UNIVERSITE PARIS I – PANTHEON SORBONNE

DESS DROIT DE L'INTERNET –ADMINISTRATION – ENTREPRISES

Memoire en vue de l'obtention du DESS

SESSION DE SEPTEMBRE 2003

# LE MARQUAGE ET LA PROPRIETE INTELLECTUELLE

*PRÉSENTÉ ET SOUTENU PAR :MICHEL BLANCHARD*

# TABLE DES MATIERES

De nombreux experts prédisent que le commerce électronique sur internet va exploser. Une forme de commerce électronique consiste à échanger des renseignements nécessaires à une transaction pour obtenir un service ou un produit. Une autre forme la plus intéressante de commerce électronique consiste en la vente de paquets d'éléments binaires constituées par la numérisation d'œuvres littéraires et artistiques. Naturellement, des raisons culturelles et pratiques font que certains types d'œuvres protégées par le droit d'auteur se vendent mal sur l'Internet. Un roman est quelque chose que nous voulons lire dans l'avion, le train, voire dans un confortable fauteuil ou même au lit, sans être connecté à l'ordinateur.

Mais de plus en plus les créateurs eux-mêmes utilisent l'informatique et dans leur processus de création ont recours, consciemment ou non, à des œuvres préexistantes. Il a été dit à ce propos que le passé est un prologue et, selon Blaise Pascal, "toute la suite des hommes pendant le cours de tant de siècles doit être considérée comme un même homme qui subsiste toujours et qui apprend continuellement". Le réseau Internet constitue déjà la plus grande bibliothèque du monde surtout permet à un nombre de plus en plus important de personnes d'accéder à ces informations par-delà frontières et cultures. ce qui crée peu à peu une énorme bibliothèque mondiale à la portée de ceux qui sont reliés au réseau.

Alors pourquoi ce type de commerce électronique semble t-il tant tarder à se développer? La réponse est simple : le droit d'auteur. Au siècle dernier, il était à la mode de prétendre que droit d'auteur et l'Internet (ou son cousin multimédia le World Wide Web) étaient associés comme l'eau et le feu et qu'en conséquence, le droit d'auteur serait appelé bientôt à s'évaporer ou à s'éteindre. Depuis ces dernières années, l'augmentation de la largeur de bande et du parc d'utilisateurs du World Wide Web, de même que les nouveaux algorithmes de compression ont permis de télécharger de nouveaux types d'œuvres, et pas seulement des textes en clair, des fichiers ASCII ou PDF. Le phénomène qui a fait couler le plus d'encre est sans aucun doute celui des œuvres musicales, notamment en raison du MP3. Ce pouvoir élargi du Web de livrer en ligne des contenus aurait dû marquer la fin du droit d'auteur tel que nous le connaissons. Paradoxalement, c'est l'inverse qui semble se produire, Un certain nombre d'initiatives "sécurisées ont été proposées et plusieurs de ces systèmes en sont au stade avancé de "l'essai bêta". Ce sont les systèmes de DRM
Avant d'approfondir les questions juridiques liés à l'apparition de ces systèmes, il est nécessaire de comprendre les questions techniques qui s'y rattache. Une première partie traitera des aspects techniques avant d'approfondir les questions juridiques qui en découle.
Ces systèmes sont apparus récemment en réaction au pratique de copie systématique de contenus protégés sur le Net. Mais sur quels concepts sont-ils fondés ? De nombreux centres de recherche ont été sollicités afin de trouver des techniques permettant à des systèmes de DRM de se développer. Ainsi les techniques de marquage sont-elles nés. S'il devient possible de marquer un fichier binaire en y incluant des informations irrémédiablement attachées, alors une nouvelle façon de percevoir les systèmes informatiques est envisageable.

Ainsi, la technologie du marquage numérique peut servir à suivre précisément l'utilisation d'un contenu ("comptage et surveillance"), à rechercher des utilisations illicites (des programmes appelés "moteurs de recherche" parcourent le Web pour

trouver les copies illicites) ou à crypter un contenu afin d'en limiter les utilisations futures. **Dans un premier temps nous approfondirons les différents aspects de cette technique de marquage**

Les systèmes de DRM utilisent ces techniques de marquage et forment des bases de données qui contiennent des renseignements sur le contenu, et, dans la plupart des cas, sur l'auteur et les autres titulaires de droits. Cette information permet au système d'autoriser des tiers à utiliser les œuvres en question. Un système de gestion du droit d'auteur comporte généralement deux modules fondamentaux, l'un servant à l'identification du contenu et l'autre à l'octroi d'une licence (ou, rarement, aux autres transactions portant sur le droit, telles qu'une cession complète). **Les systèmes de DRM seront étudier dans un deuxième temps.**

Face à des données techniques nouvelles , le droit doit s'adapter. Ainsi en est il de la propriété intellectuelle.

La Convention de Berne et de nombreuses lois nationales contiennent un inventaire des composantes de la propriété intellectuelle. Il existe deux grandes catégories : le droit moral et les droits économiques. Dans la première, on trouve le droit de paternité de l'œuvre et le droit de s'opposer à sa mutilation. Dans la seconde, les droits les plus importants sont le droit de reproduction, le droit de communication au public (qui comprend, d'après l'article 8 du Traité de l'OMPI sur le droit d'auteur, le droit de "mise à disposition") et le droit d'adaptation. Un système de DRM se préoccupe principalement des droits qui peuvent aisément faire l'objet d'une licence ou d'une cession : les droits économiques se prêtent donc mieux à la gestion électronique que le droit moral.

La transmission numérique implique la fabrication d'une copie, du moins au point de réception. Même si d'aucuns affirment que la transmission numérique fait intervenir le droit de "distribution", il n'est pas réellement distribué de copie au sens matériel. En fait, lorsqu'une œuvre protégée est téléchargée à partir d'un serveur et que l'utilisateur en fait une copie, on peut invoquer le droit de reproduction plutôt que le droit de distribution. C'est assurément la position prise par la première Déclaration commune accompagnant le Traité de l'OMPI sur le droit d'auteur (WCT).

Une question demeure en suspens, celle des exceptions au droit exclusif de reproduction. Comme en dispose l'article 9 de la Convention de Berne, ces exceptions, y compris l'usage loyal et les transactions loyales doivent avoir une portée limitée dès lors qu'une activité commerciale est en jeu, ou toute autre diffusion à grande échelle interférant avec l'exploitation normale de l'œuvre.

Un autre droit important, le droit de communication au public, qui s'applique assurément à la télédiffusion, s'applique aussi à certains cas de transmission interactive à la demande. La question se pose évidemment lorsqu'une information est envoyée à un utilisateur sans qu'il l'ait demandée (technique de la pression ou du "push"). L'article 8 du Traité de l'OMPI sur le droit d'auteur dispose que le droit exclusif de communication au public dont jouissent les auteurs comprend *"la mise à la disposition du public de leurs œuvres de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit de manière individualisée*". Il s'agit d'un droit distinct, et son titulaire ne jouit pas nécessairement aussi du droit de reproduction. Si une utilisation sur le Web exige une autorisation pour les deux droits, il peut être nécessaire d'acquitter les redevances en deux opérations différentes.

Un certain nombre de questions juridiques entravent le développement des

applications de DRM.. Par certains aspects les techniques de marquage et ainsi les systèmes de DRM tendent à renforcer certains droits (droit de propriété intellectuelle) mais par d'autres ils constituent des dangers pour l'exercice d'autres droits(la protection de la vie privée, limitation et exception pour copie privée)

Les systèmes de DRM doivent eux mêmes être protégés par des mesures de protection Pour fonctionner de manière automatique, ils ont besoin de formats et d'outils d'identification et de fourniture normalisées. Avec le développement de l'utilisation des réseaux électroniques pour accéder à des contenus protégés, il est très probable que les titulaires de droits investiront lourdement dans l'identification des œuvres numériques et le marquage permanent des identificateurs. L'application à l'échelle mondiale des traités de l'OMPI sur le droit d'auteur et sur les interprétations et exécutions et les phonogrammes devraient garantir que les données relatives à la gestion du droit d'auteur ne sont pas délibérément modifiées.

Nous aborderons, dans la dernière partie, le domaine privé des particuliers et les données les concernant, ainsi que la confidentialité des données commerciales. Ces deux questions, quelque peu différentes, sont toutefois étroitement liées du point de vue des DRM.

Les deux questions que posent le plus souvent les utilisateurs sont les suivantes :

En tant que particulier, puis-je consulter, lire, regarder ou écouter sans donner mon identité (et donc sans recevoir ensuite des sollicitations par courrier ou par téléphone, etc.)?

En tant qu'utilisateur industriel (par exemple une entreprise pharmaceutique ),puis-je télécharger tel ou tel article scientifique sans que le monde entier sache que j'en ai besoin pour mon travail de recherche et développement ?

Mais, comme il a été présenté plus haut, avant d'aborder les aspects juridiques qui sont inévitablement soulevés par une nouvelle technique comme le marquage , examinons la technique marquage numérique des oeuvres et les systèmes de DRM qui l'utilisent.

# 1. Marquage et DRM

Le marquage des données numériques fait partie du domaine de «*l'information hiding* ».
L' *information hiding* » consiste à dissimuler des informations dans un document formé de données numériques. En dehors du domaine numérique, ces pratiques sont très anciennes. Les microfilms pendant la guerre en sont un exemple. En effet, deux pratiques se sont toujours retrouvées en concurrence pour établir une liaison numérique sécurisée : la cryptographie (du grec « écriture secrète ») et la stéganographie (du grec « *écriture couverte* »).

En parallèle à ces deux techniques, deux autres techniques existent à partir d'un document de données numérisées : la cryptanalyse et la stéganalyse. La cryptanalyse est l'art de briser les chiffrements, et la stéganalyse est l'art de briser un document stéganographié . Nous verrons plus loin les divers stratégies d'attaques d'un document.

La cryptographie permet d'établir une liaison sécurisée entre une personne A et une personne B en chiffrant la communication ce qui la rend incompréhensible pour une tierce personne T..

Dans le cas de la stéganographie, la communication n'est pas chiffrée. Elle ne peut pas être détectée par une tierce personne T. T ne se doute pas que A et B échangent des messages. La cryptographie et la stéganographie sont souvent très proche mais ne vise pas le même objectif.

Le mot stéganographie vient du grec 'steganos' (caché ou secret) et 'graphy' (écriture ou dessin) et signifie, littéralement, 'écriture cachée'.
La stéganographie étudie les techniques pour communiquer de l'information de façon cachée. L'adjectif caché ne signifie pas ici que l'information est visible mais codée, il s'agit alors de cryptographie. Ici, il signifie que la présence de l'information n'est pas perceptible parce que enfouie dans une autre information.

Nous voilà plongé en plein roman d'espionnage. Vous l'aurez compris, la stéganographie dont je veux vous parler ne s'intéresse pas vraiment aux micro-films et autres valises à double fond, mais à une version plus moderne d'outils de ce genre.
Pour résumer le problème de façons plus académique, utilisons une présentation proche de celle utilisée en cryptographie. Alice et Bob ont été arrêtés et emprisonnés. Ils désirent se communiquer des informations afin d'organiser leur défense lors du procès (ou leur évasion). Ils sont autorisés à communiquer quasi librement avec la restriction que tous les messages seront lus par les responsables de la prison. Ils utiliseront la stéganographie pour communiquer leur plan.
Pour pouvoir communiquer de façon secrète, il faut d'abord pouvoir communiquer tout simplement. On attachera à des messages anodins, un message secret. Afin de décoder ce message, le correspondant doit connaître un secret et/ou la technique pour déchiffrer et extraire ce message. Il est évident que ce message caché peut être lui même codé et/ou signé en utilisant des méthodes cryptographiques. La stéganographie n'étant plus alors que la dernière étape de votre encodage, celle-ci pouvant même être destinée à cacher votre usage de la cryptographie.

Il existe aussi aux moins deux classes de techniques faisant partie de la stéganographie mais suffisamment particulière pour mériter un nom.

Filigrane (‘watermarking’) :

- Protéger les possesseurs de copyright sur des documents numériques en cachant une signature dans l'information de sorte que même une partie modifiée du document conserve la signature.
- Découvrir l’origine de fuites en marquant de façon cachée et unique chaque copie d’un document confidentiel.

Canal de communication secrète (‘cover channel’) :

- Permettre à des partenaires de communiquer de façon secrète en établissant un véritable protocole de communication secrète au dessus d’autres protocoles anodins.
- Permettre une communication non autorisé à travers les communications autorisé d’un firewall.

Un certain nombre de règles sont applicables aux systèmes de stéganographie. Les lois de Kerckhoffs enseigne que la sécurité d’un système repose sur la clef et non sur le secret de l’algorithme

Au cours des dernières décennies, ces deux techniques n’ont pas bénéficié d’une évolution identiques. La cryptographie est beaucoup plus ancienne et en avance sur la stéganographie. Au niveau théorique la cryptographie a bénéficié de nombreux travaux de recherche. Avec l’arrivée des réseaux et des oeuvres multi-média des problèmes sont apparu que la cryptographie ne pouvait résoudre seule depuis une dizaine d’années, la stéganographie des documents numériques constitue un domaine de recherche de plus en plus important.

Nous ne nous intéresserons ici qu’à une forme particulière du “data hiding” : le watermarking (ou marquage ou tatouage des données) Celui-ci diffère de la stéganographie par le fait que l’on se limite souvent à dissimuler très peu d’information (très souvent un seul bit) dans une oeuvre numérique . Ce bit a pour but de démontrer l’intégrité du document ou encore d’en protéger les droits d’auteur  Du fait du peu d’information à dissimuler, le tatouage est souvent beaucoup plus résistant. Les attaques sur un document marqué sont bien différentes des attaques sur un document stéganographié. En effet, le pirate ne cherche pas à lire les informations, mais simplement à laver le document du tatouage. Ceci nous amène directement à ce qui caractérise un bon tatouage numérique. Mais avant de continuer, je tiens à préciser que dans la suite du document je serai amené à utiliser les termes : marquage, tatouage pour désigner le marquage et je ne traiterai que du marquage des images et des films. Ceci étant précisé, listons les caractéristiques requises pour un bon tatouage.

## 1.1. CARACTÉRISTIQUES D’UN MARQUAGE

Les performances d’un marquage sont appréciées sous les quatre critères suivants : Imperceptibilité,  Robustesse, Complexité, Capacité

### 1.1.1. Imperceptibilité

Le tatouage doit être invisible à l’œil humain. Prenons deux exemples très simples pour souligner son importance. Imaginons une image en niveau de gris avec une large zone uniforme. Si l’on rajoute un peu de bruit, ceci va immédiatement se voir dans cette zone. Il faut plutôt mettre le tatouage dans des zones de fort gradient (contour de formes, zones fortement texturées,…) où l’œil est moins sensible. Un autre exemple vient du marquage des images couleurs. Il est connu que l’œil humain n’est pas sensible de la même façon à toutes les longueurs d’onde. On peut ainsi dissimuler plus ou moins d’informations suivant la teinte considérée.

### 1.1.2. Robustesse

On pourrait séparer cette rubrique en deux parties : la *robustesse* et la *sécurité*. Ces deux caractéristiques sont souvent confondues surtout dans le cas du marquage. On parle de robustesse pour définir la résistance du tatouage face à des transformations de l'image tatouée. Ces transformations peuvent être de type géométrique (rotation, zoom, découpage …). Elles peuvent modifier certaines caractéristiques de l'image (histogramme des couleurs, saturation…). Il peut aussi s'agir de tous les types de dégradations fréquentielles de l'image (compression avec pertes, filtres passe haut ou passe bas, passage analogique->numérique->analogique, impression de l'image, etc. …). Ces attaques sont dénommées « attaques aveugles », car le pirate agit sans réellement savoir ce qu'il fait. Il espère ainsi laver l'image.

La sécurité caractérise la façon dont le marquage va résister à des attaques «malicieuses ». On peut faire des parallèles avec la cryptanalyse. Le pirate va chercher à laver l'image de façon intelligente. Il est sensé connaître l'algorithme et va, en général, chercher la clef qui lit le tatouage. Cela demande souvent une analyse approfondie de la technique de marquage employée.

### 1.1.3. Complexité

Dans la pratique, la plupart des opérations de tatouage doivent pouvoir s'effectuer en temps réel (surtout la détection, pour des films par exemple). Ceci implique une contrainte supplémentaire sur la complexité des opérations utilisées pour le marquage et pour la détection.

### 1.1.4. Capacité

La capacité d'un système de tatouage numérique désigne le rapport : « nombre de données » à dissimuler sur « taille du document hôte ». Dans le cas du marquage , et comme nous l'avons vu précédemment, la capacité se limite souvent à 1 bit.. De façon générale, plus la capacité est faible, plus la robustesse et l'imperceptibilité sont fortes.

## 1.2. UTILISATIONS DE MARQUAGES

Maintenant que nous avons vu les caractéristiques demandées au tatouage numérique, voici des différentes formes de marquage :

- **Le marquage faible (ou fragile)** : Dans ce cas particulier, on demande au tatouage d'avoir une très grande imperceptibilité et une faible robustesse. Ainsi, la marque ne supportera quasiment aucun traitement. On pourra ainsi certifier ou non l'intégrité de l'image.
- **Le marquage fort (ou robuste) :** Il s'agit de la forme la plus commune de tatouage numérique Elle est en général imperceptible et surtout très robuste. Le cas limite de ce type de marquage est un **marquage visible,** comme un logo, mais avec une robustesse à toute épreuve (le Vatican a utilisé ce type de marquage pour ses documents .
- **Le marquage symétrique (ou privé) :** Le parallèle avec la cryptographie prend ici tout son importance. Le marquage symétrique signifie que l'on utilise la même clef pour insérer et détecter le tatouage.
- **Le marquage asymétrique (ou publique) :** La clef de marquage et celle de détection sont différentes Outre l'intérêt immédiat (n'importe qui peut lire la signature sans pour autant pouvoir l'enlever ou la modifier), ces techniques récentes sont plus sécurisées Elles portent officieusement le nom de « marquage de seconde génération ».

## 1.3. EXEMPLES DE TECHNIQUES DE TATOUAGE

Nous allons passer en revue quelques techniques basiques de marquage.

### 1.3.1. Marquage sur les bits de poids faibles

Cette méthode est juste anecdotique. Elle nous servira pour comprendre le mécanisme de marquage à clef privée et expliciter les problèmes de robustesse.
Imaginons que l'on travaille sur une image en niveaux de gris (pour les images en couleurs, il suffit de travailler sur la luminance), et que l'on ait seulement 256 niveaux de gris possibles (de 0 à 255). On considère qu'entre 2 niveaux de gris consécutifs l'œil humain ne fait pas la différence (en fait cela dépend des niveaux de gris ou l'on se situe, car l'œil a une sensibilité aux gradients différente selon l'intensité de gris à laquelle on se place).

Si l'on considère le niveau de gris en binaire, nous sommes en présence de 8 bits. Le changement du dernier de ces bits (le bit de poids faible) ne change le niveau de gris que d'une unité. On prend une image en deux couleurs (1 bit) et on la place sur le plan du bit de poids faible des pixels de l'image hôte.

Passons en revue les caractéristiques de ce tatouage.
L'imperceptibilité : Si au premier abord elle peut sembler bonne, la méthode ne tient compte quasiment d'aucun modèle de la vision humaine. Le marquage a lieu dans n'importe quelle région de l'image. L'environnement proche du pixel que l'on traite est ignoré.

*La robustesse : Celle-ci est très faible. En effet, le tatouage ne résiste à quasiment aucune transformation. La moindre compression va changer les bits de poids faibles et ainsi complètement laver l'image. Il en est de même pour tous les filtres. Cependant, les transformations géométriques sont assez bien supportées. En effet, on peut retrouver une partie des données après des rotations ou des recadrages.

*La sécurité : Le principe de Kerckhoffs stipule que la sécurité ne doit pas reposer sur la non-divulgation de la technique. Le pirate est censé savoir que l'information se trouve dans le dernier bit. Il peut changer à sa guise le tatouage. La sécurité est inexistante.

*La complexité : Cette méthode ne présente aucun calcul, si ce n'est un simple masquage.

*La capacité : Celle-ci est excellente, nous pouvons mettre 1 bit de tatouage pour 8 bits de données.
Le lecteur aura constaté par lui même que cette méthode n'est qu'un simple exemple de tatouage. Mais il va de soit que celle-ci n'a plus aucun avenir.

### 1.3.2. Spread spectrum (ou spectre large)

Il s'agit là de la technique de marquage la plus connue et la plus employée en ce moment. Le signal de marquage est généré de façon pseudo- tout en respectant certaines conditions. Ses valeurs sont très faibles, ce qui permet d'avoir une densité spectrale de puissance très inférieure à celle de l'image hôte. Le spectre de ce signal de marquage est très étalé (d'où le nom « spread spectrum »). Ainsi, si le pirate effectue des filtres passe bande sur l'image marquée, il ne supprimera qu'une faible partie du tatouage. Au moment de l'insertion du tatouage, on peut tenir compte d'un modèle HVS, pour modifier localement l'amplitude du tatouage et ainsi rendre le marquage moins visible. On effectue la détection du marquage en faisant la corrélation du signal watermarké et du signal de marquage.

### 1.3.3. La Transformation de Fourier

Le concept de transformation de Fourier est indispensable pour la compréhension du traitement du signal (et à fortiori du traitement de l'image). Du nom d'un mathématicien Français, la transformation de Fourier repose sur le principe suivant : quasiment toutes les fonctions sont décomposables en une somme de cosinus et de sinus à des fréquences différentes. Ainsi, lorsque l'on représente une fonction dans un repère Amplitude/Temps, la transformation de Fourier permet de la voir dans un repère Amplitude/Fréquence. On voit donc les composantes en fréquence d'un signal.

Il est important de savoir que l'on peut repasser à la fonction d'origine à partir d'une transformée de Fourier en appliquant une transformation de Fourier inverse. Notre intuition nous dit que lorsque nous avons affaire à un signal où il y a beaucoup de "petits" bruits alors les composantes en hautes fréquences vont être importantes. Ce genre de propriétés permet d'appliquer des filtres sur les fonctions. Ainsi pour adoucir une image (pour enlever le bruit) on applique un filtre passe-bas (c'est un filtre qui ne laisse passer que les basses fréquences, appelé aussi "blur"). Pour conclure, il faut se rendre compte de quelques points importants: La transformée de Fourier d'une fonction permet de voir le signal sous un autre jour. Elle donne des informations qui ne sont pas forcément triviales sur la fonction. Il existe de nombreuses autres transformations, telles que la transformation en Z etc... D'ailleurs la transformation de Fourier possède des désavantages. En effet, pour la calculer, on intègre la fonction sur tout le temps. On perd ainsi complètement l'information temporelle. Ceci ne pose pas de problèmes pour un signal stationnaire. Mais cela devient très problématique pour un signal dans lequel la fréquence varie très fortement au cours du temps.
Pour remédier à ce problème, on a développé la Transformation par ondelettes (et pour se mettre bien avec le principe d'incertitude d'Heisenberg qui nous dit que plus l'on prend une grande précision sur le temps plus l'on perd de précision sur la fréquence et vis versa). Le calcul numérique d'une transformation de Fourier prend énormément de temps, ce qui la rendait très peu exploitable à ces débuts. Une autre façon d'effectuer ce calcul à été inventé et a permis de la rendre accessible (en fait il à s'agit réellement d'une petite révolution) au commun des mortels. C'est ce que l'on appelle la FFT (Fast Fourier Transform).

### 1.3.4. Un regard sur la seconde génération de watermarking

Pour créer un marquage (watermarking) robuste le tatouage doit être placé dans les endroits ou les données sont importantes. La seconde génération de watermarking va encore plus loin dans cette direction en se proposant de tenir compte des caractéristiques géométriques des images (ou des films). Par exemple, dans une image, ces caractéristques peuvent être les bordures, les coins, les textures....Il faut malgré tout faire attention car toutes les caractéristiques ne sont pas forcément bonnes à prendre en considération. Ainsi, il faut que, si possible, elles aient les propriétés suivantes:

*Invariance au bruit (compression non conservative), il faut donc sélectionner uniquement les caractéristiques significatives.

*Covariance aux transformations géométriques-

*Localisation (c.a.d. que le recadrage ne doit pas altérer les caractéristiques restantes).

On peut remarquer tout de suite que ce genre de recherches rejoint les techniques utilisées dans la reconnaissance de formes.
Ainsi M.Kutter, S.K. Bhattacharjee et T. Ebrahimi proposent dans une de leurs publications un exemple de watermarking de seconde génération.

Dans un premier temps ils recherchent des points caractéristiques de l'image. Il existe de nombreuses méthodes pour trouver ce genre de points (comme celles du tracking, directement venues du traitement d'images ou de la reconnaissance de formes). Dans leur exemple, ils ont choisi une décomposition de l'image par l'utilisation de type "chapeau-mexicain". Il est intéressant de remarquer ici, que dans le cas d'un watermarking de seconde génération la robustesse du marquage face aux divers transformations repose en grande partie sur la stabilité des points caractéristiques (c.a.d. retrouver toujours les mêmes points quels que soient les transformations infligées à l'image).

Dans une seconde partie, ils segmentent l'image par l'algorithme de des diagrammes de Voronoi, en prenant comme base les points trouvés précédemment. Une segmentation, c'est tout simplement un découpage de l'image en différentes régions qui sont étiquettées.

On passe ensuite au marquage proprement dit. C'est à dire que l'on va marquer chacune des régions trouvées précédemment. Dans leur exemple, ils utilisent la composante bleue. Ce watermarking est appliqué sur chacune des régions. Il est intéressant à ce niveau de revenir en arrière pour se rendre compte de l'utilité de cette méthode. En effet, avec cette méthode on remarque que le watermarking est lié aux parties les plus importants de l'image. Donc si l'attaque porte sur ces points, il est vrai que le watermarking va disparaître, mais l'image perdra complètement de sa valeur car ses caractéristiques les plus importants auront étés altérées.

Ainsi, ce qui est recherché dans cette méthode ; c'est que si l'on veut s'attaquer au marquage, on va détruire l'image. Marquage et image sont donc intrinsèquement liées.

### 1.3.5. Signature par modulation d'amplitude sur les images couleurs

Cette méthode à été proposée en 1998 par Martin Kutter. Elle repose essentiellement sur des arguments statistiques. Il s'agit d'un marquage d'images en couleurs (Rouge, Vert, Bleu). Le but du marquage est (entre autre) d'être invisible pour l'oeil humain. C'est pour cette raison que la signature est uniquement sur la composante bleue de l'image, car c'est au bleu que l'oeil est le moins sensible. De plus un générateur pseudo aléatoire est utilisé pour générer une succession de positions au sein de l'image à marquer  Ces positions représentent les positions ou vont avoir lieu les marquages, et servent donc en l'occurence de clef secrète K pour retrouver la signature. Je ne vais détaillé plus la méthode mais elle permet , à partir d'une analyse statistique de l'image, d'associé une signature (un signal) bien particulière à l'image.

## 1.4. LES ATTAQUES

Nous allons aborder la question des attaques que peut subir un tatouage numérique. La sensibilité d'un marquage vis à vis des attaques est très importante. Elle influe sur deux des caractéristiques du marquage : la robustesse et la sécurité. Nous parlerons dans un premier temps des attaques dites « aveugles » (ou « blind ») qui mettent à l'épreuve la robustesse du tatouage. Ensuite, nous aborderons la sécurité des marquages face aux attaques « malicieuses » (ou « malicious »).

### 1.4.1. Les attaques aveugles

Le pirate sait que l'image est tatouée. Il cherche à laver l'image du marquage. Mais, le pirate a peu de connaissances sur l'algorithme de tatouage employé. Il cherche à

mettre en défaut le détecteur de marquage en appliquant des transformations à l'image. Il espère que celles-ci seront suffisantes pour que l'on ne puisse plus détecter le marquage. Comme dans le cas d'un vrai tatouage, celui-ci doit être résistant à toutes les formes de nettoyages et son extraction de façon « brute » doit laisser une cicatrice suffisamment importante pour rendre le document quasiment inexploitable. Le pirate a, à sa disposition, toute une palette d'attaques que l'on peut séparer en deux groupes.

#### 1.4.1.1. Les transformations géométriques

***Symétrie horizontale :** Certaines images peuvent être "flipper" sans perdre de leur sens (par exemple un paysage). Bien qu'il ne s'applique qu'à peu d'images, lorsqu'il se produit, très peu de marquages lui survivent. Ce serait une grave erreur de penser que l'on ne peut pas appliquer ce genre d'attaque à un film. En effet, essayez vous même de regarder un film qui a subit cette transformation, et vous ne vous apercevrez de rien du tout (sauf dans les scènes ou de l'écriture intervient).

***Rotation :** C'est une transformation qui est très utilisée après avoir scanné une image. Elle sert à réaligner des images (avec des petits angles) et peut être fatale à certains types de marquages.

