'Information).

C'est dans ce dernier traité WIPO que la notion de MTP apparaît. L'œuvre est l'objet de la protection du dispositif juridique. Une première ligne de défense est l'arsenal des lois protégeant les droits voisins datant de la convention de Rome de 1961. Avec l'avènement de l'ère du numérique et notamment la convergence entre les mondes « électronique grand-public » et « informatique », le piratage s'est nettement amplifié. Pour les œuvres « multimédia », dans les années 90, des systèmes techniques visant à contrer le piratage se sont développés comme deuxième ligne de défense. Hélas, ces protections sont régulièrement attaquées. Le dernier traité WIPO reconnaît donc ces protections, les nomme MTP et il introduit de nouvelles lois protégeant ces MTP. C'est une troisième ligne de défense. Les pirates ne sont donc plus seulement condamnés parce qu'ils spolient les intérêts des ayants-droit, mais aussi parce qu'ils ont contourné des MTP, ce qui semble plus immédiat à prouver.

Le CPI mentionne que c'est au producteur de recourir à l'usage des MTP avec le devoir d'en avertir l'auteur (Art. L. 131-9). Le principe de neutralité technologique fait que le CPI ne liste pas des systèmes considérés comme MTP. Le texte reste général et pour éviter une son

obsolescence. En revanche, une notion essentielle est la nature efficace de la MTP : Art. L. 331-5 « Les mesures techniques efficaces destinées à empêcher ou à limiter les utilisations non autorisées … d'une œuvre … sont protégées ... », ou encore, « On entend par MTP … toute technologie, dispositif, composant qui, dans le cadre normal de son fonctionnement, accomplit la fonction prévue par cet alinéa. Ces mesures techniques sont réputées efficaces lorsqu'une utilisation … est contrôlée par les titulaires de droits…, d'un procédé de protection … qui atteint cet objectif de protection. » Le CPI ne protège en aucun cas des systèmes trop triviaux à contourner. Une convention existe quand même sur le caractère classique de certains systèmes bien connus. C'est au contrevenant de prouver qu'un tel système ne serait pas une MTP. Pour les systèmes de protection à venir, il sera à charge du plaignant de démontrer son efficacité et donc sa classification en MTP protégées légalement.

Pour finir cette partie, il est fortement conseillé au lecteur de se référer à l'exposé suivant de Thierry Maillard sur l'articulation des lois protégeant les MTP et les exceptions comme la copie privée.

I. Aspect socio-économiques

Je ne parle ici que de l'industrie cinématographique, et plus particulièrement l'industrie américaine composée entre autres des 6 majors, dans notre jargon *Hollywood*.

Les œuvres ont plusieurs vies au sens où elles sont « vendues » plusieurs fois : sortie en salle, divertissement avion long courrier, sortie en DVD, vidéo à la demande, vente aux chaînes privées, vente aux chaînes publiques et, en fin de vie, vente aux bibliothèques et comités d'entreprise. Cette vente dans des fenêtres temporelles bien séparées s'appelle la chronologie des media. Les revenus de ces modes de distributions sont très différents. Pour les principales, la sortie en salle rapporte 25%, la sortie en DVD 55%. Une fuite, c'est-à-dire une capture du contenu en vue d'une redistribution illégale, au début de la chronologie voire avant la sortie en salle est catastrophique. Tout est mis en œuvre pour rendre ces fenêtres temporelles les plus étanches possibles. Tout se complique car *Hollywood* a découpé le monde en 6 régions, d'où 6 chronologies en parallèle. La raison est purement économique : la stratégie de communication (publicité, nombre de copies …) pour la sortie d'un film en Europe est dictée par son succès rencontré aux Etats-Unis. Cependant, une fuite aux Etats-Unis nuit non seulement aux prochaines ventes de l'œuvre sur le continent nord-américain mais aussi sur sa future distribution dans le reste du monde. La tendance actuelle va cependant vers une simplification de ces ventes en cascade, comme le montre les sorties mondiales des films à grand budget.

L'industrie du divertissement (film, musique, jeux vidéo, livre…) est la première industrie aux Etats-Unis, elle a donc les moyens de se faire entendre (lobbying pour des nouvelles lois) et de se défendre (utilisation de MTP). Cependant l'utilité des MTP / DRM reste incertaine. Des distributeurs (Apple iTunesStore, Fnac.com) se plaignent que les MTP sont un frein à la consommation. A trop vouloir protéger le contenu, on empêche le client de le consommer à sa guise, alors qu'il l'a dûment payé. Certains prétendent même que les MTP sont tellement contraignantes qu'elles poussent les gens à les contourner.

Jusqu'à la norme des nouveaux supports optiques Blu-Ray, les MTP étaient en général développées à bas coût et pour une durée de vie assez longue, d'où un niveau de sécurité assez relatif. Il n'y a de surprise pour personne : les MTP seront crackées. D'un autre côté le leitmotiv de *Hollywood* est « *Keep honest people honest* » : autrement dit, les gens ne sont pas

des pirates nés, ils sont honnêtes à moins qu'il ne soit trop facile de casser le système. Les MTP ne protègent pas le contenu contre les organisations mafieuses mais contre monsieur tout-le-monde. Un niveau de sécurité assez bas suffit. Cependant, avec Internet, il est assez simple de télécharger et d'installer un logiciel contournant une MTP sans pour cela comprendre et être capable de réaliser celui-ci. Les MTP récemment déployées comme celles de la norme AACS de protection des Blu-Ray ou des décodeurs satellite nouvelle génération sont d'une bien meilleure qualité. Notamment, un jeu de contre-mesures est prévu à l'avance pour nuire à l'économie de la redistribution illégale. Ces contre-attaques ne sont pas activées dès que les MTP sont cassées, mais au moment le plus opportun : par exemple, lorsque le pirate si sûr de lui a un grand nombre de clients qui seraient fort mécontents de ne plus pouvoir « pirater » la retransmission d'un match de football crucial pour l'équipe de France.

Pour finir cette partie, voici 3 livres sur les DRM donnant le point de vue :

- Des techniciens : *Multimedia Security Technologies for Digital Right Management*, W. Zeng, H. Yu, and C.-Y. Lin, ISBN : 0-12-369476-0, Elsevier.
- D'un journaliste : *Digital Right Management, Business and Technology*, B. Rosenblatt, ISBN : 0-76-4548891, Wiley.
- D'une juriste : *Digital Right Management*, Joan Van Tassel, ISBN : 0-24-0807227, NAB Executive Technology Briefings.

En les parcourant, j'ai retenu quelques définitions. Les MTP sont supposés… :

- Bloquer / donner l'accès au contenu suivant le contexte,
- Lier les droits à chaque contenu,
- Mettre en œuvre les règles de distribution,
- Contrôler l'usage du contenu dans la chaîne de distribution,
- Imposer des restrictions sur la durée des modes de consommation,
- Empêcher les fuites de contenus de grande valeur et leur distribution illégale,
- Garder une trace de l'origine du contenu,
- Mesurer l'utilisation du contenu,
- Respecter (assurer) la vie privée des utilisateurs,
- Vérifier la présence des publicités dans le contenu,
- Tracer l'origine des utilisateurs et assurer la redistribution des royalties,
- Collecter les revenus et redistribuer les commissions,
- Gérer le licensing lorsque l'on a passé le contenu ainsi que la rétribution,
- Faire de l'argent avec la propriété intellectuelle à l'ère du numérique.

II. Les outils techniques

Je classe les MTP en trois familles : les anciennes, les actuelles et les futures MTP.

La plus ancienne des MTP est la maîtrise du support physique stockant une représentation de l'œuvre. Ainsi, on contrôle l'accès à l'œuvre. Il peut s'agir de format physique propriétaire (dans les années 90 les disques noirs « Playstation » ou les mémoires Nintendo), ou de modification de standard (les CD « Copy-Control » ne suivent pas la norme Compact Disc Audio, les signaux analogiques sortant d'un lecteur de DVD ne suivent pas la norme PAL/SECAM car la MTP *Analog Protection System*, dit « système Macrovision », déforme les signaux vidéo. Cela empêche le playback d'une copie d'un DVD sur cassette VHS). Il s'agit aussi de format de fichiers propriétaire (Windows Media de Microsoft). De la même manière, la maîtrise du support évite la copie pirate. Cependant, avec les efforts de normalisation croissants, cette MTP tend à disparaître.