***Le recadrement :** Dans certains cas, les personnes ne sont intéressées que par un morceau de l'image (par exemple le centre). Elle recadre (en anglais "crop") alors l'image, ce qui peut détruire le marquage.

***Changement d'échelle :** Ce genre de transformations peuvent être séparées en deux groupes : les transformations uniformes (pour lesquelles on conserve les proportions, l'échelle en X varie comme l'échelle en Y) et bien sûr les transformations non uniformes (où l'échelle en X ne varie pas comme l'échelle en Y).

**Transformations géométriques:** On se contente de faire un mélange de rotations, changements d'échelles non uniformes.

**Filtres passe-bas :** Encore une fois, on utilise pour travailler dans l'espace des fréquences de l'image et dans on ne laisse alors passer que les basses fréquences. En fait, dans des termes un peu plus mathématiques, il ne s'agit ni plus ni moins que d'un produit de convolution du signal (ici l'image) avec une fonction passe bas (dont la transformée de Fourier est une Gaussienne, une fonction porte etc .... ).

**Accentuation des contours :** Ou encore appellé filtre "passe-haut" (car il supprime les basses fréquences), ou "Sharpen". Il s'agit de l'inverse du filtre passe-bas (encore appellé "Blur"). L'intêret d'une telle attaque est assez faible, sachant que l'on conserve le bruit (et les forts gradients de l'image), et que c'est souvent à ce niveau la que se situe le tatouage (car c'est dans ces zones ou l'on cache de préference de l'information).

**Attaque par Mosaique:** Il s'agit ici d'utiliser le "crop" d'une façon beaucoup plus violente et qui se prête assez bien aux pages HTML. Il suffit de découper l'image en autant de morceaux que l'on désire (plus il y a de morceaux plus l'attaque à des chances d'aboutir), puis de recoller cette image au moment de l'affichage en créant par exemple en HTML un tableau dont chacune des cellules contiendra un morceau de l'image. Cette attaque est très peu applicable en pratique, et heureusement car elle est d'une rare efficacité si l'on se donne les moyens de bien découper l'image.

#### 1.4.1.2. Les transformations fréquentielles

Les attaques ne sont pas toujours réalisées par des pirates mais parfois inconsciemment. Ainsi, la compression MPEG2 d'un film, va attaquer de façon relativement importante l'image. La quantification va modifier les coefficients de la DCT (surtout pour les hautes fréquences). Ainsi, toutes les compressions avec pertes

vont endommager l'image et altérer la détection du tatouage. J'ai pu constater que l'utilisation de compressions MPEG4, par l'intermédiaire d'un codec tel que DivX, entraîne souvent une altération très importante du tatouage. Il est indispensable que les nouveaux marqueurs en tiennent compte. A coté de cela, le pirate dispose de nombreux filtres (passe haut, passe bas, ou même passe bande) qui vont lui permettre de rechercher le meilleur compromis entre la disparition du tatouage et une faible dégradation de la qualité de l'image.

### 1.4.2. Les attaques malicieuses

Ce type d'attaques est beaucoup plus intéressant car il demande des connaissances en traitement du signal ainsi qu'une analyse sérieuse du marquage. Les attaques malicieuses sont différentes des attaques aveugles car le pirate va s'attacher à trouver la faiblesse du système qui utilise le marquage. Selon cette faiblesse, il ciblera son attaque.
Par bien des aspects, cela se rapproche beaucoup de la cryptanalyse (l'art de briser les systèmes de chiffrement en cryptologie).

#### 1.4.2.1. Exemple d'attaque sur le copyright

Comme nous l'avons vu, une des utilisations du marquage peut être la protection des droits d'auteur (« copyright »). Par exemple, le document va être tatoué avec en paramètres le nom de l'auteur, l'identification du contenu, un secret etc. Seul l'auteur connaît ces paramètres. Cette version marquée sera mise à disposition sur Internet. La version originale ne sera pas divulguée. L'auteur est le seul à pouvoir détecter le marquage pour prouver que ce document lui appartient.
Dans ce cas précis, le pirate va chercher à semer le trouble sur l'origine de l'image. En effet, il ne sert à rien d'ajouter une autre marque au contenu divulgué sur Internet. L'auteur a toujours à sa disposition la version originale. Le pirate essaie plutôt de recréer une image originale (c'est à dire sans marquage) en soustrayant un faux marquage . Ainsi, il existe deux personnes prétendant avoir la copie originale du contenu divulgué sur Internet. Il est impossible de confondre l'usurpateur.

#### 1.4.2.2. Exemple d'attaque sur la protection de copie

Ici, tous les contenus (films, fichiers musicaux …) vont être tatoués avec la même clef. Sachant cela, le pirate va chercher à estimer cette clef, ce qui lui permettra de laver tous les contenus.
Voici une description très simplifiée de « l'average attack ». Le pirate veut trouver la clef utilisée pour marquer un film. Pour simplifier, supposons que la clef soit aussi le signal de marquage : *W*. Pour tout contenu original $I^k$, la version tatouée est obtenue ainsi :

$$I^k_w \quad = \quad I^k \quad + \quad W$$

Le pirate recherche *W*. Il a accès à toutes les images tatouées $I^k_w$, mais il ne connaît pas les images originales $I^k$. Or sur un grand nombre d'images, la moyenne des images non tatouées tend vers un gris uniforme de valeur *G* (hypothèse simpliste). On peut écrire :
Ainsi, il pourra estimer la clef et la soustraire à chaque image pour pirater les contenus.
Une implémentation de cette attaque à été réalisée en tenant compte d'hypothèses plus réalistes. L'image originale est estimée par un filtrage passe-bas *F(.)* de l'image tatouée $I_w$ :

$$\hat{I}=F(I_w)$$

Le marquage est estimé par une simple différence :

$\hat{W}=I_w \quad \hat{I}$

On tient compte de la variation locale de la force du marquage par une étude HVS de l'image originale reconstruite $\hat{I}$.
Ceci est fait sur un grand nombre d'images tatouées. Les différents signaux $\hat{W}_k$ sont moyennés dans un buffer pour améliorer la qualité de l'estimation.

## 1.5. LA STEGANOGRAPHIE

Stéganographie vient du Grec "steganos" (dissimulé), et "graphy" (écriture) et signifie donc "écriture dissimulée". En effet c'est l'art de dissimuler des données.
Cette technique a pour objet la dissimulation de données dans des documents. Le but premier de cette technique est de permettre la signature de documents (pour pouvoir y mettre des copyright) mais on peut l'utiliser pour d'autres choses (plus ou moins légales). Le plan que nous allons adopter va nous permettre de passer en revue les différents supports numériques utilisés pour dissimuler des données: le texte, l'image, le son, la 3D . Pour ceux qui sont interessés je propose un bref historique de la stéganographie.

### 1.5.1. Histoire

Bien que ce qui nous intéresse ici est en rapport avec l'informatique il peut être intéressant de revenir un peu en arrière. Ainsi on se rend compte que la première forme de stéganographie répertoriée nous vient d'une histoire Grèque signé Herodotus et datant du 5eme siècle avant Jésus-Christ. L'auteur nous relate la révolte contre les lois Perses. Afin de communiquer secrètement deux chefs de guerre utilisèrent des esclaves. Ils leurs tatouaient sur le crâne le message et ensuite les cheveux repousser. L'esclave était ensuite envoyé chez le correspondant trompant ainsi l'ennemi. Une fois rasé le message était parfaitement lisible. Bien que très rudimentaire, cette méthode est un assez bon symbole de ce qu'est la stéganographie

Une autre forme de stéganographie nous est familière. Il s'agit en effet de l'encre invisible. Méthode qui a déjà fait ses preuves. On en entend parler dans les écritures Arabes et a été très utilisés par les étudiants du moyen âge. Cette encre est fabriquée, alors, à base de jus d'oignons et de chlorure d'ammoniac. L'écriture est ensuite rendue visible grâce à une source de chaleur (comme une flamme par exemple).

Ces encres furent utilisées durant la guerre de sécession (1775-1783)pour transmettre des messages entre George Washington et des agents tels que Benjamin Tallmadge
Allez, une petite illustration des mes dires avec un message camouflé de façon très insidieuse dans une clou qui était ensuite planté au milieu d'autres dans une surface en bois. Vous pouvez ainsi vous rendre compte de la difficulté de la découverte du message

Dans ce document je vais parler très librement de tatouage ou de marquage ou Stéganographie (en anglais: steganography ou data hiding) et de watermarking (ou tatouage).
En fait, on peut considérer que le watermarking est une sous-partie de la stéganographie. Dans le cas du Data Hiding, on cherche à dissimuler une quantité très importante de données (par exemple une image dans une autre image).
Dans le cas du watermarking, on cherche juste à marquer une image (on se limite

souvent à la dissimulation d'un bit: marquée/pas marquée). Le but du watermaking est de dissimuler une information qui à pour but de démontrer l'intégrité du document ou encore de protéger les droits d'auteurs.
Une autre différence très importante entre la stéganographie et le watermarking se situe au niveau des attaques qui peuvent avoir lieu contre ces techniques. En stéganographie, le pirate va chercher à lire les données dissimulées dans le document, tandis que dans le cas d'un document "watermarké" va chercher à "laver" le document de toute signature possible (ou alors il peut essayer d'usurper l'identité de l'auteur).

### 1.5.2. Marquage dans le Texte

La dissimulation de données dans du texte est une chose bien particulière, et comme nous allons le voir elle n'a pas grand chose à voir avec l'image ou le son. Et ceci pour plusieurs raisons: on ne travaille pas avec le texte dans "l'a peu près". Je m'explique, dans une image on peut considérer qu'endommager" celle ci avec un filtre passe-haut suffisamment "léger" ne change quasiment rien à la perception que nous allons avoir de celle-ci. Par contre avec un texte, soit le texte est comme l'original soit il ne l'est pas. Celui ci ne permet quasiment aucune modification. Une des exigences de la dissimulation de données est d'endommager le moins possible le texte original. Pour cela nous allons utiliser la méthode dite des "espaces".

#### 1.5.2.1. Méthodes des "espaces" (en fin de phrases)

C'est une méthode qui peut être vous sembler simpliste mais bon dans le cas du texte il n'y pas beaucoup de choix. Il y a encore ici 2 méthodes différentes quoi que reposant sur le même principe. La première méthode consiste à mettre des espaces en fin de ligne. On se définit un code à suivre et l'on commence:
exemple

0 espace en fin de ligne correspond à 0.
1 espace en fin de ligne correspond à 1.

Ca y est nous avons la base pour coder un message. Ex: ( ici les espaces sont remplacés par des "_" pour plus de lisibilité ).

bonjour ceci est un message caché. A vous de le lire. Je pense que vous commencez_ à comprendre le principe. Malheureusement tout n'est pas rose. Mais bon, nous arrivons quand même à dissimuler un octet.
Comme vous pouvez le voir dans notre exemple nous avons codé:
0 espace; 1 espace; 1 espace; 0 espace; 1 espace 0 espace; 1 espace; 1 espace.
<=> 01101011
Voici un octet de dissimulé. Les problèmes liés à la méthode:
- Il faut énormément de lignes pour coder peu de texte. En effet, il faut 8 lignes pour coder 1 octet. Donc imaginons que l'on veuille coder une phrase de 20 mots (chaque mot faisant environ 4 caractères) et que l'on code chaque caractères sur 7 bits (on optimise comme on peut), il va nous falloir environ 560 lignes rentabilité mauvaise
- Très visible par une personne extérieure qui s'y attend un peu. Et donc facilement manipulable.

Les avantages:
- Très facile et donc très simple à implémenter. Et puis ça peut marcher avec de nombreuses personnes. Bon je vois déjà des petits malins qui se disent qu'il suffit de rajouter des espaces pour coder plus de caractères sur moins de texte (vous me suivez ?). Et bien oui, mais bon alors la ça se voit comme le nez au milieu de la figure. Pour ceux qui ne comprennent pas je réexplique : En utilisant 3 espaces:
- 0 espace <=> 00
- 1 espace <=> 01

- 2 espace <=> 10
- 3 espace <=> 11

Il faut alors 4 lignes pour coder 1 octet (au lieu de 8).

#### 1.5.2.2. Méthodes des "espaces" (entre les mots)

Cette méthode est basée sur le même principe, mais cette fois-ci nous allons coder notre texte dans le nombre d'espaces entre chaque mots. C'est encore plus visible que la méthode précédente, mais le rapport texte codé sur texte hôte est beaucoup plus important.

On se met d'abord d'accord sur une convention :

- un espace entre 2 mots suivit de deux espaces entre les 2 mots suivants <=> 0
- deux espaces entre 2 mots suivit d'un espace entre les 2 mots suivants <=> 1

Pour mieux comprendre voici un exemple avec le texte suivant:

Ceci_est__essai__de_texte__caché_dans__un_texte_hôte. Vous__devez__avouer que_ce__n'est_pas_très__subtil.

_ __ : 0
__ _ : 1
__ _ : 1
__ _ : 1
_ __ : 0
__ _ : 1
__ _ : 1
_ __ : 0

=> 01110110

Et ça y est vous avez codé un octet. Voici le texte tel qu'il va réellement apparaitre, à vous de jugez si cela vous convient:

Ceci est un essai de texte caché dans un texte hôte. Vous devez avouez que ce n'est pas très subtil. Voyons un peu le rapport texte à coder sur texte hôte. Il vous faut 2 mots pour un bit, donc pour une phrase de 20 mots (20*7=240 bits), il faut un texte hôte de 480 mots, en comptant 10 mots par ligne on arrive à environ 50 lignes. On gagne un rapport de 10 comparé à la méthode des espaces en fin de ligne. Pas mal !! à vous de juger. Si vous pensiez que ces méthodes étaient étranges, attendez de voir les suivantes.

#### 1.5.2.3. Méthode des synonymes

Alors là votre texte ne va pas être désorganisé mais il risque au niveau sémantique d'être grandement modifié. Encore une méthode simple à comprendre..... Il suffit de créer une table des synonymes du genre:

Hypothèse

| 0 | 1 |
|---|---|
| gros | obèse |
| petit | minuscule |
| riche | fortuné |
| beau | joli |
| nourriture | aliment |
| bateau | navire |
| femme | épouse |
| tranquille | calme |

Exemple de  texte: Au loin je vois mon gros navire sur la mer tranquille. Oui je suis fortuné, j'ai une belle épouse et je mange de très bons aliments, et ma voiture est loin d'être minuscule.
Dans ce texte qui a l'air innocent nous avons masqué 1 octet:
gros : 0
navire : 1
tranquille: 0
fortuné : 1
belle : 0
épouse : 1
aliments: 1
minuscule: 1
<=> 01010111
Cette méthode est attrayante mais très difficile à mettre en oeuvre en pratique, et surtout il faut quand même s'autoriser une petite vérification du texte. En effet, notre langue française ne permet pas tout écrire. Par exemple: je vois passer dans la rue une superbe femme et je vois passer dans la rue une superbe épouse peut prêter à confusion.  Autre méthode

#### 1.5.2.4. Méthode syntaxique

Cette méthode est relativement peu utilisable. En effet cette méthode peut altérer le sens d'une phrase, demande énormément de texte pour en coder peu. On part du principe que certaines règles de grammaire sont un peu litigieuses et donc modifiables, sans pour autant choquer le commun des mortels . Voici l'esprit de la méthode.
Voici deux phrases quasiment équivalentes:

après y avoir passé deux mois et trois jours
après y avoir passé deux mois et, trois jours

La virgule après le "et" ne choque pas trop dans certains cas on peut donc se permettre coder un bit sur le respect ou non de la virgule après le "et":

et <=> 0
et, <=> 1

Le nombre de mots qu'il faut pour coder une phrase est donc très important. Mais pour coder le message on pourrait utiliser plus d’une seule règle.

### 1.5.3. Une typologie des marquages

La stéganographie sur un support texte est quelque chose qui ne supporte pas la fantaisie. En effet chaque retouche est directement visible par le lecteur. D'autre part un texte signé par les méthodes décrites est relativement facilement identifiable.
L'Image
Il s'agit ici du domaine le plus vaste et certainement du plus intéressant. En effet, les applications sont très nombreuses, et les méthodes à utiliser sont assez complexes (comparées à celles utilisées pour le texte). Le marquage d'images a de nombreux buts: copyright des images (très important sur l'Internet où des milliers d'images circulent sur le web), mais aussi marquage de papiers ou de billets (pour éviter le photocopiage), vérification de l'intégrité de documents  etc... A chaque utilisation correspond une méthode. En fait les techniques doivent répondre à certaines règles très importantes et souvent difficiles à concilier:
- endommager le moins possible le support sur lequel le marquage va avoir lieu. (l'oeil humain ne doit pas être choqué).
- le marquage doit pouvoir supporter le plus grand nombre de transformations possible sans être dégradé (compression JPEG, filtres, passage analogique- numérique, changement de palettes , les différentes attaques possibles sur le marquage).

- la complexité de l'algorithme doit être minimum afin de pouvoir effectuer le marquage et/ou la détection en temps réel.

Le marquage peut avoir lieu au niveau de l'image dans le domaine des fréquences:
-Technique de Watermarking tenant compte de la corrélation HVS-Canaux RGB ou même plus traditionnellement dans le domaine spatial:

-Bits de poids faibles
-Signature par modulation d'amplitude
-Watermarking par DCT à taille de blocs variable

Nous parlerons même du watermarking de la seconde génération. (un exemple proche est celui par modification géométrique). Certaines méthodes utilisent même la palette pour marquer l'image (dans le cas ou l'image possède un palette, comme pour le marquage EzStego).
Les premières méthodes de signature d'images ont étés proposées en 1993 par Caronni (bien que des articles plus anciens faisaient déjà allusion à ce type de pratiques). Les méthodes les plus récentes portent les noms de Anderson, Aucsmith, et Swansonet Al.
Les méthodes utilisées dans la stéganographie dépendent surtout du type de marquage que l'on désire:

-Marquage privé : Dans ce cas précis, on a besoin de l'image originale. Et là encore on différencie deux types:

1er type : On utilise l'image originale, l'image marquée et la clef. A partir de cela on retrouve la marquage.

2e type : On a besoin de l'image originale, de la clef, et de l'image marquée et du marquage pour savoir si OUI ou NON l'image marquée contient le marquage donné..

-Marquage semi-privé : Ici, pas besoin de l'original. on a juste besoin de l'image marquée, du marquage et de la clef pour savoir si OUI ou NON l'image contient le marquage. Ce marquage est très utilisé (par exemples pour les DVD).
En effet, imaginons un marquage spécifique à chaque pays. Le lecteur de DVD lance une application qui, avec le CD inséré dans le lecteur (image marquée) et la clef, il va regarder si l'image à été marquée et va alors autoriser ou non la lecture du DVD.

-Marquage public : (appelé aussi marquage aveugle). C'est ici le problème le plus intéressant. On ne possède ici que l'image marquée et la clef. Cela suffit à faire apparaître le marquage.

Clef(Image marquée) = Marquage

## 2.2. LES TECHNIQUES DE TATOUAGE

La principale technique de tatouage est le *watermarking*. Mais il existe aussi le
*Fingerprinting*. Ces techniques ont pour objet d'insérer des informations (texte,
code, etc.) à l'intérieur des données numérisées. Ces informations pourront prendre la forme d'un tatouage, d'un filigrane ou d'une empreinte. Cet ajout de données doit rester caché pour l'utilisateur de l'œuvre.

De nombreuses recherches scientifiques se sont développées ces dernières années sur ces sujets. Le but de ces recherches étaient de protéger les œuvres numérisées. Avec le développement des SDRM, ces techniques ont pour objectifs d'identifier, d'authentifier et de tracer les œuvres numérisées. De plus de nombreuses informations pourraient leur être associées concernant les droits si les techniques le permettaient.

# 2. APPLICATION DU *WATERMARKING* AUX DRM

Cette technique a pour but de rendre indissociable le lien œuvre numérisé ou numérique, données attachées à l'œuvre. Dans le cas des images, du flux audio ou vidéo, du texte etc..
Les filigranes, empreintes ou tatouages sont rendus indissociables des données ou du signal numérique dans lequel l'œuvre est codée. La stéganographie doit les rendre de plus imperceptible par l'utilisateur de l'œuvre.

## 2.1. LE TRACAGE PAR LE WATERMARKING ET LE FINGERPRINTING

La fonction du watermarking est la protection de l'œuvre. Attachée à l'œuvre, des informations sur ses droits sont contenues dans un filigrane ou une empreinte et sont donc transportées avec elle. Deux fonctions sont contenues dans ce marquage: : l'authentification de l'objet numérique et de son intégrité.
Le fingerprinting consiste à superposer plusieurs tatouages sur une même œuvre. A chaque traitement un nouveau tatouage est apposée. De même lors d'une copie un autre tatouage est "imprimée" dans l'œuvre. De cette façon l'œuvre peut être tracée et sa diffusion contrôlée.
Le watermarking peut être utilisée comme une signature numérique. La preuve de l'intégrité ou de l'origine de l'œuvre peut être apportée grâce à ce marquage. Si des informations concernant les titulaires du droit d'auteur ou des droits voisins et le régime des ces droits sont inscrits dans le marquage, les systèmes de DRM (Digital Right Management) peuvent les détecter. De même le droit de reproduction peut être contrôlé et les informations peuvent être vérifiées si elles ont été altérées.
Le watermarking est neutre par rapport aux divers applications qui utilisent. les œuvres. De grands progrès ont réalisés en terme de protection,. Mais la persistance des insuffisances de cette technique font qu'elle doit être associée à d'autres techniques, ,notamment les techniques cryptographiques.
Dans la cadre des DRM, la stéganographie, qui emprunte aux techniques de *watermarking* désigne plutôt un usage de ces techniques pour l'échange d'informations dissimulées.

## 2.2. MÉTHODES

Techniquement, le watermarking consiste à ajouter une quantité d'informations
numériques au signal (audio, vidéo, image, texte, etc.) par un algorithme de codage ou
« tatoueur ». Cet ajout doit, pour avoir une signification technique et économique

dans les industries culturelles, offrir des qualités de robustesse au sens où les signaux
peuvent avoir à subir des transformations nombreuses et variées par leurs natures :
compression, étirement, rotation, ajout de bruit, ré-échantillonnage, etc. qui ne doivent
pas altérer le tatouage même.

Le volume d'informations est en pratique fonction de la nature du signal, par exemple en général de l'ordre de 64 bits pour un flux vidéo de quelques secondes ou une image de taille importante qui permettent une quantité d'informations utiles. Or, pour les DRM, ce volumed'informations, objet du filigrane, doit répondre à des objectifs contradictoires :– un objectif d'imperceptibilité pour ne pas déformer l'oeuvre ou sa perception ;– un objectif de résistance aux attaques qui implique une quantité substantielle d'informations tatouées.

Les algorithmes de tatouage ont connu des évolutions importantes pour répondre à l'objectif de sécurité. L'idée générale consiste à introduire un biais dans la répartition statistique des données numériques des oeuvres. Ce biais statistique sert à coder l'information que l'on veut dissimuler, tout en étant très peu visible. Les méthodes d'introduction du biais statistique sont variées et dépendent notamment de la nature des oeuvres : images, flux audio ou vidéo.

Pour répondre à des objectifs de protection des oeuvres le watermarking doit présenter des qualités spécifiques comme la non réversibilité. Mais ces évolutions ne suffisent pas à assurer une protection technique du médium lui-même. C'est pourquoi les techniques de watermarking sont associées soit à des mesures techniques relevant de la cryptographie, soit de la cryptologie, autrement dit d'un système à clefs secrètes : une tierce personne de confiance génère pour chaque oeuvre :

-une clef secrète de tatouage, qui permet à l'éditeur d'insérer le tatouage dans l'oeuvre

-une clef de lecture qui permet de décrypter le tatouage.

Le biais peut se situer au niveau de la parité des nombres servant à coder la couleur de chaque point de l'image pour les algorithmes les plus rudimentaires, de la transformée de Fourier de l'image, de la décomposition en ondelettes de l'image. Les algorithmes de tatouage peuvent être rendus plus robustes en utilisant comme repères de coordonnées des éléments distinctifs de l'image, les coins des objets par exemple ou en éparpillant les éléments du tatouage sur la totalité de l'oeuvre, et sur la représentation spectrale de l'oeuvre.

## 1.1. APPLICATIONS DU *WATERMARKING* A DES FINS DE PROTECTION.

On utilise les techniques de tatouage pour contrôler si les droits

définies par les titulaires de droits sont respectés par les utilisateurs des oeuvres. Ce contrôle peut se faire soit à l'enregistrement de l'œuvre ou à sa lecture. Mais les solutions techniques sont peut fiables.Les applications sont le plus souvent relatives au régime des droits. Elle consiste à contrôler l'utilisation des droits en renforçant une mesure technique de protection. Elle peut aussi être utilisée comme une technique d'identification relative au régime des droits.

### 1.1.1. Mise en œuvre d'un contrôle d'enregistrement ou de lecture

Un détecteur de watermarking peut empêcher la continuation de l'enregistrement si un watermarking indique qu'elles sont protégées.
En lecture, deux watermarking sont combinés:

un watermarking robuste indiquant que l'œuvre est protégée et
un watermarking fragile.

Si deux watermarking existent et autorisent chacun d'eux un accès licite à l'œuvre ou bien si les contenus ne contiennent pas de watermarking(contenus non protégés) l'œuvre peut être exploitée.
Par contre si le watermarking fragile disparaît lors d'une manipulation du contenu non autorisée (par exemple lors d'une compression pour transmettre le contenu par Internet (cas SDMI) ou lors de la copie (cas SACD) l'œuvre ne peut pas être exploitée. En effet, après la compression, le watermarking robuste indiquant que l'œuvre est protégée , existera toujours dans le contenu mais le watermarking fragile aura disparu. :La lecture de l'oeuvre est alors inexploitable.

### 2.2.1. Points forts et points faibles

Le principal avantage de cette dernière approche est qu'elle ne vise pas directement les pirates. Elle vise plus à bloquer l'utilisation des contenus piratés chez un utilisateur normal. Le niveau d'exigence de cette technique en terme de robustesse est donc plus réduit.

Les inconvénients(notamment par rapport aux techniques cryptographiques )(A et B°

A/La robustesse des systèmes cryptographiques peut, en général, souvent toujours être améliorés en y mettant le prix bien sûr. On peut allongeant la longueur des clés. On peut en améliorant la résistance au « tripatouillage » des logiciels ou des circuits imprimés ou intégrés.

Par contre, le watermarking est très vite limité. La quantité d'informations tatouables dans un contenu est limitée de par la taille limité de l'œuvre (bien que la taille des contenus ne cesse d'augmenter) . De plus les progrès des techniques de compression vont dans le sens d'une diminution de l'information non directement utile à la qualité du contenu. Le watermarking apparaît souvent comme une information accessoire au contenu et donc supprimé au cours de la compression

B/ le watermarking est fragilisé par la mise à disposition d'un détecteur de marquage. En effet, l'utilisation du watermarking à des

fins de protection technique suppose que les dispositifs de lecture ou d'enregistrement contiennent un détecteur de watermarking, que les pirates pourront donc utiliser à des fins d'analyse. Dans l'hypothèse où il existe des contenus non protégés (cas des contenus autoproduits), des travaux de recherche semblent démontrer qu'un tel dispositif présente une faible robustesse et n'est pas adapté.

Force est de constater que toutes les méthodes de protection à base de tatouages ont systématiquement attaquées avec succès, y compris des produits de tatouage d'entreprises disposant de brevets très spécifiques et d'un niveau élevé de recherche. Les analyses d'évaluations des systèmes de watermarking semblent conclure aux mêmes résultats décevants en termes de protection, qu'il s'agisse d'attaques concernant le marquage d'images, du signal vidéo ou du signal audio, y compris par des méthodes d'attaques relativement simples.

### 1.1.2. Les usages de gestion.

Les techniques de tatouage pourrait être utilisées pour une gestion numérique des droits. L'information inscrivant la représentation des droits serait tatouée dans l'œuvre elle-même.

Ainsi, par exemple, pour la gestion du nombre de copies autorisées le watermarking a tenté d'être utilisé. Mais il apparaît très vulnérable aux attaques des systèmes électroniques de lecture. Dans le cas des supports comme le CD Audio ou le DVD, la question du watermarking n'a pas été envisagée dès la conception de ces lecteurs. L'existence d'une base importante de lecteurs ou d'enregistreurs non conformes semble condamner les techniques de watermarking pour protéger valablement les oeuvres.