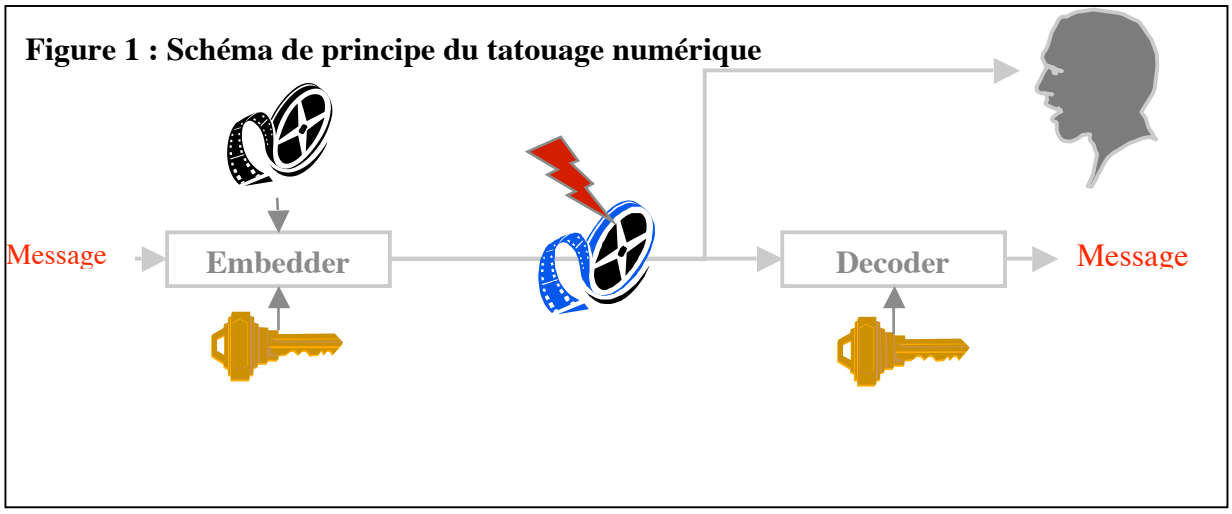
Les MTP classiques sont les primitives cryptographiques : le chiffrement, la signature numérique, les protocoles d'échange etc. Néanmoins, nous sommes loin du cadre d'étude académique. En chiffrement, Alice communique avec Bob en échangeant des messages chiffrés afin que Eve ne puisse espionner leur conversation. En protection de contenus, Hollywood tient le rôle d'Alice et le client celui de Bob. Cependant, Hollywood ne vous fait pas pleinement confiance ! Comment transmettre des contenus à quelqu'un qui peut se révéler être votre ennemi ? Bob est en fait l'appareil avec lequel le client consomme le contenu : un lecteur Blu-Ray, un décodeur satellite, un PC. Il y a deux types d'appareils. Les « walled garden » ou plateforme propriétaire et les plateformes ouvertes.

Un « walled garden » type est le décodeur satellite, où plus exactement sa carte à puce. La carte à puce est considérée comme le coffre-fort le plus sûr en électronique grand public. Elle est par exemple dotée de contre-mesures physiques d'autodestruction enclenchées à la moindre tentative d'intrusion. Il s'agit donc d'un module de confiance dans lequel sont stockées des données confidentielles (clés de déchiffrement, identifiant de client, abonnements souscris), mais c'est aussi un micro-ordinateur capable de certains calculs comme déchiffrer des mots de code. Le décodeur satellite dont la puissance de calcul est grande déchiffre le flux video à partir des mots de code (des messages très courts) déchiffrés par la carte à puce dont la puissance de calcul est réduite. Sans une carte à puce valide, le décodeur ne sait rien faire. Ce schéma s'appelle un déchriffrement en échelle.

Un PC n'est pas un appareil de confiance : il n'existe pas d'endroit sécurisé où cacher une clé de chiffrement par exemple. Du coup, le principe de base en cryptographie académique, dit principe de Kerckhoffs, stipulant que la sécurité réside dans la clé secrète et non dans l'algorithme de chiffrement, ne tient pas. Dans les MTP pour PC, l'algorithme est tenu secret (non publié) et maquillé ou obscurci afin qu'aucun pirate ne puisse le comprendre. De même, la clé secrète est divisée et cachée en de multiples endroits. C'est ce que l'on appelle de l'obfuscation de code (*secure coding* en anglais). Le but est d'empêcher la rétro-ingénieurie (*reverse engineering*), la lecture de certains paramètres, et la modification du logiciel. Nous sommes loin de la recherche en cryptographie. C'est plutôt une série d'astuces, un jeu infini du gendarme et du voleur.

Les MTP classiques comprennent aussi tout ce qui concerne l'identification de l'utilisateur (login / mot de passe, biométrie, certificat etc) et la représentation informatique d'un droit (Rights Expression Language) décrite par des notions de contenu, personne, action et durée.

Figure 1 : Schéma de principe du tatouage numérique



Abordons maintenant les nouvelles MTP. Le tatouage numérique est l'art de cacher des informations dans un contenu hôte (son, image, video, texte, modèle 3D…). C'est un problème de communication sous des contraintes assez particulières. Un premier algorithme enfouit ces informations dans un contenu sans dégradations perceptuelles, d'où le terme *watermarking,* en anglais filigrane. On tire profit des lacunes de la perception humaine pour modifier le contenu sans engendrer de perte de qualité subjective. Par exemple, l'œil est peu sensible dans les zones texturées et le long des contours dans une image fixe. Les pixels dans ces zones sont modifiés pour colporter l'information à cacher.

Le résultat est le contenu tatoué. L'information cachée est un message binaire, c'est-à-dire à destination d'une machine. Il ne s'agit pas d'information subliminale adressée au subconscient de l'utilisateur. Un deuxième algorithme, le décodeur, retrouve les informations cachées dans le contenu tatoué. Le tatouage est dit robuste si le message est décodé même si le contenu tatoué a subi des modifications (compression, filtrage, débruitage, rotation, étirement de l'image etc). Ceci explique la métaphore du tatouage : les informations sont cachées au cœur du contenu de telle sorte qu'il devrait être impossible de les enlever, comme un tatouage sur la peau. Ces modifications du contenu tatoué sont appelées attaques.

Le principe de base du tatouage veut qu'il y ait un compromis entre imperceptibilité, robustesse et taille du message à cacher : pour un niveau de dégradation donnée, plus le message est long, moins on aura de chance de le retrouver dans le contenu tatoué et attaqué. L'application de cette primitive définit la nature du message caché. Pour ce qui nous concerne, dans les MTP :

- protection de copyright : le nom de l'auteur,
- protection de copie : status du contenu (copy never, copy once, copy no more),
- cinéma numérique : numéro de salle, date et heure,
- traçage de traîtres : identifiant du client.

Cette dernière application permet de démasquer la source de la fuite, à partir d'un contenu pirate disponible sur un réseau P2P (*peer to peer*) par exemple. Des précautions sont prises pour que même si plusieurs pirates mélangent leurs copies, on puisse retrouver l'identité d'une partie des membres de la collusion. Cette fonction existe dans le système de protection Blu-Ray. Il alimente une liste noire d'appareils dits corrompus, au sens où leur identifiant a été retrouvé dans une copie pirate. Une fois répérés, ces appareils ne peuvent plus lire les disques Blu-Ray à venir.