Ainsi les fonctions techniques de protection ne peuvent pas être remplies par les techniques de watermarking. Les fonctions moins sensibles d'authentification et la fonction de preuve seraient plus faciles pour le watermarking. Mais le problème vient de ce qu'un marquage qui n'obéit pas au critère de non-réversibilité peut être employé par plusieurs personnes qui pourraient attester de l'origine d'une œuvre

Ainsi, les techniques de watermarking devraient pouvoir être utilisée comme une couche parmi d'autres de mesures de protection technique notamment cryptographiques. Elles doivent surtout s'intégrer dans des mécanismes institutionnels mais aussi techniques d'évaluation voire de certification. Ce sont ainsi développés des outils ou des entreprises qui poursuivent cet objectif. En effet, cette évolution apparaît nécessaire parce que l'apport principal de ces techniques est surtout de l'ordre de la preuve numérique en ce qui concerne l'intégrité, l'authentification, la datation, etc. Ces évolutions sont d'autant plus probables que les techniques de watermarking sont loin de ne devoir être utilisées que pour la protection de la propriété intellectuelle . Elles intéressent par exemple le domaine de la santé (imagerie médicale), l'administration

de documents, etc. donc davantage des applications de services.

## 1.2. LE FINGERPRINTING.

Les fonctionnalités élevées en termes de protection des œuvres ne condamnent pas systématiquement ces techniques pour la propriété intellectuelle au sens large. Un certain nombre d'entreprises ou d'organismes, au plan national et mondial tentent de développer de nouveaux usages.

Une application concerne la traçabilité des contenus, à des fins de lutte contre la contrefaçon. La mise en place d'un fingerprinting systématique des oeuvres, visant à intégrer dans l'oeuvre un identifiant de l'utilisateur, doit permettre, par l'analyse d'une oeuvre circulant sur les réseaux de peer to peer, de détecter et d'identifier l'utilisateur à la source de l'introduction sur ces réseaux.

L'identification d'un pirate peut conduire à des poursuites judiciaires. Mais il est difficile de conférer au fingerprinting le statut juridique de preuve. De plus à cause du délai d'aboutissement d'une telle action, le fingerprintig a plutôt une valeur dissuasive. Les opérateurs de télévision à péage , par exemple, rencontrent des difficultés dans l'identification des systèmes pirates. et sont soumis à des coûts de renouvellement important des cartes à puce. Une identification des oeuvres par est intéressante à des fins techniques, comme contribution au maintien de la protection par la révocation des systèmes pirates et le renouvellement des clés ou des systèmes compromis. Le cadre le plus adapté à une telle application est celui des services interactifs, pour lesquels il est possible d'appliquer le fingerprinting à la source, avant diffusion. Cela fait du fingerprinting un outil très complémentaire de la cryptographie.

Dans le cadre particulier du cinéma numérique, l'utilisation de fingerprinting peut
s'avérer également intéressante. Elle consisterait à insérer à chaque étape de la chaîne de
diffusion des éléments d'identification par fingerprinting. Si le fingerprinting est ajouté à
partir d'une clé privée associée de manière unique à chaque appareil et sécurisée de
manière à ne pas pouvoir être détournée, le fingerprinting ainsi constitué serait
susceptible de constituer une preuve.

Les applications de ces techniques à des fins de traçabilité sont le suivi automatique d'audience et le contrôle des rediffusions dans le cas de la télévision. Les solutions implémentées consiste à ajouter du watermarking dans le flux vidéo numérique (MPEG2) en temps réel Ainsi il est possible de comptabiliser automatiquement la consommation des oeuvres diffusées La société Nextamp(issue de Thalès) exploite ce type de techniques. La société Médiamétrie pourrait ainsi automatiser ses activités

# 3. Systèmes Numériques de Gestion des Droits(SNGD) ou SDRM

Les SNGD sont conçus pour remplir les besoins des titulaires de droits d'auteur ou droits voisins. Ces SNGD, en anglais Digital Rights Management Systems, ont pour fonctions essentielles de permettre aux titulaires de droit d'autoriser ou d'interdire la représentation et la reproduction des œuvres et ainsi d'exercer les droits exclusifs reconnus par la loi sur leurs œuvres. De tels systèmes ne sont concevables que dans l'environnement numérique, renforcés par la possibilité de communications par réseaux. Les principales sociétés qui commercialisent ces systèmes sont Microsoft, Sony, Thomson, Philips, IBM, HP..

Avec ces systèmes, l'exercice des droits des titulaires se fait sur un ensemble de licences d'utilisations octroyées à des consommateurs d'œuvres culturels. En contrepartie de l'octroi de licences, l'utilisateur consent à un paiement. Un système automatisé de rémunération constitue une partie des SNGD mais le but des SBGD est d'automatiser toute la chaîne de contrôle de la reproduction et de la représentation de l'œuvre. Par les technologies informatiques de base, comme le cryptage et le tatouage, destinée à réaliser un marquage des œuvres, les SNGD sont considérés généralement comme des mesures techniques de protection.

S'ils peuvent être considérés comme un ensemble organisé et cohérent de mesures de protection, les DRMS assure de toutes les fonctions permettant à des contenus numériques d'être commercialisés dans des conditions juridiques de protection et d'exploitation particulières. C'est que distribuer à un large public une œuvre numérique comporte des contraintes bien supérieures que celles nécessaires pour commercialiser un produit ordinaire. Cela tient à la protection particulière accordée aux œuvres culturels par le droit de la propriété intellectuelle.

Aussi les systèmes numériques de gestion de droits ont besoin pour fonctionner dans des conditions qui respectent les droits de titulaires de droit sur les œuvres, de délimiter un "espace de confiance". C'est seulement dans cet espace que pourra se réaliser la distribution de contenus numériques d'oeuvre diverses. Les fonctions d'un SGND qui nous analyserons sont toutes sensibles. Ainsi en est-il des systèmes de description des droits, d'identification et de protection des contenus numériques, d'identification et d'authentification des utilisateurs, de distribution des licences d'utilisation, de gestion des rémunérations.

Dans un espace de confiance , le titulaire des droits peut avoir

confiance dans l'utilisateur. Il le connaît (authentification), a limité les droits qu'il peut avoir sur l'œuvre en les décrivant précisément grâce à un système de description des droits. De plus il pourra être rémunéré immédiatement par l'utilisateur. Pour créer un espace de confiance, le titulaire de droits et son utilisateur doivent pourvoir échanger des informations en toute confidentialité sans qu'une tierce personne ne puisse connaître d'éléments de leur dialogue. Cet espace doit s'étendre dans tous les environnements où pourrait se situer l'œuvre, depuis le fournisseur (titulaire des droits), en passant par le distributeur(réseaux) jusqu'au consommateur (utilisateur). Pour suivre l'œuvre, il va donc falloir la marquer afin que des outils techniques puissent garantir une sécurité des transactions de l'amont (fournisseurs) à l'aval (consommateur).

Ces outils devront assurer la continuation de l 'espace de confiance entre trois environnements:

–celui des titulaires de droits qui comprend les auteurs, les artistes et interprètes et les producteurs qui sont titulaires des droits exclusifs des oeuvres, et pour les derniers propriétaires des supports de fixation des oeuvres

–celui du distributeur qui doit assurer l'encodage des oeuvres et les droits pour les diffuser au public moyennant rémunération

–celui de l'utilisateur acheteur des licences d'exploitation et du matériel analogique ou numérique.

Ces outils permettent de mettre en œuvre, de l'amont vers l'aval, les fonctions de création (3.1) , de distribution sécurisée (3.2) et d'utilisation de l'œuvre et des droits(3.3)

## 3.1. CRÉATION DES ŒUVRES ET DES DROITS.

En amont de la chaîne numérique de distribution, cette fonction comprend toutes les opérations logicielles nécessaires permettant à une œuvre d'entrer dans l'environnement numérique (ou bien d'être créée directement par un ordinateur) et ainsi que sa gestion. Pour simplifier nous supposerons l'œuvre déjà numérisée. Pour la gérer il va falloir lui associer un ensemble d'informations représentatives des droits que le titulaire souhaite lui donner. Les techniques de marquage des œuvres qui peuvent être employées pour protéger les contenus sont les mêmes que celles qui sont utilisées pour protéger les informations sur les droits

La gestion numérique des droits repose sur un concept fondamental : la séparation des oeuvres sous forme physique de la description de l'information sur les droits associés à ces oeuvres. Ainsi, lorsqu'on souhaite contrôler l'accès d'un utilisateur à une oeuvre, on lui transmet séparément l'oeuvre, sous une forme inexploitable en tant que telle, et la représentation numérique des droits relatifs à cette oeuvre.

Concrètement la gestion numérique des droits se compose de divers outils :
– définition des informations sur les droits
– description par des langages

– architectures des DRMS

### 3.1.1. DEFINITION DES INFORMATIONS SUR LES DROITS.

Les informations sur les droits sont des données qui constituent le régime des droits associés aux oeuvres protégées. Le régime des droits établit donc une relation à l'intérieur d'un DRMS entre l'environnement des titulaires de droits et celui des distributeurs.

Lorsqu'un auteur définit des droits d'exploitation d'une oeuvre, il associe, pour chaque catégorie d'utilisateur et/ou d'utilisation, un ensemble de droits d'exploitation. Ces droits seront des droits de reproduction ou de représentation. Mais les SGND peuvent programmer d'autres utilisations comme par exemple la location, le prêt et toutes sortes de formes d'utilisations fondées sur les stratégies commerciales qui ne seront limitées que par l'imagination des hommes du marketing.

L'utilisation peut se faire en fonction de diverses sortes d'accès ou selon la durée, la qualité des œuvres. Afin de la faire entrer dans l'ordinateur, la description du monde des titulaires de droits devra être numérisée . C'est l'un des enjeux d'un « guichet commun ouvert » de gestion de droits. Un DRMS pourra réaliser une gestion personnelle ou collective des droits de l'auteur Une gestion personnalisée sera plus précise et pourra faire l'objet de rémunérations individuelles proportionnelles à l'exploitation de chaque type d'oeuvres.

L'identifiant est placé à l'intérieur du fichier numériquement représentatif de l'oeuvre, au moyen de deux techniques possibles.

L'étiquetage, en premier lieu, consiste à placer dans la partie initiale du fichier une information donnant la valeur de l'identifiant selon une convention de placement, de codage, de syntaxe et de longueur. Cet identifiant sera alors utilisé comme un lien vers une base de données alimentée par les titulaires des droits.

L'aquamarquage (watermarking), en second lieu, consiste à apposer une marque codée, par exemple sur une image, en la rendant invisible mais facilement décelable.

#### 3.1.1.1. Les outils d'identification des contenus.

Dans le dialogue 'titulaire de droits', distributeur, utilisateur l'oeuvre va circuler et il faut donc l'identifier en lui donnant un numéro ou nom unique.,

##### 3.1.1.1.1. Rôle d'un système d'identification des contenus.

Ce numéro est nécessaire au traitement informatique pour décrire le régime des droits de l'oeuvre. De même les traitements sur sa protection,, sa distribution et son exploitation doivent être réalisés par des outils qui doivent pouvoir identifier le contenu de manière non ambigu.

–Le système d'identification. est choisi par le titulaire de droit. A un contenu donné doit être associé un identifiant unique. Cet identifiant sera distribué avec le contenu . Il ne faut par confondre le contenu et

son identifiant qui pointe vers le contenu

– L'ensemble des identifiants sert au distributeur, pour confectionner son catalogue commercial

–A partir de l'identifiant unique, l'utilisateur peut connaître à qui s'adresser pour demander les droits pour utiliser l'oeuvre et pour gérer son répertoire personnel

La connaissance des identifiants peut être publique. Elle ne renferme aucun secret Si un mauvais numéro est utilisé le seul risque est celui de tomber sur une autre oeuvre..

#### 3.1.1.1.2. Exemple de systèmes d'identification des oeuvres.

La technique de l'étiquetage a été retenue par les organisations internationales des titulaires de droits (plan CIS de la confédération des auteurs, identification des oeuvres audiovisuelles ISAN, voisin du digital object identification DOI lancé aux Etats-Unis), alors que la technique du watermarking conserve un caractère « propriétaire » pour des entités particulières, et notamment pour les agences de photographie.

-Le DOI (Digital Object Identifier) est un système international d'identification des documents publiés sous forme électronique.

– l'ISBN (International Standard Book Number) qui est un numéro international normalisé permettant d'identifier le titre d'un livre

-Le système d'immatriculation des images fixes numériques(photographies, dessins, peintures, illustrations, etc.).

– Les systèmes propriétaires. MPEG

L'initiative de l'élaboration d'identifiants normalisés est également nécessaire. L'initiative de cette élaboration revient, en France, à une coopération engagée en novembre 1993 entre le ministère de la culture, les organisations de titulaires de droits et l'association française de normalisation (AFNOR). Au titre d'une convention triennale 1994-1997 a pu être réalisée un intense travail d'exposition des besoins d'identification et de propositions de solutions. Ces propositions ont été relayées auprès de l'instance mondiale de normalisation ISO, l'initiative des professionnels français s'étant élargie aux instances internationales d'auteurs (CISAC), de producteurs de phonogrammes (IFPI), au monde du cinéma (AGICOA) et aux fédérations d'artistes-interprètes.

Le système d'identification des oeuvres a désormais atteint une phase opérationnelle garantie par la normalisation des codes effectuée selon les lourdes procédures de l'organisation internationale de normalisation (ISO). En ce qui concerne les auteurs, le congrès mondial que la CISAC continue de développer de son Common information system (CIS).

Les codes d'identification, en premier lieu, sont nombreux. L'ISWC (information system works code) a pour objet d'attribuer un code digital unique de 9 chiffres, précédés de la lettre T, à chaque oeuvre musicale, de la même façon que, dans le monde de l'édition, le numéro ISBN identifie chaque livre ou, pour l'industrie phonographique, le numéro ISRC chaque disque. Précédé de la lettre L ou V, le code ISWC peut également désigner un livre ou un contenu visuel.
Le système ISAN, pour International Standard Audiovisuel Number, doit, pour sa part, attribuer un code similaire aux oeuvres audiovisuelles. Sont concernés aussi bien les films et les courts-métrages, les émissions de télévision, les images vidéos et les

morceaux multimédia. Chaque numéro doit pouvoir comporter la langue originale, la durée et le type d'oeuvre ainsi que les langues de traduction possibles.
Peut être également mentionné l'IMLP (Iso Multimedia License Plate), sorte de plaque d'immatriculation des images fixes mise en oeuvre au titre de la CISAC par une vingtaine d'autorités d'immatriculation, parmi lesquelles figure, pour la France, la SACD qui a enregistré environ 10 000 images d'agences par dépôt en ligne. Un projet similaire existe concernant les oeuvres écrites : il s'agit du projet ISTC (International Standard Text Code) lancé par selon la CISAC et les organisations d'éditeurs littéraires.

L'élaboration de bases de données numériques, en second lieu, se poursuit. Peuvent être citées l'IPI (Interested Parties Information), qui élargit à tous les répertoires la base des données des ayants droit des oeuvres musicales ; l'IDA, (International Database on Audiovisual) sur les oeuvres audiovisuelles, commune à 15 sociétés dont la SACD française ; AVINDEX, base sur les oeuvres audiovisuelles des sociétés gérant la musique ; WID (World Identification Database) base en ligne centralisant toutes les données sur les œuvres musicales ; SCRI (Sound Carriers and Recording information), projet de base relative aux supports sonores ; les producteurs de phonogrammes (base IFPI) ou d'audiovisuel (base FIAPF-AGICOA) se dotent également de bases de données.
Cette énumération correspond en réalité à un rapprochement progressif d'initiatives sectorielles formant un ensemble impressionnant ayant déjà abouti en matière audiovisuelle et en matière photographique et qui devrait également aboutir pour les oeuvres musicales et écrites.

Ces bases de données, et le tatouage ou marquage des oeuvres permettront sans doute efficacement de situer leur utilisation sur le réseau internet et de prévenir ainsi la plupart des utilisations non autorisées incompatibles avec le respect du droit d'auteur.

#### 3.1.1.2. Le lien indissociable contenu – identifiant et protection

La protection d'un contenu numérique, et la liaison du même contenu numérique avec son identifiant sont deux concepts différents.

##### 3.1.1.2.1. Un lien indissociable.

On a vu que l'identifiant d'un contenu numérique peut être public c'est à dire connu de tous. Il n'a pas besoin de mesures techniques particulières de protection Par contre l'identifiant ne doit pas pouvoir être séparé de l'oeuvre.
Protéger une œuvre, c'est souvent limiter ses accès à des personnes autorisées et ces autorisations peuvent correspondre à un champ d'utilisation plus ou moins vaste. C'est l distributeur qui met en place la protection en exécutant les ordres donnés par un serveur de droits.
Le lien entre une oeuvre et son identifiant ne doit jamais être rompu de telle sorte que la seule lecture d'un identifiant d'une oeuvre puisse permettre à tout moment d'identifier l'oeuvre. Ce lien doit par exemple pouvoir résister à des opérations des opérations codage, décodage, réencodage en passant donc par le domaine analogique.

##### 3.1.1.2.2. Tatouage/Signature

Ces deux techniques vont répondre de façon différente aux objectifs suivants :

– l'objectif de contrôler si l'accès est licite
– l'objectif de contrôler le type d'utilisation, l'identité de l'utilisateur et

l'intégrité .de l'oeuvre

– Tatouage

L'information tatouée dans chaque oeuvre contient son identifiant ou une référence vers une base de données contenant des informations associées à son identifiant .

-Signature.

L'idée est que à partir d'une oeuvre numérique (constituer d'une ensemble de bits) il est possible de trouver un ensemble de bits qui la caractérisent et qui sera appelée sa signature. Une base de données de signature peut alors être constituée à partir du lien signature/identifiant. Les modifications apportées à l'oeuvre ne doivent pas modifier de façon trop importante la signature. Ainsi un lecteur d'identifiant peut à partir du contenu de l'oeuvre calculer une signature qui pourra être rapprochée de celle en base de données pour retrouver l'identifiant.

Le titulaire peut ainsi constituer une base de données signatures, associant pour chaque contenu une signature de ce dernier avec son identifiant. Ainsi, tant que l'utilisateur n'apporte pas au contenu de modifications l'altérant de manière significative, toute signature de ce contenu est proche de la signature présente dans la base de signatures, permettant ainsi de retrouver son identifiant. Dans ce cas, le lecteur d'identifiant calcule la signature du contenu, se connecte à la base de données des signatures pour trouver la signature qui est la plus proche de celle obtenue, et est ainsi capable d'identifier l'oeuvre.

Il existe deux catégories de signatures :

*Les signatures statistiques.

Pour toute oeuvre sous format numérique, il est possible de réaliser une analyse du signal numérique associé, par exemple une analyse spectrale en utilisant une transformée de Fourier. Cette analyse permet d'obtenir des données représentatives de l'oeuvre au sens physique d'un signal électrique. À partir de ces données, il est possible de constituer une signature statistique de l'oeuvre.

=*Les signatures sémantiques.

Une signature sémantique est calculée à partir des éléments de l'oeuvre qui créent du sens pour un être humain. Dans le cas de la musique, ces éléments peuvent être par exemple le nombre d'instruments et leur timbre, les mélodies, le tempo, le nombre de couplets,tels rythmes particuliers. Dans le cas d'une image ou d'une vidéo, il peut s'agir de la position relative des coins des objets représentés ou bien de la qualité des contours de certains personnages.

#### 3.1.1.2.3. Comparaison TATOUAGE/SIGNATURE

*robustesse par rapport à un usager normal de l'oeuvre

Ce seront des changements de tailles, la suppression d'une partie ou le passage par l'analogique. Il est difficile de dire si le tatouage ou la signature sont plus robustes. Néanmoins un système à base de signatures doit être finement paramétré pour tenir compte des écarts suite aux modifications.

*robustesse suite à une attaque par un pirate.

Si le pirate, souhaite supprimer l'identifiant attaché à une oeuvre. Un système mettant en oeuvre des signatures est alors plus robuste qu'un système de tatouage. En effet, un tatouage ayant été ajouté à l'oeuvre originale, on peut imaginer qu'un pirate bien informé peut le retirer, même si l'algorithme de tatouage est non-

réversible.

*robustesse suite à une attaque par coalition

Les tatouages sont particulièrement sensibles aux attaques par coalition. Lors d'une attaque par coalition, plusieurs destinataires d'une même oeuvre mélangent leurs versions afin d'obtenir une nouvelle version de l'oeuvre non identifiable En revanche, une signature est particulièrement difficile à falsifier sans altérer l'oeuvre de façon significative. Dans le cas d'une signature sémantique, et même si l'algorithme est connu par les pirates, modifier la signature d'une oeuvre implique une modification du sens de celle-ci, aboutissant en général à une annihilation de sa valeur commerciale.

*En termes de taille maximale du catalogue .

Avec un système par signatures, le temps d'identification d'une oeuvre croît avec le nombre d'oeuvre présentes dans le catalogue, tandis qu'il décroît avec la taille de chaque signature. Par conséquent, plus le catalogue est grand, plus il faut des signatures petites, et moins le système est robuste. Avec un système par tatouage, le temps d'identification ne dépend pas de la taille du catalogue, ce système est donc préférable lorsque le nombre d'oeuvre est très élevé.

*En termes d'antériorité.

Un système par tatouage ne permet d'identifier que les oeuvres qui ont préalablement été tatouées avant leur diffusion. En revanche, un système par signatures permet d'identifier toutes les oeuvre dont on possède une copie, même celles qui ont déjà été diffusées.

Le rapport robustesse/usage est en réalité très déterminant dans le choix des techniques, ce qui n'en invalide aucune, mais ne permet de constituer une grille de critères pertinents qu'en fonction des applications recherchées.

### 3.1.2. DESCRIPTION PAR DES LANGAGES

Une fois décrit les objets sur lesquels doit porter la description du langage de droit, if faut que le SGND permette l'établissement d'un dialogue entre les ayants droits et les distributeurs. C'est le but d'un langage de description des droits.

Il constitue une sorte de grammaire nécessaire pour parvenir à décrire les droits associés à chaque oeuvre, pour chaque utilisateur, et ainsi, former la « langue » des DRMS. Un langage de description des droits permet de décrire numériquement les droits sur une oeuvre sous format numérique (texte, oeuvre musicale, image fixe ou animée, vidéo, jeu vidéo, etc.).

Il s'agira d'un langage normalisé suffisamment précis pour décrire toutes les cas d'utilisation d'œuvre et aussi pour ouvert pour s'adapter à l'expression d'autres besoins. Afin de satisfaire les conditions d'interopérabilité, il devra portable entre les divers systèmes d'exploitation.

Ses fonctions lui permettront l'identification et l'authentification des personnes et des ressources, la signature et le chiffrement

#### 3.1.2.1.1. Les langages existants

– ODRL (Open Digital Rights Language).

Il est né de la fusion entre le langage XMLC (Extensible Media Commerce Language) de Real Networks et du language MRV de Nokia.

– XrML (eXtensible rights Markup Language).

C'est le nouveau nom du langage DPRL (*Digital Property Rights Language*) issus des travaux du *Xerox Palo Alto Research Center* (Xerox-PARC) et dont les brevets sont détenus désormais par *Contentguard* dont *Microsoft* est actionnaire.

##### 3.1.2.1.2. Exemple de d'utilisation du langage

Grâce à un langage de description des droits,, il est possible de décrire, par exemple, les licences suivantes :

– Achat d'un livre électronique : un utilisateur paie un ticket d'entrée, après quoi il peut consulter aussi souvent qu'il le désire le livre électronique, sans toutefois pouvoir le copier ou l'imprimer ;

– Pay per view : Un utilisateur peut consulter un livre électronique, mais il doit payer une somme fixe à chaque fois. Un utilisateur peut regarder un film sur un service de films à la demande, mais il doit pour cela payer une somme fixe à chaque fois ;

– Prêt d'un livre électronique : après avoir acheté un livre électronique, un utilisateur peut prêter ce livre à une tierce personne pour une durée déterminée. À l'expiration de la durée, l'utilisateur retrouve automatiquement l'usage du livre tandis que la tierce personne n'y a plus accès.

– Copie privée : 1 fois. Après avoir acheté le droit de consulter une oeuvre, l'utilisateur peut réaliser une et seulement une copie numérique parfaite de cette oeuvre

### 3.1.3. .ARCHITECTURES TECHNIQUES DES *DRMS* ET DES *PRMS*.

La distribution numérique sécurisée d'oeuvres et de droits implique la mise en oeuvre d'une gestion des différentes bases de données relatives aux oeuvres, aux droits licités, aux clients et à leurs utilisations. Cette gestion porte principalement sur la conformité des droits aux utilisations pour garantir l'adéquation de celles-ci aux rémunérations.

#### 3.1.3.1. Lien avec la base de données clients.

Dans le contexte où les oeuvres et la représentation des droits sur ces oeuvres sont véhiculées séparément, on peut concevoir un système où les oeuvres circulent librement sous forme chiffrée, mais où l'envoi de la représentation de la distribution des droits est soumis aux règles d'un contrat. Les règles du contrat, pouvant inclure des dispositions financières, sont décrites par un langage de description des droits. La mise en oeuvre de ce langage permet de délivrer aux utilisateurs des « concessions », c'est-à-dire des ensembles de droits sur des oeuvres.

La délivrance des concessions est généralement centralisée au niveau d'un serveur informatique, appelé « serveur de droits ». Ce serveur est la propriété du titulaire de droit, le cas échéant, par délégation ou redondance du distributeur. Le serveur de droit doit être situé dans un environnement de confiance à la fois physiquement (bâtiment sécurisé,

accès restreint au local) et virtuellement (la connexion entre le serveur et les utilisateurs est sécurisée, de telle sorte que les utilisateurs ne puissent pas pénétrer sur le serveur pour y faire des opérations illégales). Les technologies de sécurisation d'un serveur disponibles aujourd'hui sont très robustes.

Le serveur reçoit en entrée de la part des titulaires de droits, l'ensemble des licences définies, avec un langage de description des droits, de façon générique pour chaque oeuvre ; il reçoit de la part des utilisateurs, des requêtes de concessions, éventuellement accompagnée d'un paiement. Il émet en sortie, vers les titulaires de droits, le nombre de requêtes pour chaque oeuvre et le total des sommes perçues correspondantes, et, vers les utilisateurs, des concessions. Deux scénarios d'exploitation sont possibles : Les licences définies par les titulaires de droits ne sont pas nominatives. Elles sont du type : « telle oeuvre peut être achetée au prix de 20 , sa location pour un jour coûte 5 €, etc. ». De même, les bilans envoyés aux titulaires de droits sont consolidés pour chaque oeuvre, ne précisant pas le nom des personnes ayant acheté telle ou telle oeuvre . Un tel scénario garantit une protection maximale des données personnelles.
– Les titulaires de droits souhaitent personnaliser les licences, par exemple définir des catégories de consommateurs qui bénéficient d'un régime spécial. Dans ce cas les licences sont nominatives, mais cela n'implique pas que les bilans envoyés par le serveur aux titulaires de droits le soient aussi. On peut imaginer que le serveur de droits ne retourne que les recettes générées par chaque oeuvre, ou bien les dépenses effectuées par chaque utilisateur, sans que les titulaires de droits aient la possibilité de savoir exactement les utilisations de telle oeuvre par tel utilisateur. Il serait possible qu'une autorité indépendante certifie techniquement le niveau de protection des données personnelles associé à un serveur de droits, et à son interface avec la base de données clients d'un titulaire de droit.

Dans les deux cas, le serveur de droits pose des questions du point de vue du respect du droit de la protection de la vie privée. Cette question est techniquement posée par l'articulation entre les DRMS et les PRMS (Privacy Rights Management Systems) qui constitue un sujet assez neuf, mais majeur pour le développement des DRMS. L'essentiel de la problématique de la relation entre les DRMS et PRMS, chargés l'un comme l'autre de garantir des valeurs (données personnelles / distribution de contenus numériques) consiste à rendre leurs architectures compatibles sans avoir à partager leurs « secrets » respectifs. Si cette articulation est mieux maîtrisée pour les usages du commerce électronique et le respect des droits des consommateurs comme des données personnelles, elle pourrait apparaître plus problématique s'agissant de « contenus numériques », essentiellement parce que leur distribution numérique notamment sur les réseaux relève de la « communication audiovisuelle » au sens de la loi et engage donc le respect du « secret des choix des personnes ».

#### 3.1.3.2. Analyse des technologies existantes ou à l'état de projet.

Le risque de conflit entre les *DRMS* et la protection des données personnelles est fonction du degré de centralisation des remontées d'informations nominatives. Les *DRMS* fondés sur une implémentation « matérielle » des mesures techniques attirent davantage l'attention sur ce risque dans la mesure où il serait plus difficile aux utilisateurs de procéder au contournement des mesures techniques et *DRMS* en cas d'atteinte à leur vie privée ou de limitation des fonctions d'anonymisation.
Mais des règles de fonctionnement simples et contrôlables permettent d'assurer techniquement le respect du droit.

##### 3.1.3.2.1. Les systèmes centralisés

Les systèmes décentralisés, ne possèdent pas, par définition, de base de données des utilisateurs et excluent par conséquent tout risque de constitution d'un fichier nominatif. Toutefois, il faut distinguer les situations possibles :
Les systèmes sans remontée de données personnelles. C'est le cas du système Smartright qui ne vise qu'à protéger la copie des contenus, et non l'accès. Les cartes à puce servant à l'authentification sont mises en place en série lors de la fabrication des téléviseurs, et puisque ceux-ci sont vendus de façon anonyme, il n'est pas possible de relier un numéro de carte à puce avec un nom d'utilisateur. Par la suite, le système Smartright fonctionne sans voie de retour. Les données sur l'utilisation des oeuvres remontent jusqu'à la carte puce située au sein de chaque téléviseur, mais ne sont pas acheminées hors du foyer.

Les systèmes matériels avec remontée éventuelle de données personnelles Le projet TCPA (Trusted Computing Platform Alliance) est une alliance industrielle regroupant depuis 1999 Microsoft, Intel, IBM, Compaq, et HP pour chercher à doter les ordinateurs personnels de fonctionnalités de sécurité : authentification, intégrité, respect de la vie privée, notamment pour des applications de B2B ou d'administrations électroniques.
(voir annexe TCPA)

##### 3.1.3.2.2. Les systèmes partiellement centralisés

Les systèmes de gestion numérique des droits et virtuellement centralisés aujourd'hui existants réalisent une consolidation des achats au niveau des consommateurs ou bien à un niveau intermédiaire, mais pas au niveau du serveur central. Par conséquent, mis à part l'utilisateur lui-même, personne dans la gestion numérique des droits ne peut avoir accès à la connaissance des actes de consommation effectués par tel ou tel utilisateur des oeuvres ainsi distribués et contrôlés. Au-delà du graphique suivant, quelques exemples peuvent être précisés :
– Les services de films à la demande sur les réseaux de télévision par câble ou par satellite. La consolidation se fait au niveau du décodeur. Un consommateur doit préalablement acheter des jetons, le serveur central enregistre alors le nombre de jetons achetés pour chaque

utilisateur. Le nombre de jetons est stocké dans chaque foyer au niveau de la carte à puce insérée dans le décodeur. Lorsqu'un achat de programme a lieu, sans aucune répercussion sur le serveur central, le nombre de jetons est décrémenté au sein de la carte à puce.

– Les réseaux de télévision par ADSL en cours d'édification, qui permettront la mise à disposition de services à la demande sur les téléviseurs reliés à une prise téléphonique par un décodeur spécifique, prévoient une consolidation à un niveau intermédiaire du détail des consommations . Chaque DSLAM pilote les flux audiovisuels envoyés à chaque foyer en fonction des requêtes envoyées par les décodeurs situés dans les foyers, et des informations sur les clients envoyées par le serveur central.

Les opérateurs envisagent de consolider au niveau de chaque DSLAM les consommations effectuées par chaque utilisateur. Une telle option est dans leur intérêt dans la mesure où le protocole de communication n'est pas le même entre d'une part les décodeurs et les DSLAM, et d'autre part, entre les DSLAM et le serveur central. Faire remonter des informations relatives à chaque consommation jusqu'au serveur central serait pour les opérateurs une stratégie coûteuse en termes de bande passante sur les liaisons de dessertes, sur le backbone, et au niveau du serveur central.

#### 3.1.3.2.3. Les systèmes matériels potentiellement centralisés.

Les systèmes centralisés sont très répandus en ce qui concerne la protection des oeuvres diffusées sur internet. Ils devraient donc faire l'objet d'un maximum de vigilance, conformément aux principes énoncés plus haut . On notera d'ailleurs que les systèmes de peer to peer sur internet posent des problèmes similaires.

## 3.2. LA DISTRIBUTION SECURISEE DES ŒUVRES ET DES DROITS

En amont, un SGND consiste à intégrer les contenus numériques cryptés et à définir numériquement les droits (identification, description), les contenus numériques et les informations sur les droits étant traités séparément

La distribution des droits consiste à mettre à la disposition des utilisateurs les contenus numériques et leurs droits.

### 3.2.1. LES MODES DE DISTRIBUTION

Les deux mode de distribution des contenus sont les réseaux de télécommunications ou les supports optiques.

La distribution sur les réseaux concerne le réseau hertzien, mais aussi du satellite, du câble, et du réseau Internet. Dans chacun des cas, la distribution des informations se fait par des voies non sécurisées quant aux contenus transmis. La distribution sécurisée des contenus se fera sous la forme de données cryptées. Celles ci peuvent donc circuler librement sur les réseaux de télécommunications.

La distribution sur supports optiques (CD Audio, DVD, DVD, SACD) offre

un niveau de sécurisation des contenus numériques très variable. Si un système anti-copie a été implémenté dès la conception du système, ce qui est rare, le système peut offrir un bon niveau de sécurité pour un utilisateur moyen.. Choisir entre un mode de distribution par réseau ou par supports optiques se fera en fonction des impératifs de sécurité mais aussi du coût de la bande passante, le mode de consommation de l'oeuvre, et le parc de matériels installés des utilisateurs.

#### 3.2.1.1. La distribution sur réseau de télécommunications.

Le principal avantage de ce mode de distribution est sa capacité à permettre un certain degré d'interactivité avec l'utilisateur. L'interactivité permet au distributeur de sélectionner son type de transmission: diffusion en continu d'une oeuvre sur un canal donné, transmission à la demande d'une oeuvre sur un canal donné, ou encore circulation à la demande des oeuvres entre les utilisateurs. Deux grandes catégories de réseaux : les réseaux fermés (par exemple pour les services audiovisuels accessibles par câble, satellite, ADSL) et le réseau Internet (où l'établissement d'un service est libre).

##### 3.2.1.1.1. Le réseau fermé de télécommunication

Ce sont par exemple les réseaux hertziens terrestres et satellitaires,ou les réseaux câblés, Dans chaque cas, l'utilisateur a besoin, pour se connecter au réseau, d'utiliser un terminal spécifique qui prolonge le réseau fermé. L'ensemble du terminal peut être fermé et propriétaire (cas d'une console *Xbox* par exemple), ou bien simplement une carte à puce insérée dans un terminal standardisé (cas d'un terminal GSM par exemple).

Les mesures techniques de protection sont généralement un décodeur muni d'une carte à puce. En Europe, le système de chiffrement des oeuvres est celui de DVB.

Si l'utilisateur ne paye pas, , un nouveau message crypté est envoyé au décodeur pour supprimer les accès de l'utisateur.

L'algorithme du DVB implémenté sou forme matériel, est très robuste puisque, après plus de dix années d'exploitation, il n'a toujours pas été cassé. La distribution sur supports optiques.

#### 3.2.1.2. Distribution sur support optique

##### 3.2.1.2.1. Distribution sur support optique d'oeuvres musicales.

L'essentiel du piratage numérique dans le domaine musical tient à l'absence native de mesures techniques de protection appliquées aux CD Audio, notamment par comparaison au format du DVD qui comporte la mesure technique de protection qu'est le CSS (*Content Scrambling System*). Le lancement de nouveaux supports audio numériques peut être l'occasion de combler cette différence entre le secteur de l'audio et du cinéma. Cependant, si le standard DVD devait s'imposer pour le cinéma comme pour l'audio, il n'est pas certain que cet écart demeure. En pratique, cela signifierait que la copie numérique audio resterait aisée, tandis que la copie numérique d'oeuvres audiovisuelles et cinématographiques resterait –principalement et techniquement – très limitée voire impossible.

#### 3.2.1.2.2. Distribution sur support optique des oeuvres audiovisuelles.

Le standard DVD a été créé en 1995 par le consortium DVD qui regroupe 10 Entreprises. Les principales protections prévues par la norme DVD sont les suivantes :
– Le « système *Macrovision* », qui fait en sorte que le signal vidéo analogique émis par un lecteur DVD ne soit pas enregistrable sur une cassette VHS ;
– Le système de protection CSS (*Content Scrambling System*) qui consiste à chiffrer les données.

Aujourd'hui il est possible de télécharger sur Internet des « *rippers* » de DVD, c'est-à-dire des logiciels capables de déchiffrer un DVD et d'inscrire en clair le contenu de l'oeuvre sur un autre support.

### 3.2.2. LA RECONNAISSANCE DES CONTENUS ET LA REQUETE DES DROITS

Quel que soit le mode de distribution mis en oeuvre, réseau de télécommunications électroniques ou support optique, s'il existe un système de protection, l'utilisateur dispose sur son équipement de l'oeuvre sous forme chiffrée. Pour exploiter l'oeuvre, l'utilisateur doit acquérir les droits correspondants auprès d'une autorité certifiée par les titulaires de droits pour délivrer ceux-ci. Dans le cadre d'un système numérique de gestion de droits, cette autorité se matérialise généralement sous la forme d'un serveur de distribution des droits.

La requête formulée par l'utilisateur au serveur de droits doit inclure un identifiant de l'oeuvre, afin que le serveur puisse lui fournir la clef qui correspond bien à l'oeuvre. Cela suppose que le programme réalisant la requête sache reconnaître une oeuvre sous sa forme chiffrée, qu'il connaisse l'adresse d'un serveur autorisé à donner ces droits, et qu'il utilise le même vocabulaire que ce serveur pour décrire les oeuvres. Plus précisément ils doivent partager les mêmes langages de description des oeuvres et des droits.
Outre des identifiants de l'oeuvre et de la nature des droits demandés, la requête doit comporter un identifiant de l'utilisateur, et une authentification de l'utilisateur, c'est-à-dire une preuve que l'identité présentée par l'utilisateur est bien conforme à la réalité.

### 3.2.3. LA SECURISATION DE LA DISTRIBUTION DES DROITS.

La distribution des droits suppose un processus d'authentification des utilisateurs et un processus de chiffrement des droits.

#### 3.2.3.1.1. L'authentification.

En termes de robustesse, ces deux opérations successives, ne sont pas indifférentes à la solution (logicielle ou matérielle) de l'implémentation du secret et de l'interface. La distribution de droits sur une oeuvre implique une identification de l'utilisateur, par exemple pour mettre à jour les bases de données des droits ou commerciales, personnaliser la représentation numérique des droits, etc. Elle est doublée d'une authentification, pour éviter des usurpations d'identité.

L'identification se fait simplement grâce à un langage de description des personnes, que doivent partager l'utilisateur et le serveur de droits.

L'authentification est une mesure technique de protection. Elle repose en général sur un système de clefs publiques et privées. L'utilisateur possède chez lui un secret, sous forme de clef privée, qui lui est propre et connu seulement de son processus technique d'identification. Cela signifie qu'il existe chez l'utilisateur un secret qui n'est connu par aucune autre personne. Ce secret est accessible par le processus technique d'authentification de l'utilisateur, mais pas directement par l'utilisateur, afin de garantir que l'utilisateur ne partage pas le secret avec une autre personne en vue de partager ses droits avec elle .À partir de la clef privée, le processus technique d'authentification de l'utilisateur peut établir un dialogue avec le serveur de droits, en échangeant des clefs publiques. Par ce dialogue, le serveur de droits peut vérifier si l'utilisateur possède bien le secret qui prouve son identité.

La protection dans cette phase d'authentification est fondée sur la relation technique qui s'établit entre un secret pour chaque utilisateur (généralement une clef privée) et un processus technique d'authentification qui réalise l'interface entre un utilisateur, c'est-à-dire le secret authentifiant cet utilisateur et le serveur de droits.

Le processus technique d'authentification doit répondre aux exigences suivantes : le secret ne peut être divulgué à personne, pas même à l'utilisateur, et le processus technique d'authentification doit pouvoir, à la demande de l'utilisateur, établir avec le serveur de droits un dialogue authentifiant l'utilisateur.

Il existe deux grandes catégories de systèmes d'authentification, en fonction de la représentation du secret associé à chaque utilisateur. La représentation de ce secret peut être matérielle (située par exemple, dans une carte à puce ou une puce électronique) ou bien logicielle (située par exemple, la dans la mémoire vive ou le disque dur d'un ordinateur).

#### *3.2.3.1.1.1. Authentificateur matériel*

Le cas typique est celui d'une carte à puce, détenue par l'utilisateur. L'utilisateur peut transporter cette carte à puce avec lui, et l'insérer dans un lecteur avec de s'authentifier. En revanche, il ne peut pas lire lui-même le contenu de la carte à puce, ni la reproduire. C'est la solution qui a été retenue pour la plupart des systèmes de télévision à péage, où une carte à puce est insérée dans le décodeur. Des cartes à puce sont également utilisées dans les systèmes Smartright et- Medialive. Enfin, les réseaux mobiles de télécommunications mettent également en oeuvre des cartes à puce, par exemple les cartes SIM dans le système GSM. L'authentifiant matériel peut également prendre la forme d'un circuit intégré, comme par exemple dans le projet d'architecture TCPA. Par rapport aux authentifiants logiciels, les cartes à puce présentent l'inconvénient de présenter des puissances de calcul inférieures.

Toutefois, contrairement au déchiffrement d'une oeuvre par exemple, l'opération d'authentification est légère et peu consommatrice des ressources.

#### *3.2.3.1.1.2. Authentificateur logiciel*

Dans ce cas, le secret est le plus souvent généré de façon aléatoire, puis est stocké dans une mémoire informatique, mémoire vive ou disque dur par exemple.

*** *Robustesse***

L'attaque a pour but de rendre accessible le secret afin de le reproduire. Elle consiste à comprendre le fonctionnement du processus technique d'authentification, puis à l'observer pas à pas afin d'intercepter le secret. Que l'authentification soit matérielle ou logicielle, l'attaque consiste donc à opérer une « rétro-conception » du processus

technique d'authentification. Une rétro-conception (reverse engineering) logicielle est une opération complexe, hors de portée de la quasi-totalité des utilisateurs. Toutefois, elle est aisément réalisable par un pirate puisqu'il existe des outils de « débugage » et de décompilation. Celle -ci est autorisée à des fins d'interopérabilité. Les concepteurs de solutions logicielles d'authentification mettent en place des « anti-débugueurs » capables de vérifier l'intégrité de l'exécution d'un programme. Face aux outils de décompilation, il n'existe pas de solution autre que de concevoir un système très complexe, dont le pirate mettra beaucoup de temps à comprendre le fonctionnement.

De manière générale, lorsqu'une mesure technique est purement logicielle, l'utilisateur qui a le contrôle de son matériel et de son environnement, se voit ouvrir un large champ d'attaques possibles. La question pertinente porte alors sur le caractère dissuasif du temps nécessaire à la mise en cause de la robustesse de la mesure technique. En revanche, un système d'authentification matériel est beaucoup plus robuste aux tentatives de rétro-conception. Pénétrer à l'intérieur d'une carte à puce ou d'un circuit intégré est une opération extrêmement complexe en raison de la miniaturisation de ces matériels. Cette opération ne peut en aucun cas être réalisée de manière artisanale par un pirate, et il n'existe pas d'outil bon marché permettant de la faciliter. Il existe des techniques de retro-conception des systèmes matériels, reposant par exemple sur des procédés de radiographie, mais elles nécessitent des moyens financiers très élevés. De plus, il est beaucoup plus difficile de réaliser une attaque sans laisser de traces lorsque la mesure technique est de nature matérielle, par conséquent la menace de poursuites judiciaires a un plus grand pouvoir de dissuasion.

#### 3.2.3.1.2. Le chiffrement de la distribution des droits.

Après que la requête authentifiée a été envoyée au serveur de droits, celui-ci consulte la base de données des droits ou la base de données commerciale, puis retourne une représentation de ces droits à l'utilisateur. Ces droits autorisent cet utilisateur à exploiter certains des droits de l'oeuvre. Il s'agit en général d'une clef synthétique qui dépend des droits, de l'oeuvre, de l'utilisateur, afin de garantir que la clef ne pourra pas être utilisée pour d'autres droits, d'autres oeuvres ou d'autres utilisateurs. Il est indispensable que la transmission de cette clef soit chiffrée afin que ces trois paramètres ne puissent pas être modifiés, y compris par l'utilisateur destinataire de cette clef. Même si le serveur de droits est parfaitement sécurisé, le chiffrement de cette transmission suppose qu'il existe : un secret détenu par l'utilisateur mais auquel il n'a pas accès en lecture : une interface sécurisée entre ce secret, le serveur de droits, l'utilisateur, et l'oeuvre.

La problématique est donc exactement la même que dans le cas de l'authentification. L'implémentation du secret et de l'interface peut être soit matérielle, soit logicielle, avec les mêmes caractéristiques que l'authentification en termes de robustesse. Il se peut tout à fait que le secret utilisé pour l'authentification et le secret utilisé pour le chiffrement de la distribution des droits soient le même. Si l'inviolabilité du secret placé chez l'utilisateur est assurée, le chiffrement de la distribution des droits n'est pas vulnérable. Il met généralement en oeuvre un algorithme asymétrique, les attaques sur ce dernier seront inopérantes. Le maillon le moins robuste d'un système de gestion numérique des droits est la protection du secret placé chez l'utilisateur.

## 3.3. L'EXPLOITATION DES DROITS

Le contrôle de l'exploitation des droits se subdivise en deux grandes

catégories qui répondent à des problématiques différentes et donnent lieu à des solutions complémentaires de protection technique : le contrôle de l'accès aux oeuvres, le contrôle de la copie des oeuvres.

### 3.3.1. LE CONTROLE DE L'ACCES A L'OEUVRE.

Dès lors que l'utilisateur dispose sur son matériel d'une oeuvre, et d'une représentation de ses droits sur cette oeuvre, le système de gestion numérique des droits doit lui permettre d'accéder à l'oeuvre sous une forme intelligible. Cet accès passe par une opération de déchiffrement.

#### 3.3.1.1.1. L'opération de déchiffrement.

Un décodeur, ou une interface d'exploitation des droits, placé chez l'utilisateur, confronte une oeuvre chiffrée, la représentation des droits de l'utilisateur, et l'authentification de l'utilisateur. Si l'utilisateur possède les droits adéquats, le module de déchiffrement du décodeur procède au décryptage de l'oeuvre, la rendant ainsi compréhensible par le lecteur proprement dit, c'est-à-dire le module du décodeur chargé de mettre l'oeuvre sous une forme analogique intelligible à l'utilisateur.
Si le déchiffreur est matériel, il s'agit simplement d'un circuit intégré . Celui-ci reçoit, en entrée, les signaux numériques représentant l'oeuvre sous forme chiffrée, la représentation des droits de l'utilisateur sur cette oeuvre et la clef privée du décodeur. En sortie, il génère les signaux numériques représentant l'oeuvre sous forme non chiffrée. La représentation des droits et la clef privée peuvent être stockées sur une carte à puce insérée dans un lecteur de carte à puce intégré au décodeur. Il se peut également que la représentation des droits et la clef privée soient stockées eux aussi dans un circuit intégré, éventuellement le même que celui qui contient la fonction de déchiffrement.

Dans le cas où le déchiffreur est logiciel, on retrouve les mêmes modules, mais implémentés de façon logicielle. Le déchiffreur est représenté par une suite d'instructions stockée dans la mémoire de l'ordinateur, et qui seront exécutées par le processeur. La représentation des droits et la clef privée sont stockées dans la mémoire de l'ordinateur. La clef privée joue un rôle similaire dans les fonctions d'authentification et de déchiffrement. Les contraintes de sécurité pour la représentation des droits sont similaires : celle-ci est plus en sécurité dans une carte à puce ou dans un circuit intégré que dans la mémoire vive d'un ordinateur, à condition naturellement que ni la clef, ni la représentation des droits, ne circulent sans protection sur un bus de données.

Quant à la sécurité du déchiffreur proprement dit, il est beaucoup plus difficile de radiographier un circuit intégré que de lire une suite d'instructions dans la mémoire d'un ordinateur. Ensuite, la rétro-compilation est une opération difficile dans les deux cas de figure, mais il existe des outils de rétro-compilation logicielle, contrairement au cas de la rétro-compilation matérielle.

## 3.3.2. LE CONTROLE DE LA COPIE NUMERIQUE DE L'OEUVRE.

Parmi les nombreuses techniques de contrôle, nous examinerons seulement celles qui permettent de suivre le cheminement de l'oeuvre à travers le réseau par le marquage.

### 3.3.2.1. La traçabilité de l'oeuvre numérique.

S'il existe des moyens de contrôler techniquement la copie des oeuvres, certaines configurations techniques rendent impossible l'exercice de ce contrôle, notamment en raison du « trou analogique » Des mesures techniques de protection de suivi de la copie privée numérique sont développées, pas nécessairement pour garantir les droits exclusifs des titulaires de droits, mais pour faciliter l'établissement de preuve en matière
de contrefaçon.

#### 3.3.2.1.1. Le contrôle des copies

Le suivi du contrôle de la copie d'une oeuvre consiste à marquer cette oeuvre, à l'aide d'un tatouage , chaque fois qu'une copie (ou le cas échéant qu'un passage vers l'analogique est réalisé). les tatouages présentent en effet la particularité de pouvoir résister à toutes sortes de traitement de l'oeuvre (y compris un passage vers l'analogique). De plus, il est possible de superposer différents tatouages sur une même oeuvre, lors des différentes étapes de sa diffusion par exemple.

Si une oeuvre ainsi tatouée est diffusée par des pirates professionnels, ou circule sur des réseaux d'échange, il sera possible aux titulaires de droits de remonter la filière de contrefaçon. Ce système repose sur le principe que le lecteur de tatouage ne soit pas public. Ainsi, des pirates n'ont aucun moyen de savoir si le tatouage présent sur une oeuvre a été efficacement « lessivé ». Même s'ils ont mis en oeuvre des techniques d'effacement de tatouages, en diffusant une oeuvre à grande échelle ils prennent le risque d'être identifiés dans le cadre d'une enquête judiciaire.

Par exemple, lors de la distribution en ligne d'une oeuvre, le transport se faisant de manière point-à-point il est possible de tatouer l'oeuvre en y inscrivant un identifiant du destinataire. Ainsi, il est possible de suivre le parcours de chaque copie adressée à chaque utilisateur.

*Le contrôle de diffusion cinématographique.

Dans le cas du cinéma, il est de même possible de tatouer sur le film un identifiant de la salle de cinéma, voire même la date et l'heure de projection. Si un exploitant de salle de cinéma laisse un spectateur filmer l'oeuvre avec un caméscope, et que ce spectateur diffuse l'oeuvre sur un réseau d'échange, alors l'identité de l'exploitant pourra être révélée dans le cadre d'une enquête judiciaire ou simplement constatée dans le cadre des compétences des agents assermentés.

*Le contrôle de diffusion audiovisuelle.

Dans le cas de la vente de programmes audiovisuels à des chaînes de télévision, il est techniquement difficile de détecter si toutes les chaînes de télévision ont réellement payé les droits pour les oeuvres qu'elles diffusent. L'emploi des techniques d'identification, telles que la signature ou le tatouage, permet d'automatiser cette opération. Le traitement d'une image par un système de signature peut en théorie donner lieu à deux types d'erreurs : une fausse alerte : le système croit reconnaître une

image qui n'est pas dans la base, un manquement : le système ne reconnaît pas une image qui est dans la base.

Le système développé par l'INA (Institut National de l'Audiovisuel) est particulièrement performant, au sens où il génère très peu d'erreurs de ce type. Il est particulièrement robuste aux modifications des images. Ainsi, le système pourra établir une correspondance entre une image qu'on lui présente, et une image de la base, même si l'image présentée a subi des modifications telles que : un changement de contraste et de luminosité, l'ajout de cadres ou de logos, des zooms, des troncatures ou des incrustations.

L'ensemble des modifications propres à la diffusion des oeuvres audiovisuelles, en particulier la transmission par voie hertzienne et le passage en mode analogique, ne perturbe pas le système. De plus, une séquence animée n'a pas besoin d'être particulièrement longue pour que le système sache la reconnaître. Le système développé par l'INA pourrait être utilisé dans un contexte de surveillance de l'ensemble des oeuvres diffusées, dans le but d'établir une liste des oeuvres diffusées, notamment en vue de réclamer le paiement des droits sur ces oeuvres. Le fait que le système puisse reconnaître des oeuvres qui n'ont pas été préalablement marquées, à la différencedes systèmes de tatouage, est un atout essentiel pour une institution comme l'INA.

*La mesure d'audience.

Une autre application du suivi de la copie des oeuvres et la réalisation de mesures d'audience. Il peut s'agir de mesures d'audience sur des oeuvres audiovisuelles, par exemple sur les chaînes de télévision et dans les salles de cinéma, ou sur des oeuvres sonores, diffusées par exemple à la radio, à la télévision ou dans les discothèques. Une mesure d'audience implique une identification des programmes regardés par les utilisateurs. Par exemple, dans le cas de la télévision, cette identification peut être réalisée grâce à des boîtiers situés chez les utilisateurs qui enregistrent les instants auxquels des changements de programmes sont réalisés. De façon classique, les données ainsi recueillies sont ensuite confrontées aux horaires réels de diffusion des programmes. Il est possible de s'affranchir de la coûteuse comparaison avec les horaires réels de diffusion, en général différents des horaires prévus, en identifiant les programmes grâce à une signature ou un tatouage.

### 3.3.3. LES LIMITES DES PROTECTIONS DES OEUVRES NUMERIQUES.

À l'issue de la présentation analytique d'un système numérique de gestion de droits, synthétisant l'ensemble des systèmes, il apparaît que si l'ensemble des éléments concourt à sécuriser toute la chaîne de distribution des contenus, un certain nombre de failles demeurent, soit par principe, soit par choix.

#### 3.3.3.1. La libre copie analogique

Les questions posées par le « monde analogique de l'utilisateur » sont, au regard de la nature et des objectifs d'un système de gestion numérique des droits, relativement accessoires du point de vue de la sécurité des contenus numériques. Or, dans tous les

cas, la lecture de l'oeuvre suppose que l'oeuvre, transmise sous forme numérique, soit convertie sous forme analogique. En effet, les sens humains sont analogiques et les systèmes de gestion numériques des droits ne peuvent s'appliquer qu'aux oeuvres sous forme numérique .

Cela signifie, qu'entre l'extrémité de la chaîne de gestion numérique des droits, et les sens de l'utilisateur, il existe un espace lors duquel l'oeuvre circule sous forme non protégée : le « trou analogique » qui est aussi un trou de sécurité incompressible et inévitable. Dans la pratique, des moyens techniques très simples permettent d'exploiter ce « trou analogique », comme enregistrer les signaux sonores avec des microphones à la sortie des haut-parleurs d'une chaîne hi-fi, enregistrer un film avec une caméra devant un écran de cinéma, saisir le contenu numérique présent sur l'écran d'un ordinateur, etc.

Des moyens un peu plus complexes existent cependant aussi. Ils consistent par exemple, lorsque c'est possible de brancher des capteurs directement à la sortie d'un décodeur, ou à l'intérieur d'un décodeur, et de traiter les signaux obtenus de manière à supprimer les parasites. Dès lors qu'il est possible d'intercepter les signaux analogiques correspondant à une oeuvre, il est possible d'enregistrer ces signaux, et de reconstituer une forme numérique de l'oeuvre. La re -numérisation d'un signal analogique réalise une reproduction numérique dégradée par rapport au contenu numérique originale, mais indéfiniment reproductible sans dégradation supplémentaire.

Même s'il est impossible techniquement de combler le « trou analogique » de manière parfaite, il est possible d'identifier les moyens les plus utilisés d'exploitation du trou analogique, et de modifier en conséquence les oeuvres de façon à ce que ces moyens soient induits en erreur. Toutefois, les mesures techniques de protection correspondantes sont peu robustes. Pour un consommateur, la valeur d'une oeuvre est la valeur des signaux analogiques qu'il perçoit, en provenance du lecteur dans lequel elle est insérée. Cependant, si une capture puis une re-numérisation de ces signaux analogiques sont réalisées, la copie en résultant a une valeur commerciale inférieure, qui peut varier selon le type de contenu :

*En matière de programmes audiovisuels.

La valeur des copies analogiques est généralement très inférieure. Par exemple, la copie d'un film enregistré dans une salle de cinéma avec un caméscope n'a qu'une valeur commerciale faible. De même, l'enregistrement à la sortie d'un téléviseur d'un film diffusé en numérique par satellite ne fournit qu'une copie de qualité VHS, dont la valeur est inférieure à celle du DVD correspondant.

*En matière d'enregistrement musical.