Une autre nouvelle MTP est l'identification de contenu. A un contenu donné, un algorithme calcule un résumé de quelques centaines de bit. Ce résumé capture les éléments les plus perceptuellement significatifs du contenu. Il est comme une empreinte unique du contenu. Contrairement à un hash cryptographique, il n'est pas dépendant de la représentation informatique du contenu. Par exemple, quel que soit le format codant une image, le résumé reste inchangé. L'ordinateur établit alors une base de données associant à chaque résumé des informations comme le titre de l'œuvre, l'auteur, les droits etc. Lorsqu'un contenu suspect lui parvient, il calcule son résumé et regarde s'il appartient à sa base de données. On donne ainsi la possibilité à l'ordinateur de reconnaître des contenus. YouTube utilise par exemple ce système pour reconnaître les contenus téléchargés par les utilisateurs : le contenu reconnu comme copie d'une œuvre est ou bien refusé ou bien accepté et l'ayant-droit percevra une partie des revenus publicitaires engendrés par la consommation de ce contenu sur le site. C'est ce que l'on appelle le filtrage de contenu.

Une dernière MTP récente est la virtualisation. Prenons l'exemple des lecteurs Blu-Ray. Dans ces appareils, un espace est réservé pour y charger une MTP venant du disque. Le code objet de cette MTP est tout d'abord analysé par l'appareil pour savoir s'il est bien authentique. C'est le cas si sa signature numérique est correcte. Ceci évite de charger un code malicieux. Une fois chargée, la MTP, à son tour, est capable de sonder l'appareil hôte pour vérifier qu'il n'est pas hacké. Une fois cette double vérification faite, l'utilisateur peut enfin visualiser le film. La virtualisation rend possible une protection à la carte, disque par disque, et un renouvellement : si une MTP est contournée, elle est remplacée dans les nouveaux disques sans pour cela mettre les lecteurs Blu-Ray à la casse.

III. Conclusion

En guise de conclusion, voici quelques tendances actuelles concernant les MTP.

Plus de DRM pour l'audio. Les revenus des ventes d'œuvres musicales sont en forte baisse. On estime que tant que le Compact Dics Audio ne sera pas remplacé, la protection de la musique est vouée à l'échec. C'est pourquoi la vente de morceaux de musique ne s'accompagne plus de DRM. En revanche, cette tendance ne vaut absolument pas pour les films et les jeux dont les budgets de production sont nettement supérieurs.

Les DRM seront moins intrusifs. Leur défaut majeur longuement décrié est leur manque d'interopérabilité. Les DRM ne seront plus dans les appareils de l'utilisateur. Une fois entré dans sa sphère privée, *home network* dans le jargon, l'utilisateur fera ce qu'il veut du contenu. En revanche, les DRM auront l'ambition de surveiller l'Internet : YouTube filtre les contenus téléchargés sur son site, les sources des fuites sur les réseaux P2P sont démasquées, les personnes téléchargeant des contenus pirates sont repérées et graduellement incitées à arrêter de telles pratiques, les fournisseurs d'accès Internet diminuent la bande passante allouée aux téléchargements des réseaux P2P. Cette mouvance va vers un contrôle a posteriori. Ces DRM visent moins l'acte de piratage que la mise à disposition et la consommation de contenus piratés. Cette mouvance s'appelle le DRM 2.0 depuis la conférence *Online Content for Creativity*, organisée par le directoire général *Information Society and Media* de la commission Européenne, où la question « *Is filtering DRM 2.0 ?*» a été posée à une table ronde. En France, on pense bien sûr à la loi dite HADOPI et à ses nombreux contournements possibles : comment accuser son voisin, comment utiliser la connection d'un autre, comment échanger des données chiffrées sur P2P, comment échanger des données de manière anonyme sur P2P. Les mécanismes de filtrage sont pour l'instant assez primaires et très imparfaits (filtrage de paquets étiquetés P2P), mais les avertissements seront dissuasifs pour la majeure partie des personnes. Les contournements par chiffrage et anonymat sont techniques, et il n'est pas sûr que M. tout-le-monde, ayant déjà reçu un avertissement par courrier recommandé, fasse confiance aux dires sur Internet de supposés experts et prenne le risque de les utiliser. La confiance sur Internet est aussi un problème pour les « pirates ».

Dernier point, la question n'est pas de savoir si une MTP sera cassée, mais de savoir quand elle le sera, et que faire à ce moment-là. Le maître mot est **renouvellement**, ou plus banalement, le jeu du gendarme et du voleur.