Concernant les programmes musicaux diffusés à la radio, la situation est la même que pour les programmes audiovisuels. En revanche, il semblerait que les lecteurs CD audio présents sur le marché présentent en sortie des signaux analogiques d'une excellente qualité lorsqu'il n'existe pas — tout simplement — une sortie numérique non protégée, comme c'est le cas sur de nombreuses platines de CD Audio de salon, permettant de reconstituer une copie de l'oeuvre fidèle à l'original. C'est d'ailleurs l'objectif des systèmes de restitution haute fidélité (hi-fi). Il est donc techniquement extrêmement difficile d'empêcher la copie analogique des oeuvres. En revanche, des techniques existent pour savoir quel utilisateur serait impliqué dans la réalisation de cette copie (par exemple l'emploi de watermarking d'oeuvres cinématographiques diffusés en salle). Les techniques utilisables poursuivent principalement des objectifs de dissuasion , ou bien, participent à la constitution de preuves dans le cadre de la lutte

contre la contrefaçon Surtout, l'intérêt économique de développer des techniques de limitation du trou analogique semble assez faible. Enfin, la mise en oeuvre de protection technique de la copie analogique pourrait rencontrer une hostilité des consommateurs sans rapport avec l'intérêt économique recherché, d'autant que les niveaux de dégradation de reproduction sont élevés et que la distinction entre contenu numérique et oeuvre re-numérisée est assez importante et devrait s'accroître. Même si la probabilité que ce genre de technique résiste à une attaque est faible, le contrefacteur ne peut pas vérifier si son attaque a réussi et il court le risque de subir des poursuites judiciaires s'il diffuse des copies illégales.

Après avoir présenté une introduction aux techniques de marquage des oeuvres numériques et les systèmes de DRM qui sont réalisés à partir d'elles, il faut s'interroger sur les conséquences de ces techniques dans l'ordonnancement juridique et plus particulièrement dans celui de la propriété intellectuelle. Traditionnellement la propriété intellectuelle se décompose en propriété littéraire et artistique et la propriété industrielle. La propriété industrielle concerne la protection juridique par des titres tels que le brevet d'invention, les marques et les dessins et modèles. Il est vrai que. de nombreux brevets (environ 200) ont été déposés pour protéger divers procédés de marquage des oeuvres numériques. L 'étude de ces brevets n'est pas l'objet de ce mémoire. Bien plus intéressant est la façon dont les techniques de marquage vont influer le droit de la propriété intellectuelle, le droit se devant toujours de s'adapter à l'évolution de nouvelles techniques.

Dans une première partie seront étudiés les droits que. les techniques de marquage et les systèmes de DRM vont protéger ou consolider (4) pour continuer sur les droits. que. ces techniques menacent(2)

# 4. LES DROITS RENFORCES PAR LE MARQUAGE

La plupart des recherches effectuées sur le marquage des oeuvres numériques depuis ces dix dernières années l'on été au départ à l'initiative des auteurs ou plutôt des sociétés d'auteurs. Mais les états ont très vite trouvé des intérêts dans ces recherches notamment pour pourvoir répertorier l'ensemble des oeuvres. La fonction de police des Etats se doit aussi de réagir contre la contrefaçon qui peut se développer, en particulier sur Internet. Comme nous l'avons déjà vu dans la première partie, le monde numérique est caractérisé par cette incroyable facilité à manipuler les données. On pourrait dire que. dans ce monde « on copie comme on respire ». Le marquage et les systèmes de DRM seront alors une technique protectrice du droit de propriété littéraire et artistique(4.1) et le droit interdit le contournement d'un mesure de protection du droit d'auteur comme le marquage(4.2)

## 4.1. LA PROPRIETE LITTERAIRE ET ARTISTIQUE

Les droits de propriété littéraire et artistique protègent chacun des éléments d'une création numérique (son, images fixes, texte, vidéo..) et chacun des intervenants à la création, à l'interprétation , la distribution et à l'enregistrement de cette création. Ainsi les droits d'auteurs protègent la conception et la réalisation de l'oeuvre. Les droits voisins protègent les auxiliaires de la création, c'est à dire les prestataires tels que les artistes interprètes et producteurs de ces interprétations de l'oeuvre sur un phonogramme (phonogramme désigne tout support de son enregistré) ou un vidéogramme (vidéogramme désigne tout support de vidéo enregistré)

L'oeuvre numérique susceptible de marquage sera ainsi examinée selon les protections accordées par le droit, au titre du droit d'auteur (1.1.1), et au titre des droits voisins (1.1.2).

### 4.1.1. DROITS D'AUTEUR

Historiquement, la première convention internationale relative au droit d'auteur date du 9 octobre 1886, la Convention de Berne signée et ratifiée par plus de 80 pays En droit français, le principe de la protection du droit d'auteur est posé par l'article L.111-1 du Code de la Propriété Intellectuelle (CPI) *: « L'auteur d'une oeuvre de l'esprit jouit sur cette oeuvre, du seul fait de sa création d'un droit de propriété incorporelle exclusif et opposable à tous. Ce droit comporte des attributs d'ordre intellectuel et moral ainsi que des attributs d'ordre patrimonial*

#### 4.1.1.1. conditions de protection du droit d'auteur

Aux termes de l'article L.112-2 du Code de la propriété intellectuelle, la protection légale a vocation à s'appliquer à toutes *les oeuvres de l'esprit quels qu'en soit le genre, la forme d'expression le mérite ou la destination*». Toutefois malgré les termes généraux de la loi, les créations intellectuelles ne sont pas automatiquement protégées par le droit d'auteur, la protection ne bénéficie qu'aux oeuvres de l'esprit

répondant à certains critères.

C'est la jurisprudence et non la loi qui détermine quelles sont les créations intellectuelles protégeables par la loi et que l'on pourra qualifier d'oeuvre. Les deux critères d'appartenance sont l'originalité et la forme

Toute oeuvre de l'esprit doit, pour bénéficier de la protection légale, satisfaire à deux exigences : tout d'abord, l'exigence d'une concrétisation formelle de l'oeuvre qui la rende matériellement perceptible. Ensuite, l'exigence d'une forme originale : l'originalité est la condition nécessaire et suffisante pour bénéficier de la protection du droit d'auteur.

#### 4.1.1.1.1. L'originalité (contraire de la banalité)

L'originalité est l'expression juridique de la créativité de l'auteur, elle est définie comme l'empreinte de sa personnalité. La condition d'originalité est une notion relative. Les juges apprécient le caractère original de l'oeuvre au cas par cas. L'originalité se distingue de la nouveauté qui est entendue objectivement

Classiquement, l'originalité est perçu par les juges

*«comme l'expression de la personnalité de la personne de l'auteur* » (TGI de Paris 27 avril 1942),

* «le *reflet de la personnalité de l'auteur* » (CA Paris 4 mars 1982),

* «*la vision personnelle de l'auteur* » (CA Paris 18 juin 1992)

* «*le ton personnel de l'auteur* » (TGI de Paris 24 mars 1982)

* «*l'empreinte émotionnelle personnelle*»

Il s'agit d'une conception subjective d'un système de droit qui place l'auteur au centre de son intérêt. En effet, deux grands systèmes juridiques existent dans le monde à travers les pays de droit d'auteur (latin: France) et les pays de copyright (anglo-saxons: Royaume-Uni) La conception traditionnelle du droit d'auteur français est de protéger la personnalité de l'auteur qui s'exprime à travers cette oeuvre. Pour cette raison, toute création qui serait créée à partir de la pure logique systématique, et contraignante et où l'auteur n'interviendrait pas suffisamment à travers sa personnalité ne peut être traditionnellement protégée par le droit français contrairement aux droits anglo-saxons. Le rendement, l'efficacité sont normalement absente du droit d'auteur, l'auteur étant plus considéré comme un artiste que comme un exécutant.

Mais la jurisprudence récente des Tribunaux français évolue et la conception traditionnelle et subjective de l'originalité se rapproche d' une logique plus économique afin de protéger l'investissement.. Aujourd'hui le droit d'auteur se rapproche du droit du copyright.

Déjà dés 1924, la cour d'Appel de Paris avait accordé la protection par le droit d'auteur au fameux annuaire Bottin au motif que *Le fait de réunir des données en un ensemble ordonné et complet et de les classer comporte un travail important » et « qu'il ne faut pas perdre de vue qu'il*

*s'agit d'une oeuvre composée à grand frais*». La Cour en déduit que *le résultat de ce travail donne lieu à un droit privatif, véritable droit de propriété.*

Depuis, on ne compte plus les décisions qui ont admis l'originalité de catalogues *(CA Nancy 10 juillet 189*3), de guides d'adresses *(C.Cass 31 mars 199*2), d'un ouvrage dressant le catalogue de certains types de logiciels *(CA Paris 27 mai 199*2), et même de barèmes de prix *(C.Cass 21 mai 197*5).

Un important arrêt PACHOT (C.Cass du 7 mars 1986) définit l'originalité comme « *l'effort personnalisé allant au delà de la simple logique automatique et contraignante, la matérialisation de cet effort résidant dans une structure organisée* ».

Ou encore, de nombreux arrêts accordent la protection par le droit d'auteur à une oeuvre, au motif que l'auteur a fait preuve d'un savoir faire et de persévérance.

En sens contraire, en vertu d'un autre courant de décisions, *« La représentation des articles pour animaux domestiques est d'une originalité limitée* » et *« la disposition des articles offerts à la vente est trop banale pour être protégée* » (CA Paris 4 mai 1982).

Dans le même sens, une décision de la Cour de Cassation le 8 décembre 1987 refuse la protection à des fiches techniques, au motif que « *leur présentation était banale et usuelle* », ou encore qu'elles étaient réalisées « *selon un ordre imposé* » et « *dans une présentation formelle, banale et usuelle* ».

#### 4.1.1.1.2. Le champ d'application

La loi accorde sa protection à toute oeuvre sans distinction *du genre, de la forme d'expression, du mérite ou de la destination* .(Article L.112-1 CPI)

Le titre d'une oeuvre, dès lors qu'il présente un caractère original bénéficie de la même protection que l'oeuvre (Article L112-4 CPI)

La loi du 11 mars 1957 énonce en premier lieu le **droit moral** de l'auteur (Chapitre 2 du titre 1 du CPI) objectif philosophique qui est celui de respecter la personnalité de l'auteur contenue dans son oeuvre Ce n'est qu'en second lieu que la loi consacre les droits patrimoniaux de l'auteur, qui répondent à un objectif économique, qui est celui de permettre à l'auteur de vivre de sa création, par l'attribution d'un monopole, le droit exclusif d'autorisation. Cependant, dans la pratique, les droits patrimoniaux ont pris un ascendant considérable, c'est la raison pour laquelle nous aborderons d'abord les **droits patrimoniaux.**

### 4.1.1.2. LES DROITS PATRIMONIAUX DE L'AUTEUR

En droit français, le droit de reproduction et le droit de représentation forment les droits exclusifs de propriété incorporelle que détient l'auteur sur l'exploitation de son oeuvre « Le droit d'exploitation appartenant à l'auteur comprend le droit de représentation et le droit de reproduction. oeuvre(Article L.122-1 CPI : ) . La propriété matérielle est un droit différent indépendant de la propriété intellectuelle

.Les droits patrimoniaux s'appliquent à tout support et technique de

reproduction et de représentation, l'énumération n'étant pas limitative. Le champ d'application de ces droits est très large. Une utilisation secondaire de l'oeuvre comme la réalisation d'une oeuvre dérivée (adaptation) ou un mode de reproduction et de transmission numérique (numérisation, stockage).nécessitera l'obtention par l'utilisateur de droits patrimoniaux distincts de ceux obtenus pour l'oeuvre initial. De même, une étendue de l'exploitation différente (partielle ou totale) ou une finalité(commerciale ou non commerciale).différente correspondra à des droits différents. Le consentement de l'auteur devra donc être obtenu pour chaque procédé de reproduction et chaque mode de représentation.. Ce n'est donc pas parce qu'un auteur à autoriser l'exploitation de son oeuvre en salle de cinéma qu'il l'a autorisé à la télévision ou sur Internet.

#### 4.1.1.2.1. . Le droit de reproduction

L'article L.122-3 du Code de la propriété intellectuelle dispose que :

*La reproduction consiste dans la fixation matérielle de l'oeuvre par tous procédés qui permettent de la communiquer au public d'une manière indirecte. Elle peut s'effectuer* **notamment** *par imprimerie, dessin, gravure, photographie, moulage, et tout procédé des arts graphiques et plastiques, enregistrement mécanique, cinématographique ou magnétique. (…)*

Une reproduction établit donc un lien entre une oeuvre et un support. C'est notamment le cas lorsque la partition d'une texte littéraire (un écrit) , un dessin imprimés (reproductions dites « graphiques »), ou bien d'un disque (vinyle ou disque compact) ou d'une cassette (reproductions dites « mécaniques »). Pour le professeur Gautier, l'adverbe « notamment » est un moyen d'expression des textes qui permet à la loi de s'adapter au modernisme. Il permet d'envisager des types de création qui n'existaient pas au moment de l'élaboration de la loi.

La reproduction numérique d'une oeuvre analogique, la mise à disposition d'un fichier sur le réseau(peer to peer) ou le téléchargement de fichiers constituent des reproductions Cependant pour que le droit de reproduction ait lieu de s'appliquer, il est nécessaire que ce procédé de reproduction permette *« de la communiquer au public d'une manière indirecte » .*

En matière de droit communautaire, la Commission a présenté le 10 décembre 1997 une proposition de directive relative à l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information qui est venu la directive "droit d'auteur" de 2001.

La déclaration commune sur l'article 1.4 du traité de l'OMPI sur le droit d'auteur, posant le principe que le droit de reproduction s'applique *« pleinement »* dans l'environnement numérique en précisant : *« Il est entendu que le stockage d'une oeuvre protégée sous une forme numérique sur un support électronique constitue une reproduction au sens de l'article 9 de la convention de Berne ».*

La Commission semble prendre en considération la reproduction mise en oeuvre lors d'une diffusion en ligne : *« la définition harmonisée du droit de reproduction couvrira tous les*

*actes pertinents de reproduction directe ou indirecte, provisoire ou permanent, en ligne ou hors ligne, sur support matériel ou immatériel ».*

L'application du droit français en la matière a été éclairé par deux ordonnances du 14 août 1996. Le juge des référés du Tribunal de Grande Instance de Paris a eu à se prononcer dans deux affaires similaires, où étaient mis en cause deux jeunes étudiants ayant mis en ligne, des oeuvres de Michel Sardou (1ère affaire) et de Jacques Brel (2ème affaire). A cette occasion, le juge a autorisé la diffusion d'un communiqué de presse rappelant que : **«** *toute reproduction par numérisation d'oeuvres musicales protégées par le droit d'auteur susceptible d'être mise à la disposition de personnes connectées au réseau Internet doit être autorisée expressément par les titulaires ou cessionnaires des droits* **».**

Finalement l'extension du droit de reproduction à l'environnement numérique est acquise depuis une décision du Conseil du 16 mars 2000(JOCE L 89 du 11 avril 2000) qui approuvent les déclarations communes concernant le traité de l'OMPI sur le droit d'auteur adoptées par la conférence diplomatique le 20 décembre 1996.

*Article 1.4/ Le droit de reproduction énoncé à l'article 9 de la Convention de Berne et les exceptions dont il peut être assorti s'appliquent pleinement dans l'environnement numérique, en particulier à l'utilisation des œuvres sous forme numérique. Il est entendu que le stockage d'une œuvre protégée sur un support électronique constitue une reproduction au sens de l'article 9 de la Convention de Berne*

En application de cette décision la directive du 22 mai 2001 a mis en œuvre ce principe dans son article 2 concernant les reproductions provisoires.

Les Etats membres prévoient le droit exclusif d'autoriser ou d'interdire la reproduction directe ou indirecte, provisoire ou permanente, par quelque moyen et sous quelque forme que ce soit, en tout ou partie.

##### *4.1.1.2.1.1. Limitations du droit de reproduction dans l'environnement numérique*

Le développement du numérique a bouleversé la notion classique de reproduction.

Les nouvelles technologies ont, d'une part, rendu indispensable l'insertion d'une nouvelle exception applicable aux reproductions provisoires.

Alors que les reproductions « classiques » permettent de mettre à la disposition du bénéficiaire l'oeuvre reproduite, dans le monde binaire, certaines reproductions provisoires répondent essentiellement à des impératifs techniques nécessaires à la transmission et à l'exploitation rationnelle de l'oeuvre.

Certains de ces modes de reproduction sont indispensables au fonctionnement des ordinateurs et des réseaux. Ces copies éphémères ou temporaires de données indispensables au fonctionnement rationnel de l'informatique sont:

Le routing consiste pour un routeur (ordinateur gérant un réseau) à acheminer

des données sur une route en optimisant la transmission. Une fois le chemin déterminée, l'ordinateur utilise un protocole pour transmettre les données sous forme de paquets.

Le caching consiste à stocker temporairement sur des disques ou en mémoire, des données pour les rendre rapidement accessible pour un abonné à un réseau ou pour un utilisateur disposant d'un navigateur.

Le browsing consiste à visualiser des données par morceaux en les chargeant et déchargeant en mémoire.

Le streaming est une sorte de browsing entre un client et un serveur distant. Il permet d'écouter ou de visionner un contenu multimédia à la volée, c'est à dire simultanément à son téléchargement..

Ces copies, sont susceptibles de mettre en cause le droit exclusif de reproduction sur les oeuvres ou les objets protégés. C'est pourquoi la directive du 22 main 2001 est intervenue pour concilier ces impératifs techniques et le droit exclusif de reproduction.

L'article 5 § 1 s'applique aux actes de reproduction provisoire. Cependant l'application de l'exception est soumise à plusieurs conditions. Deux d'entre elles apparaissent essentielles, l'une ayant trait à la nature provisoire de la reproduction, l'autre à sa destination.

Concernant la nature provisoire de la reproduction, celle-ci doit être transitoire ou accessoire :

Le terme transitoire semble viser les copies éphémères nécessaires à la transmission des données (ex : routing). Le terme accessoire semble viser quant à lui les stockages temporaires effectués pour des raisons techniques (ex : browsing, streaming, caching client et proxy). Certains parlementaires européens proposaient que la reproduction provisoire soit « accessoire et transitoire » afin d'exclure le caching proxy du champ d'application de l'exception.

Concernant la destination de la reproduction provisoire celle-ci doit avoir pour unique finalité : une « *transmission dans un réseau entre tiers par un intermédiaire* » ou une « *utilisation licite* » d'une oeuvre ou d'un objet protégé.

Cette seconde condition induit un traitement différent selon que la copie provisoire est partie intégrante d'un procédé de transmission ou non.

Dans le premier cas, l'exception s'applique sans considération de la licéité de l'utilisation de l'oeuvre ou l'objet protégé transmis. Ceci a pour but de dégager les intermédiaires techniques, impliqués dans la transmission, de toute responsabilité s'agissant des reproductions provisoires qu'ils effectuent dans le cadre de leur activité.

Cependant le considérant 59 précise que les titulaires de droits pourront demander à un juge qu'il ordonne à l'intermédiaire de mettre fin à une atteinte à leurs droits. On peut en déduire que si une oeuvre est mise en ligne sans l'accord de l'auteur, il pourra exiger que celle-ci soit retirée du cache proxy alors même que l'intermédiaire bénéficie de l'exception de reproduction provisoire.

Le droit de reproduction s'applique aux reproductions « *directe ou indirecte, provisoire ou permanente, par quelque moyen et sous quelque forme que ce soit, en tout ou en partie* ».

Le droit de représentation ou droit de communication au public (dénommé comme tel par de nombreuses législations étrangères, et par le traité de l'OMPI, article 8) est le corollaire indispensable du droit de reproduction pour la protection des oeuvres, puisqu'il sanctionne la communication effective de

l’oeuvre au public.

#### 4.1.1.2.2. Le droit de représentation

L’internet et autres réseaux numériques remettent en cause la notion traditionnelle de droit de communication au public. Premièrement, le fait que des personnes puissent avoir accès individuellement à des contenus, notamment dans le cadre de services à la demande, remet fondamentalement en cause la notion de public. Les internautes ne sont en effet pas réunis dans un même lieu lorsque les oeuvres leur sont communiquées. En outre, contrairement aux communications classiques, le récepteur des oeuvres et prestations joue un rôle actif dans la sélection du contenu et dans le choix du moment de la réception. Or la communication au public est généralement entendue comme le fait de transmettre une oeuvre à un public passif, ou du moins qui n’a pas le choix des oeuvres qu’il entend, public composé de plusieurs personnes dans un même espace.

En conséquence, aussi bien l’OMPI que l’Union Européenne ont inclus dans la définition du droit de communication au public la *« mise à disposition du public de telle manière que chaque membre du public peut y avoir accès de l’endroit et au moment qu’il choisit individuellement ».* Cette définition inclut les actes de communication sur demande, ainsi que tout acte de communication d’oeuvres sur les réseaux.

Le Code de la propriété intellectuelle définit le droit de représentation en son article L.122-2 qui précise : *La représentation consiste dans la communication de l’oeuvre au public par un procédé quelconque, et notamment :*

*1) Par récitation publique, exécution lyrique, représentation dramatique, présentation publique, projection publique et transmission dans un lieu public de l’oeuvre télédiffusée ;*

*2) Par télédiffusion. La télédiffusion s’entend de la diffusion par tout procédé de télécommunications de sons, d’images, de documents, de données et de message de toute nature.*

*Est assimilée à une représentation l’émission d’une oeuvre vers un satellite.*

Le terme « télécommunication » est défini par la loi du 30 septembre 1986 relative à la liberté de communication : *on entend par télécommunication toute transmission, émission ou réception de signes, de signaux, d’écrits, d’images, de sons ou de renseignements de toute nature par fil optique, radio électricité ou autres systèmes électromagnétiques.*

Il résulte de ce qui précède qu’il ne fait aucun doute, en droit français, que le réseau numérique entre dans la définition légale du procédé indirect de communication au public.

Avec l’avènement des réseaux numériques, la question de la pertinence de cette dualité des notions reproduction / représentation se pose inévitablement. En effet, l’internaute n’entre en communication par représentation avec l’oeuvre que si

elle a été préalablement fixée, notamment sur le disque dur de son ordinateur. Une partie de la doctrine aujourd'hui est favorable à l'émergence d'un droit patrimonial unique des auteurs qui serait « le droit d'exploitation numérique »

Cependant le Conseil d'Etat dans une étude intitulée « Internet et les réseaux numériques » indique que l'avantage de la solution française d'une répartition simple en deux prérogatives accordées aux auteurs : le droit de reproduction et le droit de représentation (contrairement aux législations étrangères qui confèrent aux auteurs une grande variété de sous droit : droit de distribution, droit de présentation au public, droit de création des oeuvres dérivées, droit de transmission, etc.) offre une faculté d'adaptation grâce à la jurisprudence. *« On sait bien qu'il est plus facile de faire évoluer une jurisprudence que de modifier la loi. Or nous sommes dans un domaine où la technique évolue très rapidement, ce qui réclame de la souplesse ».* Et ainsi le Conseil d'Etat de conclure *Il ne paraît nullement nécessaire de créer un droit spécifique de transmission numérique, de distribution numérique ou de mise à disposition du public sur le réseau comme cela paraît envisagé dans certains pays comme les Etats-Unis ou le Japon .*

Il apparaît, conformément aux principes du droit d'auteur, que lorsqu'une société entend mettre à la disposition du public des oeuvres musicales (l'attitude active d'émission ne fait aucun doute étant donné qu'un site commercial recherche activement le public par toutes sortes de procédés comme le marketing, la promotion, la publicité, les liens hypertextes,etc.), elle commet un acte d'exploitation qui comprend la reproduction et la représentation des oeuvres et ce, quelque soit le type de service proposé, écoute ou téléchargement.

#### 4.1.1.2.3. Le droit moral

Une autre question qui se pose est celle de savoir comment s'applique ce qu'on appelle le droit moral. Si le commerce électronique du droit d'auteur suppose à l'évidence des droits patrimoniaux, il ne saurait faire abstraction du droit moral. Il s'agit du droit de l'auteur de faire respecter l'intégrité d'une œuvre et d'en revendiquer la paternité même après pleine cession de tous les droits économiques. Des systèmes de DRM bien conçus devraient pouvoir traiter une situation ambiguë et ne pas se contenter de répondre par oui ou par non. Il existe déjà des systèmes perfectionnés qui peuvent aider à protéger le droit moral de deux façons. Premièrement, le système permettant au titulaire du droit et à l'utilisateur de conclure un contrat (avec ou sans intermédiaire), les parties peuvent stipuler que la modification de l'œuvre n'est pas autorisée ou que la paternité doit être reconnue d'une certaine manière. Deuxièmement, les titulaires de droits peuvent imposer des conditions spéciales. Ainsi, un photographe peut ajouter une mention limitant l'utilisation de son œuvre aux entreprises qu'il a décidé. Ainsi il pourra interdire l'exploitation de ses photographies, par exemple à des fabricants de tabac ou de boissons alcoolisées

#### 4.1.1.2.4. La reconnaissance par le copyright d'un droit de distribution numérique

Etudier le droit de distribution séparément du droit de reproduction relève pour le droit d'auteur du contresens, cependant en *copyright* ce droit est autonome et détaillé, c'est ce qui justifie son étude de manière séparée.
La définition du droit de représentation de l'article L. 122-2 du Code de la propriété
intellectuelle peut s'interpréter comme comprenant le droit de distribution.

Quant au *copyright il* consacre spécifiquement ce droit à l'article 17 U.S.C. 106 (3).
*"§ 106.Exclusive rights in copyrighted works Subject to sections 107 through 121, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following:* […]
*(3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lendin*g"
Le droit de distribution est sujet à épuisement, pour le *copyright* il s'agit de la « *first sale doctrine* ». Comme son nom l'indique, ce droit prend fin lors de la première vente mais l'analyse retenue par les juges américains fait échapper les copies numériques à ce régime. Le droit de distribution vise les « *copies* » mot qui, par son double sens, vise à la fois les exemplaires matériels et les copies immatérielles en *copyrigh*t.

#### 4.1.1.2.5. Vers un droit d'accès ?

Le numérique et la nouveauté engendrée ont renouvelé de nombreuses analyses traditionnelles et en ont fait naître de nouvelles. La théorie du droit d'accès repose sur un constat simple, « *tous les actes de perceptions ou de matérialisation d'une copie numérique exige un accès préalable* ».[1]L'ère numérique pourra faire disparaître l'acquisition d'une oeuvre telle que nous la connaissons actuellement. Au droit de propriété corporelle sur l'exemplaire se substituerait la faculté d'avoir un accès possible de manière permanente à l'oeuvre. La possession « *having* » serait remplacée par la jouissance de l'oeuvre « *experiencing* ». La technologie mettra fin à la « *market failure* » [118] et permettra de ne payer que ce que l'on consomme. Pour le professeur Jane Ginsburg, le droit d'accès ne va pas supplanter le *copyright* mais au contraire « *the access right is an integral* part [119] *of copyright* ». Mais il semble que ce droit d'accès ait été perçu en France davantage comme une couche supplémentaire au droit d'auteur. Le droit d'accès envisagé repose essentiellement sur la technique ; l'article 17 USC § 1201 (a) 1 (A) dispose qu'il est interdit de contourner la mesuretechnique qui assure le contrôle de l'accès à l'oeuvre.

## 4.2. LA PROTECTION JURIDIQUE DES MESURES DE PROTECTION

Les copies sauvages sur le net qui ne respectent pas les droits d'auteurs doivent être stoppées par de nouvelles décisions prisent au niveau de la communauté internationale. Le raisonnement est simple. Le droit d'auteur en tant que droit exclusif est menacé par la technique. La technique doit venir au secours dur droit incapable de contrôler le respect de l'œuvre. Mais, comme toutes mesures techniques peut être neutralisées ou contournées, le droit doit interdire ces actes de neutralisation et de contournement. Le droit doit donc protéger "la bonne technique" qui protège le droit d'auteur.

Les techniques de marquage permettent désormais de contribuer à protéger matériellement les oeuvres . Ainsi les auteurs et autres ayant droits disposent d'une protection juridique (voir 1.1 la propriété littéraire et artistique) et d'une protection par la technique (la mesure ou dispositif de protection).

Plus généralement les mesures techniques tels que le marquage, ont pour objet de protéger des droits portant sur les œuvres diffusées numériquement et sont de deux ordres:

- les unes permettent d'identifier les œuvres et éventuellement leurs auteurs, interprètes ou producteurs(l'accès à l'œuvre)
- les autres visent à prévenir tout acte portant atteinte à la propriété intellectuelle, par exemple en effectuant une copie illicite de l'œuvre.(l'accès aux informations sur le régime des droits)

Le premier type de mesures techniques de protection est déjà couramment en exploitation dans de nombreux systèmes alors que le deuxième type est plus récent

Mais certains textes juridiques ont organisés un troisième niveau de protection. (voir directive du 22 mai 2001 transposition des traités OMPI de 1996) contre le contournement de ces mesures de protection. Selon V-L Benabou, la directive compose une valse à trois temps, en premier lieu, elle reprend l'acquis, puis l'enrichit et le modifie, et enfin elle y renvoit.

### 4.2.1. Identification des œuvres numériques

La propriété intellectuelle, comme toute propriété, se traduit par une mémorisation de l'identité de l'objet, assortie de l'identité de son propriétaire. L'objet numérique, souvent présenté comme un « immatériel », est en réalité contenu dans un fichier informatique délimité dans l'espace et dans le temps et pouvant être copié et échangé, en particulier dans un but commercial. Dans l'univers matériel, l'identification n'est pas nouvelle, ainsi de l'immatriculation automobile ou du code-barre.

L'article 12 du traité sur le droit d'auteur de l'OMPI recense les procédures d'identification dans des termes juridiques particulièrement explicité par M.Daniel Lecomt dans *les normes et les standards du multimédia*: « Le fait que l'OMPI interdise de toucher l'identifiant est une garantie pour l'avenir : *sans aucun doute, à échéance de quelques années, il ne sera plus possible de vendre une oeuvre numérique ou sous forme numérique sans que celle-ci soit identifiée et donc immatriculée au sens propre (le matricule étant dans l'oeuvre).* Cette immatriculation ayant été délivrée par une tierce partie de confiance, cela garantit que les données qui ont été fournies pour l'immatriculation sont conservées en sécurité et restent accessibles, sous conditions bien entendu que *(…) l'identification est suffisante et (…) permet d'envisager tout type de traitement automatique*. On voit aussi que sera puni non seulement celui qui a créé un faux document, mais aussi celui qui le revend ou en fait usage, ce qui responsabilise encore plus le gestionnaire de contenu. Cela impose à l'intermédiaire ou au client final de s'assurer de la provenance du matériel qu'il utilise.

Dans le cas d'utilisation de l'aquamarquage, il faudra un avertissement indiquant que l'image est marquée, pour confirmer la conformité aux règles énoncées, mais aussi pour éviter un nouveau marquage, qui pourrait prêter à confusion. En effet, il est prévu d'avoir deux marquages, l'un au niveau de la création (ou de la production, dans le cas d'un produit audiovisuel complexe) et l'autre au niveau de la distribution (identification de l'utilisateur autorisé ou du profil d'utilisateurs autorisés). Ce modèle de protection permet, en cas de découverte d'un objet ne se trouvant pas dans une situation normale d'utilisation, de savoir à qui il appartient, mais aussi à qui il a été livré et qui en était responsable.

Cette protection juridique est défini dans le Traité de l'OMPI sur le droit d'auteur du 20 Décembre 1996 où les notions d'oeuvre, d'utilisateur sont définies. Les articles 10 et 11 suivants traitent les limitations des droits et des mesures de protection.

Article 10

***Limitations et exceptions***

*1) Les Parties contractantes peuvent prévoir, dans leur législation, d'assortir de limitations ou 'exceptions les droits conférés aux auteurs d'oeuvres littéraires et artistiques en vertu du présent traité dans certains cas spéciaux où il n'est pas porté atteinte à l'exploitation normale de l'oeuvre ni causé de préjudice injustifié aux intérêts légitimes de l'auteur.*

*2) En appliquant la Convention de Berne, les Parties contractantes doivent restreindre toutes limitations ou exceptions dont elles assortissent les droits prévus dans ladite convention à certains cas spéciaux où il n'est pas porté atteinte à l'exploitation normale de l'oeuvre ni causé de préjudice injustifié aux intérêts légitimes de l'auteur.*

Article 11

***Obligations relatives aux mesures techniques***

*Les Parties contractantes doivent prévoir une protection juridique appropriée et des sanctions juridiques efficaces contre la neutralisation des mesures techniques efficaces qui sont mises en oeuvre par les auteurs dans le cadre de l'exercice de leurs droits en vertu du présent traité ou de la Convention de Berne et qui restreignent l'accomplissement, à l'égard de leurs oeuvres, d'actes qui ne sont pas autorisés par les auteurs concernés ou permis par la loi.*

L'article 11 (et 12) distingue entre d'une part les mesures visant à limiter l'utilisation de l'œuvre et d'autre part les mesures qui visent à identifier l'œuvre. Avec le marquage stéganographique et le filigrame, l'origine de la copie peut être prouvée même si la marque reste invisible pour l'utilisateur.

Article 16

*Limitations et exceptions*

*(1) Les Parties contractantes ont la faculté de prévoir dans leur législation nationale, en ce qui concerne la protection des artistes interprètes ou exécutants et des producteurs de phonogrammes, des limitations ou exceptions de même nature que celles qui y sont prévues en ce qui concerne la protection du droit d'auteur sur les _oeuvres littéraires et artistiques.*

*(2) Les Parties contractantes doivent restreindre toutes les limitations ou exceptions dont elles assortissent les droits prévus dans le présent traité à certains cas spéciaux où il n'est pas porté atteinte à l'exploitation normale de l'interprétation ou exécution ou du phonogramme ni causé de préjudice injustifié aux intérêts légitimes de l'artiste*

*interprète ou exécutant ou du producteur du phonogramme.*

*Article 18*

***Obligations relatives aux mesures techniques***

*Les Parties contractantes doivent prévoir une protection juridique appropriée et des sanctions juridiques efficaces contre la neutralisation des mesures techniques efficaces qui sont mises en oeuvre par les artistes interprètes ou exécutants ou les producteurs de phonogrammes dans le cadre de l'exercice de leurs droits en vertu du présent traité et qui restreignent l'accomplissement, à l'égard de leurs interprétations ou exécutions ou de leurs phonogrammes, d'actes qui ne sont pas autorisés par les artistes interprètes ou exécutants ou les producteurs de phonogrammes concernés ou permis par la loi.Convention de Berne et qui restreignent l'accomplissement, à l'égard de leurs oeuvres , d'actes qui ne sont pas autorisés par les auteurs concernés ou permis par la loi.*

Les pays de l'Union Européenne ont transposés ces principes dans la directive du 22 mai 2001. Elle définit une protection juridique *contre la neutralisation des mesures techniques efficaces qui sont mises en oeuvre par les auteurs dans le cadre de l'exercice de leurs droits et qui restreignent l'accomplissement d'actes qui ne sont pas autorisés par leurs auteurs concernés ou permis par la loi.* Cette directive est en cours de transposition.en France et fait l'objet d'un projet de loi discuté depuis le début de l'année 2003. La date limite e transposition était le 22 Octobre 2002. L'objet de cette directive est d'adapter aux droits d'auteur et droits voisins aux évolutions technologiques et particulièrement à la société de l'information.. De leur côté les Etats Unis ont adopté le DMCA Digital Millenium Copyright Act) qui correspond en Europe à la directive du 22 Mai, EUCD : European Union Copyright Directive.

### 4.2.2. Un régime juridique précis

Plusieurs dispositifs techniques, basés la plupart du temps sur les techniques de marquage et de cryptage, sont définis (1.2.1.1) . Les pays membres sont tenus de faire respecter par des mesures appropriées la protection matérielle (1.2.1.2)

#### 4.2.2.1. Définition d'une mesure technique de protection

Pour être qualifier de mesure technique, celle-ci doit présenter les caractéristiques suivantes :

##### 4.2.2.1.1. Limitation

L'article 6.3 énonce : *Aux fins de la présente directive, on entend par «mesures techniques », toute technologie, dispositif ou composant qui, dans le cadre normal de son fonctionnement, est destiné à empêcher ou à limiter, en ce qui concerne les œuvres ou autres objets protégés, les actes non autorisés par les titulaires des droits.*

##### 4.2.2.1.2. Efficacité :

D'après l'article 6.3 de la Directive, « *L efficacité est présumée lorsque l'utilisation d'une oeuvre est contrôlée par un code d'accès ou un système de cryptage, de brouillage ou toute transformation ou lorsque le mécanisme de contrôle de copie parvient à assurer effectivement son objectif.*

##### 4.2.2.1.3. Contournement interdit:

D’après l’article 6.1 de la Directive, *Les États membres prévoient une protection juridique appropriée contre le contournement de toute mesure technique efficace, que la personne effectue en sachant, ou en ayant des raisons valables de penser, qu'elle poursuit cet objectif.*

Ainsi dans son article 6 elle impose aux Etats membres une nouvelle infraction qui s’ajoute à celle de contrefaçon. Celle-ci concerne l’acte de contournement des « mesures techniques efficaces ». Non seulement l’acte même de contournement est visé, mais aussi le fait de fabriquer, importer, distribuer, vendre, louer, posséder à des fins commerciales ou faire la promotion d’outils ayant pour objet principal le contournement de ces mesures techniques. Ainsi, la technique vient protéger les droits d’auteur, et réciproquement, le droit vient protéger la
technique.

Le marquage d’une oeuvre à la demande d’un titulaire de droits sera ainsi qualifier de mesure technique de protection. Un système de DRM qui est composé d’un ensemble de mesures de protection cohérent ou bien un système de protection ou de limitation de la copie seront des mesures techniques de protection

#### 4.2.2.2. Sanctions du non respect de la protection

Le but de cette directive est la mise en place d’une protection juridique harmonisée afin de promouvoir la distribution des oeuvres sur le marché intérieur
Ainsi selon le considérant 56 :
*Le risque existe, toutefois, de voir se développer des activités illicites visant à supprimer ou à modifier les informations, présentés sous forme électronique, sur le régime des droits dont relève l’oeuvre ou l’objet, ou visant à distribuer, importer aux fins de distribution, radiodiffuser, communiquer au public ou mettre à sa disposition des oeuvres ou autres objets protégés dont ces informations ont été supprimées sans autorisation. Afin d’éviter des approches juridiques fragmentées susceptibles d ‘entraver le fonctionnement du marché intérieur, il est nécessaire de prévoir une protection juridique harmonisée contre toute activité de cette nature.*

La directive européenne veut empêcher les activités illicites qui modifierait le régime des droits contenu dans l’oeuvre, par exemple dans le tatouage.

##### 4.2.2.2.1. Les actes illicites

*Article 6*
*Obligations relatives aux mesures techniques*
*1. Les États membres prévoient une protection juridique appropriée contre le contournement de toute mesure technique efficace, que la personne effectue en sachant, ou en ayant des raisons valables de penser, qu'elle* poursuit cet objectif.
*2. Les États membres prévoient une protection juridique appropriée contre la fabrication, l'importation, la distribution, la vente, la location, la publicité en vue de la vente ou de la location, ou la possession à des fins commerciales de dispositifs, produits ou composants ou la prestation de services qui:*
*a) font l'objet d'une promotion, d'une publicité ou d'une commercialisation, dans le but de contourner la protection, ou*
*b) n'ont qu'un but commercial limité ou une utilisation limitée autre Que. de contourner la protection, ou*
*c) sont principalement conçus, produits, adaptés ou réalisés dans le but de permettre ou de faciliter le contournement de la protection de toute mesure technique efficace.*

Ainsi l'interdiction porte aussi sur la diffusion ou la communication des moyens permettant d'outrepasser les systèmes de protection des contenus numériques protégés, notamment la possibilité de poursuivre ceux qui mettraient à disposition des logiciels destinés au piratage.

#### *4.2.2.2.1.1. L' élément matériel*

La directive prévoit deux régimes de protection juridique correspondant à deux types actes illicites à travers les articles 6 et 7. En conformité avec les traités OMPI de 1996, l'article 6 vise les actes tendant à contourner des dispositifs de protection informatifs, l'article 7 des dispositifs coercitifs.

Un dispositif informatif protège les informations suivantes :

les informations directes : ce sont des données qui peuvent être fournies par les titulaires de droits pour permettre l'identification de l'oeuvre (nom de l'auteur, titre, etc..)

les informations indirectes : Il s'agit du code qui représente les systèmes de marquage des oeuvres audiovisuelles comme par exemple l'ISAN.

Le dispositif coercitif a pour finalité de contrôler une oeuvre sujette aux droits d'auteur et doit avoir une certaine efficacité L'effectivité absolue d'une mesure technique ne pouvant pas jamais être certaine, le juge devra examiner si la mesure contournée était suffisamment solide compte tenu de l'état de la technique. Le juge constatera que la mesure technique de protection n'a pas résisté et donc que la mesure n'est pas efficace. L'efficacité sera examinée en fonction du but poursuivi par cette technique. L'article 6-3 donne aux mesures techniques une présomption d'efficacité et les protègent .. quant elles sont efficaces.

Article 6-3 les mesures techniques sont réputés efficaces lorsque elles atteignet cet objectif de protection.

L'article 6-3 est donc un peu tautologique et nécessitera d'être interprété par la jurisprudence.

#### *4.2.2.2.1.2. L'élément moral*

L'incrimination de l'acte illicite de contournement est soumise à la présence d'un élément moral, savoir ou avoir des raisons valables de penser que. l'objectif poursuivi est la neutralisation non autorisée). La directive impose un caractère volontaire aux atteintes à l'information. Selon l'article 7.1, il faut que. les actes , *que la personne effectue en sachant, ou en ayant des raisons valables de penser, qu'elle poursuit cet objectif.*

Ainsi le critère de l'illicéité du dispositif de contournement n'est pas précisément défini ce qui peut permettre, selon les intérêts en présence, d'adapter la situation.

### 4.2.2.2.2. Les sanctions

La sanction des actes de contournement est celle appliqué lors d'une contrefaçon selon l e projet de transposition de la directive du 22 mai 2001.

### 4.2.3. Un régime juridique incertain

#### 4.2.3.1. Violation de la mesure technique pour accès légitime

Une question reste en suspend : l'utilisateur qui force une mesure technique efficace pour bénéficier d'une exception ou pour accéder à une oeuvre qui n'est plus ou pas protégée, pourra-t-il être poursuivi pour l'acte de contournement lui-même ?
Le fait de contourner une mesure technique ou de diffuser des équipements le permettant est susceptible de constituer une faute, une négligence, un acte illicite ou un tort, autant d'actes générateur d'une obligation de réparation du préjudice causé. Manipuler un décodeur pour ne pas payer est un exemple.

Par un autre raisonnement, on pourrait considérer que la distribution d'équipement de contournement de mesures techniques peut constituer une atteinte au marché d'un concurrent, une entrave à la libre concurrence et provoquer une désorganisation de l'exploitation de son entreprise. Ainsi le fait de distribuer des "dongles" qui imiteraient les clés originales est condamnable. Bien sûr un tel moyen n'est applicable que dans un contexte de concurrence déloyale commerciale.

#### 4.2.3.2. Droit d'auteur ou brevet sur le logiciel

Les procédés qui permettent de couvrir les informations sur le régime des droits sont souvent des procédés de marquage apparents ou invisibles. La directive du 22 Mai 2001 protège le marquage contre un détournement. En protégeant les moyens d'identifier une oeuvre, la directive encourage un système de dépôt de créations. Le droit d'auteur traditionnel tend à faciliter la création. Aussi aucune démarche administrative n'est nécessaire pour bénéficier de la protection. Mais l'Etat qui souhaite contrôler la circulation des oeuvres ou bien l'industrie qui souhaite contrôler les divers usages de l'oeuvre ont pour préférence un système de dépôt

### 4.2.4. Un régime juridique nécessaire ?

Selon certains juristes (Isabelle Vaillant) les mesures techniques n'ont besoin de protection supplémentaire contre le contournement. Ni la Directive du 22 mai 2001, ni les Traités de l'OMPI de 1996, n'assimilent le contournement de mesures techniques de protection à de la contrefaçon. Dans le cadre de la transposition de directive "droit d'auteur"", il ne faudrait rien changer dans le code de la propriété intellectuelle.

Les mesures techniques sont d'ores et déjà protégées par le droit français, au niveau du droit civile, pénal(fraude informatique, droit des logiciels); Ainsi une mesure technique, au sens de l'article 6, permet toujours de protéger un système de traitement automatisé de données. De plus la loi pour la confiance dans l'économie numérique vient étendre les incriminations relatives à la fraude informatique et les rendre conformes aux objectifs fixés par la Directive.

# 5. LES DROITS MENACES PAR LE MARQUAGE DES OEUVRES

Les systèmes de DRM comme les nouvelles techniques en général ont souvent tendance à modifier l'équilibre subtil entre les libertés, équilibre fondateur de notre Etat de droit. Aussi dans une première partie, examinerons-nous d'abord en quoi ces systèmes menacent particulièrement les droits fondamentaux(5.1). Mais, dans la monde numérique des oeuvres numériques une technique de protection des droits d'auteur comme le marquage est destiné

## 5.1. DROITS FONDAMENTAUX

### 5.1.1. RESPECT DE LIBERTE D'EXPRESSION

***Article 11.*** *- La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme ; tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi.* **Déclaration des Droits de l'Homme et du Citoyen, 1789** ***Article 19.*** –

*Tout individu a droit à la liberté d'opinion et d'expression, ce qui implique le droit de ne pas être inquiété pour ses opinions et celui de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit.* **Déclaration des Droits de l'Homme, décembre 1948 (Assemblée générale de l'ONU).**

La commission spécialisée "libertés individuelles" du Conseil supérieur à la propriété littéraire et artistique (CSPLA), l'organisme chargé par le ministère de la Culture de préparer la transposition de la directive européenne sur les droits d'auteur dans la société de l'information, a publié le 26 juin un avis. Présidé par Maurice Viennois, conseiller honoraire à la Cour de cassation et membre de la Commission nationale de l'informatique et des libertés (Cnil), le groupe de travail avance des propositions qui sont contraires aux recommandations de la Cnil elle-même qui remettent en cause des libertés publiques sur internet.
Créé en mai 2001, le CSPLA réunit les principaux syndicats d'auteurs, éditeurs, producteurs et diffuseurs, deux associations de consommateurs et huit "personnalités qualifiées". Dans son avis du 26 juin, le Conseil propose d'abord que, pour faciliter la recherche d'infractions en contrefaçon sur le réseau, la durée de détention des données de connexion par les opérateurs techniques soit portée à trois ans, soit "la durée de prescription de l'action pénale en matière de délits".
Les principes du régime de conservation et d'effacement de ces données ont été fixés par la loi sur la sécurité quotidienne (LSQ) du 15 novembre 2001, dont les décrets d'application n'ont toujours pas été adoptés. Lors de l'examen du texte, la Cnil, garant officiel de la protection des libertés en informatique, s'était prononcée pour que ces "logs" de connexion ne soit pas conservés au-delà de trois mois.
Après concertation avec les autorités judiciaires, le Forum des droits sur l'internet, l'organisme de "corégulation" de l'internet en France, recommandait de son côté une durée de conservation maximale d'un an.
La commission du CSPLA va plus loin, en voulant permettre aux sociétés de créer des fichiers d'adresses IP d'internautes pratiquant l'échange de contenus illicites, qu'il

s'agisse de musique, de films ou de logiciels. Elle souhaite ainsi "que le Parlement trouve (...) une solution permettant aux sociétés de gestion et aux ayants-droit de procéder à la constitution de tels fichiers dans le seul but d'assurer la protection de ces droits".
En rendant cet avis, la commission soutient a posteriori un amendement sénatorial au projet de loi de transposition de la directive sur la vie privée, adopté par la Chambre haute le 1er avril dernier. Le sénateur Alex Türk, vice-président de la Cnil, avait fait étendre aux entreprises victimes d'infractions le droit de procéder à des "traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté". Les majors et sociétés de protection de droits d'auteur pourraient ainsi collecter des informations nominatives sur les usagers de réseaux P2P en infraction avec le droit d'auteur
Pourtant, dans un avis émis le 15 mars 2001 à la demande de la société Webcontrol, la Cnil avait estimé que la constitution sur les réseaux peer-to-peer de fichiers d'infractions par des sociétés privées était non-conforme aux principes de la loi "informatique et libertés".

Au moment où l'Assemblée nationale s'apprête à examiner en deuxième lecture la loi sur la confiance dans l'économie numérique, le CSPLA soutient encore dans son avis une "transposition parfaite" de la directive "Commerce électronique" à l'origine de la loi. Les dispositions de ce texte prévoient entre autres la mise en cause de la responsabilité des hébergeurs n'ayant pas obtempéré à la demande de retrait d'un contenu à "caractère illicite".

Cette responsabilité des hébergeurs, déjà prévue et finalement retoquée dans des lois précédentes, fait pourtant encore largement débat. Depuis longtemps, les associations mobilisent contre ce devoir de censure imposé aux prestataires techniques sur notification des ayants-droit, même sans décision de justice.

La dernière recommandation de la commission est sûrement la plus étonnante et tient presque de l'anticipation orwelienne. Dans son avis, elle prend acte du développement de solutions techniques permettant "de créer un système général d'empreinte informatique permettant de vérifier si les fichiers échangés sur le réseau sont autorisés et de bloquer les échanges de fichiers illicites lors de leur passage par un serveur ou un routeur". Soit le fin du fin de la "gestion de droits numérique" (Digital Rights Management, DRM), permettant d'identifier, de localiser et d'intercepter à tout moment tout contenu en circulation sur le réseau, grâce à un système de marqueurs logiciels intégrés aux fichiers.
La commission prend le soin de rappeler qu'un tel système de police du réseau géré en direct par les ayants-droit ne pourrait naturellement être mis en place que s'il est "conforme notamment au principe constitutionnel de protection de la vie privée et aux stipulations de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales". Gageons que les majors du divertissement et les sociétés de droits d'auteur sauront un jour attaquer ces derniers garde-fous, ainsi qu'elles ébranlent déjà les garants officiels des libertés sur le réseau.

### 5.1.2. DROIT AU RESPECT DE LA VIE PRIVEE

Il est fort possible qu’il existe des bases juridiques sur lesquelles on pourrait s’appuyer pour revendiquer un droit à la protection de la vie privée ou à la confidentialité lors de l’accès à un contenu protégé. En fait, aux États-Unis, des spécialistes universitaires ont soutenu que la Constitution protégeait le droit de lire de façon anonyme. Dans de nombreux pays européens, les données privées sont protégées et ne peuvent être

utilisées qu'en respectant des conditions rigoureuses.

En France, pour Michel Gentot, Président de la Commission Nationale de l'Informatique et des Libertés, "A s'en tenir à la protection des données personnelles, on pourrait considérer que cette protection est assurée dès lors que les personnes concernées disposent d'un droit d'accès et de rectification et de la garantie que les données demeureront confidentielles. ". Ce sont les opérateurs commerciaux qui le pensent. La loi du 6 Janvier 1978 et le directive européenne du 24 Octobre 1995 précisent que la protection va bine plus loin. Selon Michel Gentot, dans l'Administration publique au service des citoyens de G.Chatillon, page 328, "*il s'agit principalement de recherche si la collecte de données toujours plus nombreuses et leur exploitation informatique est acceptable au regard des "droits et libertès" des personnes mais, aussi si le regroupement dans un même ensemble jusqu'alors traités de manière étanche est nécessaire, pour quelle finalité, pour quels avantages."*

Un système de DRM n'est pas suffisant pour protéger la vie privée mais c'est probablement le meilleur instrument dont on dispose à cet effet. À cet égard, il faut aussi se demander comment identifier les différentes copies numériques (qui, présumera-t-on, ont été vendues à un utilisateur donné) sans menacer le respect de la vie privée ou de la confidentialité. Si les différentes copies sont identifiées, par exemple au moyen d'un filigrane contenant un code de transaction, une des solutions pourrait consister à les numéroter, sans inclure de données identifiant l'utilisateur qui a "commandé" la copie en question. Les numéros de copie pourraient être reliés, dans une base de données sécurisée, aux différents utilisateurs. Il serait possible, s'il y avait pour cela une bonne raison – par exemple une décision judiciaire –, d'établir le lien entre le numéro de copie et l'utilisateur. Le recours à des tiers de confiance qui agrégeraient les données relatives à l'utilisation pourrait être particulièrement important pour l'utilisateur. Un agrégateur ou une organisation de gestion collective utilisant un système de DRM pourrait ainsi préserver la confidentialité du lien éventuel entre une copie donnée fournie en ligne et un utilisateur particulier. Le propriétaire du contenu recevrait, avec la rémunération de l'utilisation de ses œuvres, un compte rendu sur le nombre d'utilisations, éventuellement avec une indication du type d'utilisateurs, mais aucun renseignement sur les différents utilisateurs. Sans ce type de garantie de la confidentialité, il risque d'être très difficile d'assurer le développement du commerce électronique du droit d'auteur. En d'autres termes, un système de DRM bien conçu, qui agrégerait les données de façon à protéger la vie privée et la confidentialité, est probablement indispensable pour le succès du commerce électronique du droit d'auteur.

### 5.1.3. La gestion des droits collectifs

Le développement de ces techniques de marquage ou de tatouage aura très certainement des conséquences sur la gestion collective des oeuvres. Comme le précise le livre vert de la Commission européenne sur le droit d'auteur et les droits voisins dans la société de l'information de juillet 1995, les techniques numériques permettront, grâce à ces outils techniques, une « gestion plus fine et individualisée des droits ».

Dès lors que chaque oeuvre et chaque utilisation de l'oeuvre sont directement identifiables sur le réseau internet, il est parfaitement possible d'imaginer la possibilité pour les créateurs de conclure directement avec les utilisateurs des conventions relatives aux oeuvres. Cette gestion individuelle des droits aurait le mérite, pour certains, d'affiner la tarification pour améliorer l'adéquation entre le prix et l'usage de l'oeuvre. Les sociétés de gestion collective plaident en revanche en soutenant que ces dispositifs techniques de protection renforceront leur présence sur le réseau Internet en

leur confiant un rôle de surveillance de l'utilisation de ces techniques ou de catalogage des œuvres disponibles.

Comme le souligne Pierre Sirinelli, les sociétés de gestion collective doivent apporter la preuve de leur utilité sur le réseau internet en permettant la mise en place, notamment, de guichets uniques de négociation de droits, qui seraient particulièrement utiles s'agissant d'oeuvres multimédias pour lesquelles de nombreuses autorisations doivent être sollicitées.

## 5.2. VERS UN ABANDON DE CERTAINS EXCEPTIONS

Les exceptions ou limitations au droit d'auteur sont très nombreuses. A titre d'exemple, une liste de deux pages en est fournie par l'article 5 de la directive du 22 mai 2001. Les systèmes de DRM vont remettre en cause le bien-fondé de ces exceptions.

Les systèmes de DRM vont permettre un rapprochement plus étroit entre l'auteur et le consommateur. Certains artistes (David Bowie, Madonna, Prince…) se sont exprimés en faveur d'une diffusion indépendante de leur musique sur internet, sans passer par les maisons de disques. Cette nouvelle position des auteurs vient bouleverser le modèle économique d'une industrie du disque, très attachée à l'exploitation ancienne des droits d'auteur. Bien sûr la découverte, le financement, la production, l'enregistrement et le promotion de nouveaux talents restent essentiellement dans les attributions des maisons des disques. Il n'en demeure pas moins que les évolutions technologiques liées aux marquage des œuvres et aux systèmes de DRM permettent aux titulaires de droits d'envisager un éventuel retour au droit exclusif en matière de rémunération pour copie privée audiovisuelle.

Ainsi la copie privée(5,.1.1), la rémunération pour copie privée(5.2.2) et la licence légale (5.2.3) pourrait être remis en cause (5.2.4)

### 5.2.1. L'Exception de Copie privée

En France, l'article L.122-5 du Code de la propriété intellectuelle formule ainsi " l'exception " de copie privée : " *lorsque l'œuvre a été divulguée, (…) l'auteur ne peut interdire les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective* ". Ainsi, les actes de reproduction d'une œuvre de l'esprit, réalisés dans la sphère privée, échappent-ils au monopole de l'auteur.

L'article 122-5 a vocation à être appliqué à toutes les oeuvres

Pourtant l'exception de copie privée a été supprimée dans la directive du 14 mai 1991 sur la protection juridique pour les programmes d'ordinateur,(Logiciel 5.2.1.1.1) ainsi que dans celle du 11 mars 1996 sur la protection juridique des bases de données. (5.2.1.1.1.2) pour les bases de données.

#### *5.2.1.1.1.1. Logiciels*

Les logiciels. connaissent une exception au droit de reproduction. L'article L.122-6-1 du Code de la propriété intellectuelle n'autorise la personne titulaire d'une licence d'utilisation à reproduire le logiciel que dans deux cas de figure.

sauvegarde

Tout d'abord, lorsque cette copie est réalisée à des fins de sauvegarde, mais à condition que celle-ci soit " *nécessaire pour préserver l'utilisation du logiciel* ". De nombreux logiciels étant commercialisés sous forme de CD-Rom, support

particulièrement fiable, on peut considérer que leur duplication ne se justifie pas au regard de cette finalité.

Indispensable à l'utilisation

La copie de logiciels est également autorisée lorsque celle-ci est indispensable à l'utilisation du logiciel, "*conformément à sa destination, y compris pour corriger des erreurs* ".

En dehors de ces deux hypothèses limitées, la reproduction d'un logiciel, par exemple à l'aide d'un graveur de CD-Rom dont l'usage s'est répandu, constitue une contrefaçon. Il en sera de même pour les jeux vidéo et les œuvres multimédia. Pour accéder à ce type de créations, il faut utiliser des logiciels. Ces logiciels systèmes ou applicatifs. qui accèdent à ces oeuvres, peuvent être complètement transparents pour ces utilisateurs de jeux ou de multimédia. Mais la copie de ces œuvres nécessite copie de logiciels. Or, nous l'avons vu ci-dessus, ce sont les dispositions légales relatives à la copie de sauvegarde ou indispensable à l'utilisation qui en réglementent la reproduction.

#### *5.2.1.1.1.2. Base de données*

Les bases de données, introduites dans le Code de la propriété intellectuelle par une loi du 1er juillet 1998, ne peuvent également donner lieu à la réalisation de copies privées. Il n'est pas surprenant de constater que ces deux premières œuvres de " *l'ère numérique* " à avoir bénéficié des dispositions du Code de la propriété intellectuelle, ont été écartées du champ d'application de l'article L.122-5.

Le " *numérique* " impose, en effet, de repenser l'exception de copie privée.

### 5.2.1.1.2. La particularité de la copie " numérique "

Le droit ne fait pas la distinction entre une copie analogique ou une copie numérique. Avant l'arrivée du numérique, la possibilité offerte à toute personne d'enregistrer sur un support magnétique une œuvre musicale, diffusée à la radio, ou une œuvre audiovisuelle, diffusée par une chaîne de télévision, pouvait causer un préjudice financier important aux intervenants de la création musicale et audiovisuelle. Ce préjudice économique fut compensé par la création, par une loi du 3 juillet 1985, d'une redevance perçue sur le prix de vente des supports vierges (cassettes audio et vidéo) et redistribuée aux ayants droit par des sociétés de gestion collective des droits.

Mais les nouvelles technologies de reproduction numérique des oeuvres modifient considérablement la notion de copie. Techniquement, la reproduction d'une œuvre sur des supports analogiques provoque une altération de la qualité de l'œuvre reproduite. De nombreuse fréquences ont été perdues et filtrées. Ceci freine la prolifération des copies qui se dégradent naturellement. La copie n'a pas la qualité de l'original. Par contre, dans le monde numérique, " cette sorte d'autolimitation n'existe plus pour les copies numériques " (Internet et les réseaux numériques, Rapport du Conseil d'Etat de juillet 1998). Dupliquer au moyen d'un graveur un CD-audio s'apparente plus à la création d'un véritable " clone " numérique de l'œuvre qu'à la création d'une simple " copie " de celle-ci.

Les nouvelles pratiques du numérique Au-delà de cette caractéristique de la copie numérique, ce sont également les nouvelles pratiques d'exploitation et de diffusion des œuvres qui renouvellent le débat sur le bien-fondé de l'exception de copie privée. En effet, le " copiste " peut aujourd'hui devenir très facilement un " diffuseur " de l'œuvre. C'est particulièrement vrai s'agissant de l'internet.

### 5.2.1.1.3. Internet et la copie privée

Le problème que soulève l'exception de copie privée dans le cadre d'un réseau comme

l'internet est double.

Certains ont d'abord tenté d'invoquer cette exception, suite à la mise en ligne, sur leur site web, d'œuvres dont ils n'étaient pas cessionnaires des droits. Les textes des chansons de Jacques Brel et de Michel Sardou ont ainsi été numérisés par des étudiants et diffusés sur le site de leur école sans l'autorisation des titulaires des droits. Les auteurs des faits reprochés soutenaient que les reproductions étaient licites, puisqu'elles étaient destinées à un usage privé et non à une utilisation collective. Selon eux, leur site constituait un " *domicile virtuel* " visité par les utilisateurs, sans aucun rôle d'émission de leur part puisque ce sont les visiteurs qui prenaient l'initiative de venir " *visiter* " leur site. Le juge des référés, saisi par les ayants droit des auteurs concernés, a rejeté l'argument de la copie à usage privé sur l'internet, considérant qu' " *en permettant à des tiers connectés au réseau Internet de visiter leurs pages privées et d'en prendre éventuellement copie, et quand bien même la vocation d'Internet serait-elle d'assurer une telle transparence et une telle convivialité* ", les intéressés " *favorisent l'utilisation collective de leurs reproductions* ". Dès lors, ils ne pouvaient prétendre au bénéfice de l'exception de copie privée.

Au-delà de la question de savoir si le responsable du site dispose de l'autorisation de l'auteur pour mettre son œuvre en ligne, on considère généralement que le particulier qui télécharge, sur son ordinateur personnel, des œuvres qu'il a pu trouver sur le réseau, n'est pas un contrefacteur, puisqu'il bénéficie de l'exception de copie privée, (sauf pour des bases de données et des logiciels)  Mais une analyse plus précise de l'exception de copie privée peut faire douter de cette solution. Pour bénéficier de l'exception de copie privée, encore faut-il avoir légitimement accès à l'œuvre qui sera l'objet de la reproduction. Ainsi, le particulier peut dupliquer sur cassette audio une œuvre musicale parce que la station de radio qui diffuse cette œuvre le fait en accord avec les ayants droit. Qu'en est-il lorsqu'un site web propose au téléchargement des œuvres musicales sans l'accord préalable des titulaires des droits ? La personne qui les télécharge ne risque-t-elle pas elle-même de réaliser un acte de contrefaçon ? Si le phénomène de la copie privée ne reçoit pas de régulation législative, les tribunaux auront certainement, à se prononcer sur cette question. Avec le marquage des œuvres il sera plus facile au titulaire de droit d'établir son cheminement à travers le réseau en constituant des preuves plus facile à interpréter. L'acte de contrefaçon pourra être plus facilement établi.

##### 5.2.1.1.4. L'exception de copie numérique :

Plusieurs solutions de nature législative sont proposées pour circonscrire le périmètre d'exploitation d'une œuvre protégée, particulièrement sur l'internet.
Dans son rapport " *Internet et les réseaux numériques* ", le Conseil d'Etat suggère de " *(…) poser comme principe légal que la copie privée, c'est-à-dire, strictement réservée à l'usage privé du copiste et non destinée à un usage collectif, est autorisée, sauf interdiction expresse du titulaire des droits sur l'œuvre, notifiée au copiste lors de la copie initiale sur le site par un message explicite* ". La délégation de l'Assemblée nationale pour l'Union européenne, conduite par son rapporteur, Monsieur Jacques Myard, a adopté une position plus radicale en proposant la suppression de l'exception de copie privée sur l'internet.
Mais la notion de " *copie privée* " n'est pas nécessairement simple à appréhender en matière d'internet compte tenu de certaines pratiques, notamment celle du " *cache* ". Pour ne pas encombrer les réseaux et favoriser la fluidité des connexions, les fournisseurs d'accès procèdent à des copies de sites sur des serveurs-relais. La directive

du 22 Mai 2001 sur l'harmonisation du droit d'auteur a voulu tenir compte de ces particularités de fonctionnement, propres à l'internet. Aussi a-t-elle introduit, dans son article 5, la notion de " *copie technique* ". Celle-ci consiste en une reproduction provisoire qui fait " *partie intégrante d'un procédé technique ayant pour unique finalité de permettre une utilisation d'une œuvre (…) et n'ont pas de signification économique indépendante* ". Cette " *copie technique* " doit, selon la directive, constituer une exception au droit de reproduction.

Ainsi l'exception pour copie privée et pour copie transitoire ou accessoire existe en droit. Pour comprendre les conséquences des systèmes de DRM sur ces exceptions, il convient d'abord de définir la rémunération pour copie privée.

### 5.2.2. DEFINITION DE LA REMUNERATION POUR COPIE PRIVEE

Les créations ne sont possibles que si elles sont accompagnées d'un rémunération. Mais le droit exclusif des auteurs est d'autant moins bien respecté que la technique moderne permet aux utilisateurs de réaliser eux-mêmes, par de nouveaux procédés techniques, des copies des œuvres. Le législateur a du intervenir pour remédier à cette perte liés à l'exception de copie privée. Par une loi dite loi 'Lang' du nom du ministre de l'époque, il a instauré la loi du 3 Juillet 1985. Dans son article 31 cette loi prévoit une rémunération pour copie privée des œuvres fixés sur phonogrammes ou vidéogrammes au bénéfice des auteurs.
Cette rémunération est une somme d'argent versée en contrepartie de la reproduction réservée à une usage privé des œuvres sonores et audiovisuelles. Mais cette définition doit être complétée d'une réflexion pour déterminer la nature juridique de cette rémunération.
Jusqu'en 1992, des doutes persistaient sur la nature du droit à rémunération. Cette rémunération était tout à tour qualifié de taxe parafiscale, d'indemnité au profit des auteurs ou de droit exclusif des auteurs. Finalement , contrairement à la taxe de 3% instaurée sur les appareils de reproduction par l'article 22 de la loi de finances du 30 décembre 1975 il ne s'agit pas d'une taxe.
Aujourd'hui, depuis l'instauration en 1992 de l'article L 111-1, alinéa 2 du CPI qui indique que *le droit d'auteur comporte des attributs d'ordre intellectuel et moral, ainsi que des attributs d'ordre patrimonial, qui sont déterminés par les Livres I et III du Code de la Propriété intellectuelle*, il ne fait plus de doute que cette rémunération est un droit d'auteur. La codification du CPI est supposée avoir été fait en 1992 à droit constant. La loi du 3 Juillet 1985 relative "aux droits d'auteur et aux droits des artistes interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle" a été codifiée, pour ce qui est de la rémunération pour copie privée, aux articles L 311-1 à L 311-8 du CPI, c'est à dire quelle compose le titre premier du livre III du CPI.
L'article L 331-5 précise notamment que les types de support, ainsi que les taux de rémunération et le modalités de versement, sont déterminées par une commission présidée par un représentant de l'Etat. La composition de cette commission est mixte, c'est à dire qu'elle regroupe l'ensemble des personnes concernées par la rémunération pour copie privée audiovisuelle. Ainsi la commission est composée pour moitié, de personnes désignées par les organisations représentant les bénéficiaires du droit à rémunération, à savoir les auteurs, les artistes interprètes et le producteur de phonogrammes et de vidéogrammes. Le reste de la commission se compose, pour un quart, de personnes désignées par les organisations représentant les fabricants ou importateurs de supports vierges et , pour un quart, de personnes désignées par les

organisations de consommateurs.
La loi du 3 Juillet 1985 a été adoptée dans un contexte où la reproduction numérique n'existait pratiquement pas. A l'époque le marché de la reproduction audiovisuelle était dominée par les magnétophones à cassettes des années 1960( et l'enregistrement des radios à modulation de fréquence) et les magnétoscopes ( et l'enregistrement des émissions de télévisions). Ces systèmes mécaniques et électroniques d'enregistrement sont dits analogiques, car il conserve le son sous sa forme originale sans nécessiter une opération de numérisation. L'article L 311-4 précise que *le montant de la rémunération est fonction du type de support et de la durée d'enregistrement qu'il permet*. Dans l'idée du législateur, il n'envisageait pas que des œuvres puissent être stockés su des CD ou des disques durs puisque dans ce cas le type de support ne peut plus être évalué en durée d'enregistrement mais plutôt en capacité et en format de stockage.
Pendant plus de quinze ans, la rémunération était basée sur un prix de 1,50F par heure pour les phonogrammes et 2,25F par heure pour les vidéogrammes. Avec l'apparition des nouveaux procédés de reproduction numérique et les développement du réseau internet, la copie privée a suscité un enthousiasme tel que le préjudice causé aux auteurs du fait de la généralisation de la copie privée devenait insupportable. La loi du 17 juillet 2001 portant diverses dispositions d'ordre social, éducatif et culturel a étendu la compensation financière à l'ensemble des œuvres de l'esprit susceptibles d'être reproduites pour un usage privé.

### 5.2.3. LA LICENCE LEGALE

Aucun article du CPI ne fait référence directement au terme de licence légale. Il s'agit d'une construction doctrinale. Selon M. Strowel, la licence légale consiste dans "le retrait du pouvoir de l'auteur de s'opposer à l'utilisation de son œuvre contre le paiement d'une rémunération". Une licence légale est une licence qui est imposée à l'auteur par la loi. L'autorisation dont dispose l'utilisateur ne lui a pas été octroyé par l'auteur, comme le principe du droit exclusif de l'auteur le voudrait. Il s'agit donc d'une exception au droit exclusif de l'auteur. Pour l'utilisateur la licence légale est vue comme la liberté d'utiliser l'œuvre moyennant le paiement d'un rémunération.
L'objet de la loi du 3 juillet 1985 était de moderniser la loi du 11 mars 1957 en vue de l'adapter au progrès des techniques de reproduction et de télécommunication. Avec cette loi le législateur a instaurer une double licence légale. Ainsi, en ce qui concerne les phonogrammes, l'article 214-1 du CPI institue une licence légale, assortie en contrepartie d'un droit à rémunération dit rémunération équitable. L'artiste interprète et le producteur ne peuvent s'opposer à la communication directe du phonogramme dans un lieu public (dès lors qu'il n'est pas utilisé dans un spectacle) à sa radiodiffusion, à la distribution par câble simultanée et intégrale de cette radiodiffusion. Les deux circonstances ainsi prises en compte (comportant en fait toutes deux une communication directe à un public) sont conformes à l'article 12 de la convention de Rome : *Lorsqu'un phonogramme a été publié a été publié à des fins de commerce, l'artiste interprète et le producteur ne peuvent s'opposer :*

*1/ à sa communication directe dans un lieu public (c'est à dire le cas type des discothèques et du disc jokey), dès lors qu'il n'est pas utilisé dans un spectacle*

*2/à sa radiodiffusion, non plus qu'à sa distribution par câble simultanée et intégrale …*

### 5.2.4. Retour vers la liberté contractuelle grâce aux systèmes de protection

Le mécanisme de licence légale est l'objet de nombreuses critiques de la part des

titulaires de droits qui pensent que leur droit exclusif n'est pas respecté et pas suffisamment compensé par une rémunération. Les consommateurs ont le sentiment de disposer d'un "droit à la copie privée". Les nouveaux systèmes de DRM aurait la préférence des auteurs car il permettent d'envisager un retour à la liberté contractuelle. Mais ce retour ne sera possible que si la technique le permet() et si les systèmes de DRM permettent de fixer le montant de la rémunération.

Le livre vert de la Commission des Communautés Européennes sur le droit d'auteur et les droits voisins dans la société de l'information rappelle l'importance des moyens de protection: "*si des moyens techniques limitant ou empêchant la copie privée sont instaurés, la justification de la licence légale que constitue un système de rémunération s'estompe"*

De même, comme nous l'avons vu plus haut, la directive du 22 Mai 2001 s'intéressent aux systèmes de protection numérique. Selon la directive, dans son considérant 52, les titulaires de droits peuvent recourir à des mesures techniques compatibles avec les exceptions et limitations relatives à la copie à usage privé ( par exemple le contrôle du nombre de reproductions). Selon le considérant 25, Ces mesures techniques peuvent permettre d'identifier l'œuvre, l'auteur et les titulaires de droit, mais également de fournir des informations sur les conditions et le modalités d'utilisation de l'œuvre et facilité la gestion des droits y afférents. En outre, sous réserve des principes de protection de la vie privées posés par le considérant 57 de la directive du 24 Octobre 1995, les systèmes relatifs à l'information peuvent traiter des données à caractère personnel relatives aux habitudes de consommation des particuliers ou aux comportements en ligne. Ainsi les systèmes de DRM pourraient remplacer la protection légale par une protection technique. En fait ces systèmes n'ont vocation à remplacer la protection juridique accordée par le droit de la propriété intellectuelle et ceci pour deux raisons.

Tout d'abord, la protection des mesures techniques demeure indissociable de la protection des œuvres de l'esprit. En effet, en case de neutralisation de dispositifs techniques, les sanctions ne semblent encourues que si la neutralisation vise l'accomplissement d'un acte non autorisé par les titulaires de droit ou interdit par la loi. Le considérant 47 de la directive du 22 Mai 2001 fait référence aux mesures techniques destinées à empêcher ou à limiter les actes non autorisés par les titulaires de droits. Les exceptions au droit exclusif ne devraient pas être considérées comme des actes non autorisées. Selon l'article 122-5 du CPI , *lorsque l'œuvre a été divulguée, l'auteur ne peut* interdire les exceptions au droit d'auteur, notamment *les représentations privées et gratuites effectuées exclusivement dans un cercle de famille.* Un auteur ne peut donc faire des exceptions reconnus par la loi des actes non autorisées. Ainsi la neutralisation d'un système de protection numérique ne semble pas pouvoir être sanctionné en tant que telle. Ceci est contraire aux dispositions relatives aux intrusions dans les systèmes informatiques suivant les articles 323-1 et suivants du Code Pénal.

Ensuite, les règles de protection du droit d'auteur et des droits voisins doivent être maintenues compte tenu de l'efficacité très relative des systèmes de protection. Nous savons bien qu'en théorie les dispositifs techniques de protection sont très efficaces, d'ailleurs un utilisateur moyen ne peut pas les contourner. Mais il faut tenir compte du fait que la propagation des solutions se fait très vite du niveau individuel ou niveau collectif. Pour un exemple, le systèmes SDMI a partiellement été mis en défaut alors qu'il était réputé infaillible.

Ainsi, tant que les moyens techniques ne permettront pas de contrôler le phénomène de la copie privée, le système de licence légale constituer la solution pour les titulaires de droits. Les systèmes de DRM permettent par ailleurs de rapprocher auteur et consommateur.

Aujourd'hui les dispositifs techniques empêchant la reproduction non autorisée et les mesures relatives au marquage des œuvres numérisées rendent possible le contrôle des utilisations. Internet se présente aujourd'hui comme un système de distribution d'oeuvres numérisées. Au fond la licence légale avait été instituée à cause de l'impossibilité de faire respecter le droit exclusif de l'auteur sur sa création. Des considérations matérielles et pratiques faisaient qu'il était impossible de mettre en présence des interlocuteurs identifiables pour faire respecter le droit exclusif dans la sphère privée.

# 6. .CONCLUSION

En conclusion, voilà une quinzaine d'années que les technologies dites de tatouage watermarking permettent de protéger le droit d'auteur contre les copies illicites. Une application de ces techniques pourraient servir à établir un dialogue plus fiable entre les avocats et les juridictions lors des communications des pièces de procédure. Selon Georges Chatillon (dans l'administration électronique au service des citoyens, page 239) les pièces pourraient être tatoués par les avocats et relus avec des clés par les juridictions. Pourtant ces techniques sont souvent considérées comme complexe à utiliser. Selon Jean-François Théry, Président de Section au Conseil d'Etat, (dans l'administration électronique au service des citoyens, page 240) *cette technique est peu utilisée et reste extrêmement compliquée.*

Pourtant ces techniques de marquage des œuvres font l'objet de recherche et développement dans le monde entier. L'enjeu de la maîtrise de l'utilisation des œuvres par des moyens techniques est considérables pour le développement du commerce électronique. Lorsque la marque ajoutée à l'œuvre sera capable de résister à un traitement ou une attaque de données quelconques, la stéganographie aura atteint sa maturité. Elle sera alors à la base de nouveaux systèmes sécurisés où les utilisateurs sont identifiés, les actions sont enregistrés dans un environnement sécurisé de confiance, les systèmes de DRM.

On entend de plus en plus parler de "DRM" (Digital Rights Management, gestion des droits numériques) ce derniers temps. Du Palladium de Microsoft à la décision récente de Radio France d'émettre en ligne uniquement au format Windows Media Player, en passant par la sortie d'albums illisibles sur les ordinateurs, la question des droits numériques occupe aujourd'hui une place centrale dans l'évolution de l'informatique, et est l'objet de nombreuses fausses idées, qui tendent à dénaturer le débat
C'est le moins que l'on puisse dire. Parler aujourd'hui de DRM, c'est rappeler à certains qu'ils ne peuvent lire avec leur ordinateur un CD légalement acheté, qu'ils ne peuvent pas l'importer pour l'écouter sur leur iPod, quand on n'en appelle pas au manque respect de la vie privée, soupçonnant certaines compagnies mal intentionnées de regarder d'un peu trop près le contenu des disques durs...
Dans le domaine de la musique, les majors ont tenté en effet réglé la question en mettant sur le marché des CDs bénéficiant d'une protection qui les rend tout simplement illisible sur un PC. La présence discrète d'un logo au dos du CD est censée prévenir le consommateur qui, s'il souhaitait ripper le CD en mp3 pour son lecteur, ou tout simplement écouter le CD sur son ordinateur, doit passer son chemin.

Ce système, qui n'est qu'un exemple de DRM parmi d'autres, est malheureusement le premier contact (et le principal) avec la gestion des droits numériques pour de nombreux utilisateurs. Ceci explique sans doute qu'il est difficile d'aborder le sujet avec calme et sérénité. Ajoutons à cela l'initiative Palladium, qui, si on l'observe avec un regard pessimiste, ne laisse présager rien de bon pour les libertés individuelles, et on comprend aisément que les DRM sont perçu au mieux comme une nuisance, au pire comme l'expression d'un complot visant à empêcher l'honnête utilisateur de jouir de ce qu'il a acheté.

Il doit pourtant être possible d'évoquer cette question en comprenant quelques

éléments essentiels. Les DRM sont partout. Les sharewares qui cessent de fonctionner au bout d'un certain temps si la licence n'est pas payée constituent une forme de gestion des droits : l'auteur d'un programme tient à garder un certain contrôle sur son oeuvre. Dans un cadre plus général, la signature électronique des documents est aussi un système de gestion des droits (qui se rapproche alors plus de la sécurité).

Sans rejeter sur les grandes maisons de disque le responsabilité du blocage, il convient de comprendre qu'il est important pour ces maisons de protéger leur investissement, fût-il de qualité artistique discutable...

C'est un fait : la production d'oeuvres numériques s'épuisera si leurs auteurs ne sont pas protégés, par divers dispositifs adaptés. Aujourd'hui, indépendamment des gains réalisés par ailleurs, on peut comprendre l'agacement des majors qui voient les albums de nombreux artistes disponibles en téléchargement illégal avant même la sortie officielle du disque. Néanmoins, la colère de l'acheteur d'iPod qui ne peut pas écouter un CD acheté sur son lecteur MP3 parce qu'une multinationale de la musique l'a décidé est tout aussi légitime.

Aujourd'hui, non seulement les utilisateurs sont loin d'être emballés par l'idée d'utiliser des systèmes de DRM, mais Apple en a presque fait son cheval de bataille. La première offensive fut la campagne "rip, mix, burn" ("encode, mixe, grave"), qui, bien qu'accompagné d'un message appelant à ne pas "voler la musique", était complètement explicite (et a d'ailleurs valu à Apple un rappel à l'ordre). La position officielle d'Apple sur le sujet de la gestion des droits numérique a été rappelée par Phil Schiller à l'occasion de la controverse Palladium : "notre attitude est de protéger les droits des utilisateurs". Apple laisse l'utilisateur décider de l'utilisation qu'il fera de son iPod, par exemple, et n'y a donc pas intégré de DRM (la solution retenue consiste à cacher les fichiers mp3). De même aujourd'hui, ni Quicktime, ni iTunes n'intègrent de système logiciel de DRM.

Mais cette situation semble difficile à tenir. En effet, la question de l'ajout d'un système de DRM se pose cruellement pour Quicktime. La décision récente de Radio France le rappelle. La radio publique française a décidé de n'émettre en ligne qu'au format Windows Media player, arguant que ce système était celui lui offrant les meilleures garanties de protection de l'oeuvre émise. Le revers est symbolique pour Quicktime dans ce cas précis, mais d'autres exemples récents vont de ce sens : des offres pour télécharger des albums ont vu le jour, qui ne fonctionnent là encore qu'avec Windows Media Player, car elles reposent sur son système de gestion des droits. Même si cela semble paradoxal, l'adoption d'un système de DRM semble inéluctable pour Apple. Comme le montrent les travaux même du MPEG4-forum, l'ajout d'une couche de gestion des droits a été prévue dès le début du travail sur le format. Le schéma détaillant l'architecture du MPEG4 présente donc une intriguante couche censée gérer la propriété intellectuelle du document.

Les systèmes de DRM apparaissent donc comme nécessaire mais le droit devra trouver le juste milieu dans la protection juridique des mesures de protection.
Le droit de la propriété intellectuelle doit donc s'adapter à ce nouvel environnement. Le droit international et le droit communautaire se sont déjà adaptés pour offrir une protection à ces nouvelles techniques. Les Etats membres ont déjà dépassé le délai de transposition de ces mesures dans leur droit national depuis le 22 décembre 2002. Ainsi les nouvelles technologies du numérique ont bouleversé la notion classique de

reproduction, en définissant par exemple une nouvelle exception applicable aux reproductions provisoires et peuvent être une menace pour nos libertés fondamentales.

Aujourd'hui la question est celle de la transposition en droit français la directive européenne. Est-ce que le droit de la propriété intellectuelle doit être modifié à cette occasion. Savoir si les mesures techniques doivent être protégées par le droit de la propriété intellectuelle et donc la contrefaçon est l'objet d'un débat à propos de la transposition en France de la directive du 22 mai 2003.. . Certains pensent que le droit civil peut protéger les mesures techniques. A cet égard, le contrat, la concurrence déloyale, la fraude ou même l'abus de droit sont loin d'avoir livrés tous leurs secrets. Mais, avant d'explorer les pistes du droit commun, il est impératif de déterminer avec précision les frontières du monopole de l'auteur. Dans ce débat il faudra alors se rappeler les propos visionnaires que le Doyen Savatier tenait, en 1959, à propos du droit d'auteur : « ce n'est pas à la personne humaine d'être l'esclave des techniques ; c'est à elles de servir l'homme ».

# 7. [1] BIBLIOGRAPHIE


## OUVRAGES

-P.Y.Gautier, Propriété littéraire et artistique, PUF, 4e Edition mise à jour
-G.Chatillon,B. du Marais, l'Administration électronique au service des citoyens
-A.Hollande, X.Linant de Bellefonds, Pratique du droit de l'informatique
-X.Linant de Bellefonds, Droits d'auteur et droits voisins PLA, Delmas
B.Edelman, La propriété Littéraire et Artistique
F.Asseraf-Olivier,E.Barbry, Le Droit du multimédia, PUF
D.Lecomte, Les normes et les standards du multimédia, Dunod informatique
JEAN Frayssinet, Informatique fichier et libertés

## ETUDES, RAPPORTS ET COLLOQUES

Internet et les réseaux numériques, Etude du Conseil d'Etat, Edition de la Documentation française, 1998
Gabriel de Broglie, Le droit d'auteur et l'internet, PUF
Valérie Laure Benabou
Isabelle Vaillant
Le livre vert de la Commission européenne sur le droit d'auteur et les droits voisins dans la société de l'information de juillet 1995

## MAGAZINE SPÉCIALISÉE

Zdnet

## ARTICLE

V-L Benabou, La directive droit d'auteur, droits voisins et société de l'information : valse à trois temps avec l'acquis communautaire Revue Communication-Commerce electronique

## RÉFÉRENCES INTERNET

Textes officiels: www.legifrance.gouv.fr
Site gouvernemental Français: www.internet.gouv.fr
Sacem: www.sacem.fr
La journal du net: www.journaldubet.fr
Site juridique: www.legalis.net
INPI: www.inpi.fr
Legifrance: www.legifrance.fr
OMPI: www.ompi.int


1

# 8. ANNEXES

## -ANNEXE: SIGNATURE D'UNE OEUVRE NUMERIQUE

L'INA a développé un système de signature sémantique pour les images et les vidéos. Ce système permet une reconnaissance automatique des oeuvres, ce qui facilite leur identification. Il peut être utilisé à des fins de traçabilité des oeuvres, c'est-à-dire du suivi de leur diffusion. De même, l'IRCAM a développé un système de signature statistique pour les oeuvres sonores.

# ANNEXE DISTRIBUTION SUR SUPPORT OPTIQUE D'OEUVRES MUSICALES.

L'essentiel du piratage numérique dans le domaine musical tient à l'absence native de mesures techniques de protection appliquées aux CD Audio, notamment par comparaison au format du DVD qui comporte la mesure technique de protection qu'est le CSS (*Content Scrambling System*). Le lancement de nouveaux supports audio numériques peut être l'occasion de combler cette différence entre le secteur de l'audio et du cinéma. Cependant, si le standard DVD devait s'imposer pour le cinéma comme pour l'audio, il n'est pas certain que cet écart demeure. En pratique, cela signifierait que la copie numérique audio resterait aisée, tandis que la copie numérique d'oeuvres audiovisuelles et cinématographiques resterait –principalement et techniquement – très limitée voire impossible.

***1982: Les vidéodisques*** apparaissent. Ils mesurent entre 20 et 30 centimètres de diamètre. Même si la lecture est effectuée par un faisceau laser, le signal est de type analogique. Les vidéodisques ont connu un succès très limité.

***Le vidéo CD*** est un format qui a été défini par le Livre blanc publié par *Philips*, *Sony*, *JVC* et *Matsushita* en 1993. Ce standard permet de stocker 72 minutes de données vidéo sur un CD Audio, mais avec une qualité de restitution qui reste inférieure en pratique à celle obtenue avec une cassette VHS (les données sont compressées selon la technique MPEG-1).

Ce format n'a pas été retenu pour la distribution des oeuvres audiovisuelles.

***– Le CD Audio : un format nativement non sécurisé.***

*Sony* et *Philips* sont à l'origine de la distribution de la musique sous forme numérique.–**1980: CD Audio,** dont la capacité utile est de 750 Mo, à travers le système de codage et les procédures de corrections d'erreur ;

–**1984:** le **Cédérom**, dont la capacité utile est de 650 Mo pour prendre en compte l'intérêt du CD Audio comme mémoire
amovible de stockage pour les ordinateurs personnels qui commencent à se répandre ;

–**1990:** , définit le standard des disques inscriptibles et réinscriptibles : si la plupart des CD Audio sont de type « lecture seule » et ne
peuvent être « écrits », un **CD-R** (*Recordable*) est un Cédérom enregistrable une seule fois, le cas échéant en plusieurs fois (multisession) tandis que le **CD RW** est un Cédérom réinscriptible jusqu'à mille fois.

Le standard du CD Audio ne prévoit nativement aucun système de protection de l'oeuvre. Normalement, tout lecteur peut accéder aux données, et les transmettre vers un graveur ou un ordinateur, sans avoir besoin de demander les droits sur l'oeuvre. De plus, ce standard laisse aux industriels une très faible marge de manoeuvre pour mettre en place des systèmes d'accès ou de protection contre la copie Ils sont donc obligés d'inscrire les mesures techniques à la frontière de la

norme, allant parfois au-delà. Les écarts avec la norme qui en résultent sont à l'origine des problèmes de « jouabilité » des supports optiques, c'est-à-dire de compatibilité entre les CD Audio protégés et certains lecteurs, notamment des lecteurs de CD Audio dans les autoradios. Dans ce contexte, les standardssuccessifs du CD Audio conduisent à exclure du sein d'un système numérique de gestion de droits la distribution des contenus numériques musicaux sous formes de CD Audio.

***– Le Super Audio Compact Disc (SACD) : standard nativement sécurisé.***

Ce standard, développé par *Philips* et *Sony* cherche à supplanter le CD Audio en offrant aux auditeurs des avantages qualitatifs très supérieurs et aux titulaires de droits un système de protection contre la copie. Cependant son développement commercial ne décolle pas.

***Un standard pour une qualité de haute définition***. Les avantages du SACD du point de vue de la haute définition sonore tiennent à trois caractéristiques principales :

**– Des avantages de qualité et de pureté de la restitution sonore grâce à un**

**procédé d'enregistrement** : le DSD *(Direct stream digital)* plus efficace que le PCM (*Pulse Code Modulation*).

(112)

**– Un enregistrement *multi-channel*** jusqu'à 6 canaux équivalents aux bandes-son du DVD pour créer une ambiance « *Surround* » réalisée par six haut-parleurs : trois devant (à gauche, au centre et à droite), deux derrière (à gauche et à droite) plus un caisson de basses optionnel.

- **Un format de haute définition qui ne diminue pas l'offre de titres** puisque la précision de gravure étant plus fine, le stockage d'informations (4,7 Go) est plus élevé que celle d'un CD Audio (780 Mo).
- Les filtres utilisés pour l'enregistrement garantissent une plus grande fidélité et la fréquence d'échantillonnage (nombre d'enregistrements du signal sonore par seconde) est égale à 2,82 GHz contre 44,1 MHz pour le CD, les hautes fréquences ne sont donc plus

perdues. Enfin le SACD apporte une innovation en matière de dynamique (écart entre le son le plus bas et le son le plus fort), celle-ci est égale à 122 dB pour un enregistrement SACD, contre 96 dB pour enregistrement CD.

La protection technique du SACD et sa robustesse relèvent d'une solution essentiellement cryptographique. Les données audio sont enregistrées sur le support de façon cryptée. Le procédé physique de gravure est en revanche le même que pour enregistrer un CD Audio classique, mais les données numériques

ne peuvent être interprétées que si on possède la clé de décryptage. Cette clé comporte une partie commune à tous les disques SACD et une partie propre à chaque titre. La partie commune se trouve dans les lecteurs SACD, inscrite physiquement dans la puce de lecture. La partie propre au titre est inscrite sur le disque par un procédé de gravure spécifique.

De plus, les données d'en-tête d'un disque SACD sont cryptées et

inscrites avec le même procédé de gravure spécifique. Ces données indiquent le nombre de pistes, leur durée et leur position sur le disque, elles sont indispensables à la lecture. La clé et les données d'en-tête, imprimées sur le disque de façon inhabituelle, constituent un « filigrane » (la clé de décryptage se trouve inscrite en dur sur la puce de lecture d'un lecteur SACD). La robustesse de la protection technique est fondée sur le cumul de plusieurs types de sécurité et notamment la licence. En premier lieu, un SACD ne peut-être utilisé sur un lecteur dépourvu de licence. Son utilisation requiert la lecture des données d'en-tête qui, étant gravées sur le filigrane, ne peuvent pas être lues avec un lecteur ordinaire de CD Audio. Ces données d'en-tête sont cryptées et donc inutilisables si l'on ne dispose pas d'un lecteur SACD muni d'une licence. En second lieu, si un SACD est copié avec un enregistreur en vente libre, il ne fonctionnera pas. En effet, les enregistreurs CD Audio que l'on trouve sur le marché n'ont pas la capacité de graver le filigrane caractéristique des SACD.
Or, les enregistreurs SACD produits exclusivement par *Philips* et *Sony* ne devraient être que l'objet d'une location aux professionnels et jamais mis à la vente. Enfin, dans tous les cas, les données audio restent cryptées, par conséquent sans la clé inscrite pour une partie sur le filigrane du SACD et pour l'autre sur la puce de décodage d'un lecteur, les données audio sont illisibles. La clé utilisée mesure 80 bits et n'apparaît jamais de façon explicite sur un bus de données à l'intérieur d'un lecteur. L'algorithme de chiffrement est gardé secret et il est implanté en dur ce qui rend impossible une tentative de rétro-conception.
Ainsi, le piratage d'un SACD nécessiterait de lourdes infrastructures.
**Les lecteurs de SACD.** Tous les lecteurs SACD mis sur le marché permettront de lire les CD Audio ordinaires, afin que les utilisateurs puissent continuer à utiliser ceux qu'ils possèdent. Chaque lecteur SACD possède deux émetteurs lasers, un à 780 nm pour lire les CD Audio traditionnels et un à 650 nm pour lire les SACD.
**Les lecteurs CD Audio.** Un lecteur CD Audio ne peut pas lire un disque SACD, en effet il lui manque entre autres éléments, un émetteur laser à 650 nm, la technologie pour lire le filigrane, les clés de décryptage et la puce de lecture spécifique. Il est inconcevable de faire évoluer simplement un lecteur CD Audio vers un lecteur SACD, les utilisateurs doivent donc acheter un nouvel équipement.
**Les lecteurs hybrides.** Certains éditeurs mettent sur le marché des CD Audio hybrides qui sont compatibles à la fois avec les lecteurs CD Audio et les lecteurs SACD. Toutefois un CD Audio hybride lu avec un lecteur CD Audio ordinaire ne permet de bénéficier ni de la qualité sonore du SACD ni du *Surround*. Il peut également être piraté très facilement.
(
PSP (*Pit signal processing*) : la largeur du sillon et non plus seulement la profondeur est porteuse d'informations.
Obtention de l'algorithme de cryptage par une lecture des instructions envoyées au processeur à l'intérieur du lecteur SACD.
**La commercialisation du SACD depuis plusieurs années traduit**

**de réelles**
**difficultés** qui tiennent à trois éléments : l'étroitesse du catalogue (moins de 200 titres disponibles dont la moitié bénéficie de l'enregistrement en Multi-channel*Surround*), l'écart de prix entre SACD (~20€) et CD Audio (~15€), enfin le coûtdes lecteurs SACD (~250 €) dont la gamme est encore réduite en sorte que le lancement du SACD reste dérisoire : ~ 6 600 lecteurs SACD ont été vendus dans le monde en 2001. L'échec commercial pour le moment constaté tient en réalité beaucoup aux choix des standards techniques – incompatibles – proposés aux *majors* entre le SACD et le DVD-Audio (DVD-A). L'incertitude pèse autant sur la formation d'un catalogue attractif que sur les attitudes d'attente des consommateurs.

– ***Le DVD-A : un standard nativement sécurisé.***

Le DVD audio est le standard DVD Audio publié par le Forum DVD en 1990..*BMG Entertainment*, *EMI Music*, *Universal Music* et *Warner Music* se sont engagés à éditer des DVD Audio. Une entreprise similaire a été conduite par le DVD Forum, conduisant à la publication de la norme DVD-Audio en 1999, révisée en 2000 pour tenir compte du fait que le système de protection des DVD ait été cassé.

Au sens de la norme, un DVD-Audio ne peut en général pas être lu sur un lecteur DVD-Video. La plupart des DVD Audio mis en vente sont cependant compatibles avec les lecteurs de DVD Video, ils présentent alors le même niveau de sécurité que les DVD Vidéo, c'est-à-dire qu'ils peuvent être copiés en utilisant un lecteur DVD d'ordinateur. De plus, contrairement aux films, les extraits sonores peuvent circuler facilement sur les réseaux *peer to peer* car leur taille est plus modeste. Les DVD-Audio non compatibles avec les DVD-Video, donc plus robustes, sont protégés grâce la technologie CPPM (*Content Protection for Precorded Media*) développée par le consortium « 4C entity » Il cherche à partir d'un cadre de sécurité de la plupart des contenus numériques (CSPA) à établir des technologies de protection du DVD A. La technologie CPPM remplace la technologie CSS2 qui était initialement prévue pour le DVD-Audio avant que CSS ne soit cassé.

Elle est plus robuste, notamment au niveau de la gestion des clefs, mais reprend les concepts fondamentaux de CSS. La « guerre des standards » entre SACD et DVD Audio ralentit considérablement la pénétration des nouveaux équipements, comme ce fut le cas lors de la compétition entre VHS et Betacam. En effet, SACD et DVD Audio étant incompatibles, les consommateurs préfèrent attendre que l'un d'entre eux atteigne une position dominante avant d'investir dans un nouvel équipement. Fin 2002, les industriels ont commencé à mettre sur le marché des lecteurs capables de lire à la fois les SACD et les DVD Audio. Cette nouvelle donne devrait accélérer l'extension du parc de lecteurs capables de lire des supports optiques pour la musique protégée.

Même si la distribution d'une oeuvre est réalisée sur supports optiques, il est possible de la coupler avec un système en ligne de gestion des droits. Dans un tel système, les droits présents sur le support optique sont réglés lors de l'achat du support, ils permettent de déchiffrer une partie des oeuvres présentes sur le

disque. Pour accéder aux autres œuvres présentes sur le disque, il faut télécharger en ligne d'autres droits grâce à un système classique de DRM, comme celui de *Microsoft*. Cette idée a été exploitée lors de la diffusion gratuite d'un single du groupe *Oasis* à l'intérieur du *Sunday Times* en Angleterre. Les droits présents sur le disque permettaient d'écouter le titre une seule fois. Afin de l'écouter à volonté, il fallait acheter en ligne des droits supplémentaires. De même, le dernier album de *Daft Punk* est livré avec un code qui permet, en se connectant en ligne à un serveur de droits, d'avoir accès à des oeuvres supplémentaires.

## ANNEXE Distribution sur support optique des oeuvres audiovisuelles.

Le standard DVD a été créé en 1995 par le consortium DVD qui regroupe 10 entreprises. En fonction du nombre de couches, la capacité d'un DVD varie entre 4,7 Go et 17 Go, ce qui est suffisant pour enregistrer un film entier avec une excellente qualité d'image et un son multicanal.

Les principales protections prévues par la norme DVD sont les suivantes :

– Le « système *Macrovision* », qui fait en sorte que le signal vidéo analogique émis par un lecteur DVD ne soit pas enregistrable sur une cassette VHS ;

– Le système de protection CSS (*Content Scrambling System*) qui consiste à
chiffrer les données.

Aujourd'hui il est possible de télécharger sur Internet des « *rippers* » de DVD, c'est-à-dire des logiciels capables de déchiffrer un DVD et d'inscrire en clair le contenu de l'oeuvre sur un autre support. On peut remarquer que le premier « *ripper* » a été écrit après la décompilation d'un logiciel de lecture de DVD, livré avec un lecteur de DVD pour ordinateur personnel. On peut s'interroger si le système CSS aurait été cassé si aucun lecteur DVD pour PC, nécessairement accompagné d'un pilote donc d'un lecteur logiciel, n'avait été mis en vente. L'impact de ce piratage est toutefois resté assez limité, dans la mesure où les réseaux d'échange ne sont encore ni assez rapides ni assez ergonomique pour permettre le téléchargement de film, et où les graveurs de DVD-ROM restent encore assez chers.

**ANNEXE: solutions de protection sur supports optiques.**

*Windows Media Player* est un exemple de solution logicielle, moyennement robuste, mais techniquement facile à mettre à jour. La durée de vie, en termes de sécurité, d'un protocole de transmission de la clef privée est supérieure au temps que mettent les équipes de développeurs de *Microsoft* pour concevoir le système suivant. Par conséquent, chaque fois qu'une faille de sécurité du système *Windows Media* est exhibée, *Microsoft* peut diffuser immédiatement sur Internet une nouvelle version du lecteur *Windows Media Player* qui résout le problème. L'opération est transparente pour les utilisateurs, qui tout au plus doivent confirmer leur accord au sujet de cette mise à jour.

Au-delà de la simple mise à jour des lecteurs logiciels en réponse à la découverte de failles de sécurité, la connexion bidirectionnelle des lecteurs logiciels avec un serveur de droits autorise d'autres applications de protection du droit d'auteur. Il est ainsi possible de concevoir un système où les lecteurs installés sur les ordinateurs sont capables de détecter les oeuvres piratées stockées sur les disques durs de ces ordinateurs, et procèdent à leur effacement. Inversement, les solutions matérielles, par exemple les décodeurs de la télévision numérique à péage, sont plus robustes. Mais il est plus coûteux de modifier le système de protection, puisqu'il faut envoyé à chaque abonné une nouvelle carte à puce.

## ANNEXE Les titulaires de droits

Si c'est généralement l'auteur qui est titulaire des droits sur une œuvre au moment de la création, il arrive aussi qu'en raison d'une relation juridique, par exemple dans le cadre d'un contrat de travail ou de louage de services ou d'ouvrage, la titularité des droits ne revienne pas à l'auteur. La question se complique dans le cas d'un film ou d'une pièce de théâtre, où il peut y avoir d'autres titulaires (par exemple producteurs, artistes interprètes ou exécutants). En outre, la cession du droit d'auteur est courante (par exemple d'un auteur à un éditeur, ou entre éditeurs). Le système de gestion électronique du droit d'auteur doit savoir qui détient le droit d'autoriser l'utilisation d'une œuvre en tout ou partie à un moment donné et, éventuellement, qui a droit à une partie des redevances.

**ANNEXE : L'IRCAM : UN EXEMPLE DE MARQUAGE**

L'outil développé par l'IRCAM (Institut de Recherche et Coordination Acoustique/Musique) permet de calculer pour chaque oeuvre sonore une signature. Ainsi un exploitant du système peut constituer une base de données de signatures, et utiliser cet outil comme un mécanisme d'identification des oeuvres en effectuant des comparaisons de signatures. La signature d'une oeuvre est calculée en fonction de données statistiques extraites du signal. Le système est particulièrement sensible, ainsi il est capable de faire la différence entre deux interprétations d'une même oeuvre. Cette sensibilité peut toutefois être gênante lorsque l'outil est utilisé pour opérer une reconnaissance automatique des oeuvres. Ce système d'identification peut être utilisé pour des applications de mesures d'audience. Il permet en effet d'obtenir de façon automatique des listes de diffusions correspondant à ce qui passe à la radio, à la télévision et dans les boîtes de nuit. Associé à une technologie de « web monitoring » il permet de collecter des informations sur l'offre musicale sur Internet, sur les goûts des utilisateurs et la proximité culturelle de certains morceaux.

En revanche, un tel système pourrait difficilement être utilisé comme un moyen de protection contre la copie.

## 8.1. ANNEXE TCPA/PALLADIUM

En tant que tel et à ce jour, il pourrait ne pas poser de problème sur ce dernier point. Fondé sur une option d'opt-in et des fonctions d'anonymisation, TCPA permettrait aux utilisateurs de protéger les fichiers placés sur leurs ordinateurs, en rendant par exemple impossible leur lecture sur d'autres ordinateurs.

Les craintes exprimées quant à la possibilité d'utilisation de TCPA pour recueillir des informations sur les individus, voire les surveiller, sont infondées tant qu'il n'est pas question de mettre en place un serveur centralisé qui fédérerait l'ensemble du système . TCPA met à disposition des utilisateurs des fonctions de sécurité, qui peuvent être utilisées en mode local, sans qu'une autorité centrale soit informée des opérations. Le fait que chaque puce TCPA, située au sein de chaque ordinateur soit dotée d'un numéro d'identification unique, ne soulèverait alors pas nécessairement de problème, mais à la condition expresse que l'utilisateur puisse, s'il le souhaite, et librement, désactiver tout usage de l'identifiant de puce, un tel choix ne devant pas non plus donner lieu à la constitution d'une quelconque base de données de données nominatives. Il faut toutefois noter Que. cette condition renverserait les principes du droit européen du respect de la vie privée. En réalité, il conviendrait – a priori – qu'il n'y ait pas de fichier de données personnelles, sauf si l'utilisateur l'admet en bénéficiant des conditions d'informations nécessaires.

Le projet de Microsoft « Palladium » rebaptisé « Next Generation

Secure Computing Base » a été reconfiguré quant à ses objectifs initiaux qui tendaient à accroître les fonctionnalités du système d'exploitation Windows en terme de sécurité.

Les nouvelles fonctionnalités intéressant notamment les professionnels reposeraient sur des composants matériels et logiciels et tendraient à accroître la sécurité des ordinateurs personnels, notamment en garantissant la confidentialité des fichiers. La gestion numérique des droits et Palladium sont deux technologies indépendantes, l'une pouvant fonctionner sans l'autre.

Cependant, il existe une forte synergie entre elles. Si Palladium était installé sur les ordinateurs des particuliers, il pourrait renforcer de manière très significative les systèmes de DRMS, en premier lieu celui protégeant le logiciel d'exploitation Windows. Cependant, dans une telle hypothèse, Palladium pourrait — par effet de bords — sécuriser d'autres services, y compris des services libres de droits ou mettre en difficulté l'interopérabilité du système d'exploitation et de sécurité avec certains logiciels. Comme d'autres systèmes centralisés (Windows Media Player par exemple, en ce qui concerne la consommation d'oeuvres sécurisées) Palladium pourrait présenter des risques de centralisation de données nominatives. Toutefois, les fonctionnalités de sécurité nouvellement au centre de Next Generation Secure Computing Base devraient se distinguer des DRMS de Microsoft, notamment de Microsoft Windows Rights Management Services (RMS).

## ANNEXE : LES SYSTEMES SDMI ,ATM, MACROVISION

Classiquement, on peut distinguer deux sortes de systèmes de protection : les systèmes permettant d'empêcher la reproduction non autorisée des oeuvres protégées et les systèmes de protection permettant le marquage des oeuvres numériques.

Les premiers systèmes offrent la possibilité d'interdire ou de limiter les copies réalisées à partir de supports. Le système " Watermark ", mis au point par la Secure Digital Music Initiative (SDMI) est ainsi destiné à empêcher la piraterie musicale. Dans ce cas, la protection des fichiers repose sur l'altération du signal audio. La copie de l'oeuvre devient alors inutilisable. Les seconds systèmes ne préviennent pas *a priori* les actes de contrefaçon. Le marquage des oeuvres numériques a pour fonction de prouver la violation des droits des titulaires et d'inciter les utilisateurs à respecter les droits exclusifs. Ce procédé inscrit sur l'oeuvre une sorte de tatouage numérique sur lequel figure des informations sur l'origine de la création, les noms des titulaires des droits sur celle-ci, ou bien encore les utilisations autorisées. Ainsi, l'Audiosoft Tracking Master (ATM) est un logiciel qui piste la musique sur les réseaux numériques. Implanté aux deux extrémités de la chaîne (sur les serveurs et les lecteurs), il détermine l'audience des oeuvres protégées, mais surtout la destination de toutes les transactions musicales. Mais le système ATV n'a pas pu se développé. La société Audiosoft a disparu début 2003. Son ancien dirigeant, Alexandre Saltiel, évoque l'illusion sur laquelle reposent Pressplay et Musicnet, les projets de distribution musicale payante imaginés par les majors. *« Dans le climat actuel, ces services ne seront pas rentables avant au moins 5 ans ; il s'agit surtout de marketing, mais tant que des systèmes gratuits de type Kazaa ou Audiogalaxy existeront, je ne crois pas que les consommateurs seront prêts à payer pour écouter de la musique sur le net.*

Ces systèmes de protection sont des systèmes de protection contre la copie privée numérique. Cependant, il existe également des systèmes de protection permettant d'empêcher la reproduction analogique. A titre d'illustration, le système " macrovision ", qui protège les cassettes vidéo destinées à la location et à la vente, est un procédé qui brouille la commande automatique " gain control " du magnétoscope lorsque celui-ci est en train de reproduire une cassette à partir d'un enregistrement VHS ou S-VHS. La copie obtenue ne peut être visionnée tant sa qualité est médiocre. Si ce système s'avère très efficace, il demeure une exception. De manière générale, les systèmes de protection empêchant la reproduction analogique demeurent peu performants en comparaison des systèmes de protection numériques. Surtout, ils n'offrent pas les propriétés de contrôle, de marquage et d'identification que garantissent les systèmes de protection numériques. Or, ce sont ces propriétés qui remettent en cause le système de licence légale car les titulaires de droits sont désormais en mesure d'autoriser ou d'interdire la reproduction de leurs oeuvres dans la sphère privée et de fixer éventuellement le montant de la contrepartie financière.

## ANNEXE : LES SYSTEMES SDMI ,ATM, MACROVISION

Le projet rassure les maisons de disque mais inquiète les défenseurs de la protection des données personnelles. Le système d'Apple est un système de DRM avec double identifiant couplé à une base de données centrale fichant chaque client. L'iTunes Music Store, la plate-forme payante de téléchargement d'Apple, est doté d'un système de gestion des droits numériques (DRM). Les procédés d'identification et de traçage stricts des fichiers sont des solutions propriétaires.

Ainsi un même fichier ne peut être copié que sur trois Mac différents et une "playlist" (liste de titres) ne peut pas être gravée plus de dix fois (ou alors il faut changer l'ordre des morceaux). Comment fonctionne ce système? La firme de Steve Jobs s'est basée sur la technologie DRM intégrée au format des fichiers qu'elle a retenue pour son iTunes Music Store: l'AAC (Advance Audio Codec). Développé par l'américain Dolby Laboratories, ce format est également le coeur audio du Mpeg4. Tous les morceaux ont ainsi l'extension ".m4p", le "p" signifiant protected. Ce marquage permet ainsi d'identifier de manière unique tout morceau téléchargé.

Le système d'Apple a également recours à deux identifiants pour associer chaque morceau à un utilisateur et une machine.

Le premier est "l'Apple ID", l'identifiant de chaque client des services en ligne d'Apple - du support technique à l'Apple Store en passant par le bouquet de services ".Mac" (messagerie, stockage en ligne, etc.).

Le second identifiant est l'"adresse MAC" de l'ordinateur qui permet de reconnaître chacune de nos machines en ligne. Il s'agit en fait de l'identifiant de connexion au réseau internet de chaque carte Ethernet (ou adresse MAC (Media Access Control Address), a ne pas confondre avec l'abréviation Mac pour Macintosh), intégrée d'origine à la carte mère des ordinateurs Macintosh.

Quand un morceau est téléchargé, une base de données centrale est renseignée. Apple sait alors qui transfère quoi et sur quel ordinateur. Si par la suite, l'utilisateur copie le morceau sur un autre ordinateur, il devra se reconnecter à l'iTunes Music Store pour pouvoir lire ce morceau. Par simple comparaison avec la base de données centrale, Apple autorise ou non l'ordinateur à lire le fichier. Lors de l'inscription chez Apple, pour obtenir son Apple ID, il faut laisser ses nom, prénom, adresse, téléphone, adresse e-mail, jour et mois de naissance, et son numéro de carte bancaire. À ces informations, seront désormais associés les morceaux de musique téléchargés. Apple possèdera donc une base de données très précise, désormais étoffée des goûts musicaux de ses clients.

Par défaut, l'utilisateur recevra ces publicités d'Apple ou de ses partenaires selon le principe de "l'opt-out" en opposition à "l'opt-in", pourtant vivement recommandé par la Commission de Bruxelles S'il ne le souhaite pas, il doit donc décocher une case spécifique du formulaire d'inscription. Bref, le système d'Apple n'a rien à envier au service d'authentification en ligne Passeport de Microsoft, qui avait été vivement décrier par les défenseurs des libertés individuelles. Les mécanismes d'identification de l'utilisateur.mis en place par Apple sont dangereux. si quelqu'un viole le système Apple et vole les Apple ID. Mais le risque est identique avec d'autres logiciels. Par ailleurs, sans cette technique, les majors de musique n'auraient sans doute pas accepté un accord avec Apple.

# 9. GLOSSAIRE

Attaques : Il y a deux types d'attaques des marques :

- celles liées au signal : on ne travaille que sur le medium marqué en essayant de le détériorer assez peu pour que ce ne soit pas perceptible, mais quand même suffisamment pour retirer la marque ;
- les attaques cryptographiques : elles s'inspirent des attaques rencontrées en cryptologie ; elles essayent d'exploiter les faiblesses de l'algorithme ou du protocole mis en place pour définir des méthodes générales pour retirer les marques.

Clé : Une clé est un secret nécessaire pour identifier une marque. Dans les principaux modèles de watermarking, elle permet aussi bien d'inscrire la marque que de la lire ou de l'enlever. C'est pourquoi elle doit rester secrète. Les protocoles mettant en place ce type de marquage à clé symétrique font intervenir l'utilisation de tiers de confiance, gardiens de la clé.

Etalement de spectre : L'étalement de spectre est une technique utilisée dans les télécommunications radio, notamment par les militaires, pour disperser un signal sur une large bande de fréquence, de façon à le rendre discret et résistant aux interférences. On comprend donc que ce modèle est d'application immédiate au watermarking. Pour voir une référence sur l'étalement de spectre dans les télécoms, cliquer

Extraction : Un procédé de marquage fait intervenir deux concepts : le tatouage et l'extraction. L'extraction est l'étape où on retrouve la marque incrustée sur le medium.

Fingerprinting : Le fingerprinting est une application du watermarking dans laquelle la marque (on dit alors l'empreinte) varie d'une personne à l'autre. Dans le cas d'une diffusion de copies illégales, on peut ainsi retrouver la ou les personnes dont l'exemplaire du medium est à l'origine de la fraude.

iPOD : balladeur numérique musical fabriqué par Apple qui peut tenir dans une main et enregister et se connecter au PC pour charger les fichiers MP3(plus d'un million d'exemplaires vendus)

JPEG : Compression d'images, avec perte d'information, fondée sur la DCT(.Discrete Cosine Transform) Elle part du principe que les hautes fréquences sont moins visibles à l'oeil pour les retirer. Une compression JPEG à 50 % laisse l'image visiblement quasi-inchangée. Certains algorithmes de marquage, pour mieux résister à cette compression, inscrivent la marque dans les moyennes fréquences de la DCT, c'est-à-dire dans le domaine encore invisible, mais qui va résister à la compression JPEG.

Luminance : Un en couleur a trois degrés de liberté. Une représentation standard est la représentation (R,G,B) qui fait intervenir les niveaux de rouge, vert et bleu du pixel. Une représentation isomorphe est la représentation (Y,U,V) où Y désigne la luminance du pixel et U et V définissent sa chrominance. Plus la luminance est forte, plus le pixel est clair. La plupart des algorithmes de marquage d'images

travaillent sur la luminance des pixels. Pour ceux-là, on peut tester leur solidité sur des images noir et blanc.

Medium : On désigne par medium toute pièce de données, comme une image, un son, une séquence vidéo.

Pixel : Le pixel (picture element) est la plus petite division d'une image. C'est un point pour l'image.

PRMS: Privacy Rights Management Systems

QuickTime: Logiciel sous Mac ou PC/Windows pour la création multimédia et pour la lecture de contenus audio et vidéo numérique

Stéganographie : La stéganographie est la science qui consiste à cacher de l'information dans un quelconque medium de façon à ce que seul un utilisateur muni du secret adéquat puisse retrouver cette information.

Tatouage : Un procédé de marquage fait intervenir deux concepts : le tatouage et l'extraction. Le tatouage est l'étape où la marque est incrustée sur le medium.

Traçabilité : Cet anglicisme désigne la possibilité de "tracer" un coupable : quand une coalition de taille raisonnable de personnes se mettent d'accord pour casser une sécurité (cryptographique ou de marquage), on veut identifier au moins un des membres de cette coalition.