EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR RESEARCH

WORKING PAPER

Protection and implementation of intellectual property rights in security technologies for digital media

Scientific and Technological Options Assessment Series

STOA 118 EN

EUROPEAN PARLIAMENT

WORKING PAPER

Protection and implementation of intellectual property rights in security technologies for digital media

Scientific and Technological Options Assessment Series

STOA 118 EN

12-2003

This study was requested by the European Parliament's Committee on Industry, External Trade, Research and Energy within the STOA Workplan 2002.

This paper is published in English only.

Authors : Prof. Dr Franck Leprévost
Prof. Dr Bertrand Warusfel
Faculté de Droit de Paris V
F-75001 Paris

Responsible Official : Pernille Winther
Division for Industry, Research, Energy, Environment and STOA
Tel: (352) 4300 22568
Fax: (352) 4300 27720
E-mail: DG4-STOA@europarl.eu.int

Manuscript completed in December 2003

Further information on DG4 publications
can be accessed through : www.europarl.eu.int/studies

Luxembourg, European Parliament, 2003

Printed in Luxembourg

Executive summary

Prof. Dr Franck Leprévost and Prof. Dr Bertrand Warusfel

This study on the 'Protection and implementation of intellectual property rights in security technologies for digital media' was requested by the Scientific and Technological Options Assessment (STOA), on behalf of the Committee on Culture, Youth, Education, the Media and Sport of the European Parliament (restricted invitation to tender No 116741 of 22 July 2002).

The study was based on a previous study by the same authors, entitled 'Security technologies for digital media', also requested by STOA and submitted in May 2001.

Introduction

The present study concerns the protection and implementation of intellectual property rights in security technologies for digital media. Since digital media is a broad concept, the focus of this study is on digital content (sound, pictures or a combination thereof) involving the transfer of value.

What is of interest here is not so much an exhaustive description of detailed technological solutions, but rather an analysis of their generic properties and their classification according to these properties.

One of the major goals of the study was to describe how the choice of certain security technologies and their implementation would affect the structures of business in the information sector (access providers, content providers, copyright associations, etc.), as well as the legal context of access and use of the information resources by consumers (especially in connection with the new 2001 Copyright Directive). It was, of course, necessary to identify the potential standards (which may already be industry standards, and/or standards already delivered by standardisation bodies), and their interoperability.

Conclusions

Analysis of the current available technologies and their uses (detailed in parts A to C of the study) led to the following three conclusions. First, there exists today a technological offer regarding the protection of digital goods. Second, some of the weaknesses of this offer explain in part the low level of use of digital goods. Third, this lack of use explains why these technical possibilities do not have a significant impact on the volume of digital counterfeiting.

The technological offer regarding protection of digital goods

The technologies necessary to construct and exploit digital rights management (DRM) are nowadays available. They mainly make use of cryptographic and steganographic techniques, as well as several methods already used for the security of information systems.

However, these technologies suffer from two main weaknesses, negatively affecting their expansion and use.

First of all, they are not properly standardised and depend on proprietary standards. The standardisation efforts in this area are really quite modest, and are not sufficient to convince the relevant industries to achieve a consensus. For example, the new MPEG4 (ISO/IEC 14496, 1999) norm proposes only a description mode of intellectual rights (IPMP) and security technologies, without standardising the technologies themselves. Similarly, the European Standardisation Committee (CEN) offers a very general and descriptive framework regarding the architectures of DRM, but does not offer a real European norm in this area (see the provisional version of its report, CEN/ISSS, February 2003). However, one should note the interesting initiative entitled 'OpenDRM ', whose aim is to promote a reference framework for DRM that would be compatible with the practices and philosophy of OpenSource software.

The second weakness concerns the fact that the reliability of these technologies has still not been proved. The renowned failure in 2001 of the SDMI project in the digital music area is still not forgotten. Even if some of the basic technologies used appear reliable when considered apart (for instance, those relative to digital signatures or cryptography), other technologies can still be improved (watermarking, among others). Moreover, the weaknesses essentially appear at the level of their implementation and interoperability with and within complex software designed for DRM purposes.

The security underlying the DRM systems is a legitimate expectation of the producers on the one hand, and the users on the other. The producers want to see a return on their technical and commercial investments around the DRM; they need these measures to be efficient and dissuasive with respect to the various forms of digital counterfeiting. On the other hand, the users have two concerns. Firstly, they want to be sure that their private data (identity, banking details, nature of the product ordered, etc.) are safely managed. Secondly, they do not want to have to change their software too frequently, often a consequence of the dual race between security threats and technological developments. On both sides, the uncertainty regarding the reliability of security technologies negatively affects their expansion and use on a large scale.

Use of these techniques on the market

The fact that there is little information available suggests that the security techniques are not yet regularly being used on the market for the protection of digital data. And those that are used on a relevant scale (e.g. for audio CDs) lead to criticisms and practical problems.

The music industry case should be observed very closely**.** Indeed, it seems that this industry is the only one, despite the failure of the SDMI project, which has officially announced its strategic intention to invest in security systems, and to assume responsibility for the consequences they have on consumers. As a result, concentration in this activity sector (which is mainly dominated by five multinational players) could lead to a de facto standard for protecting audio CDs and for downloading music online. This would have a substantial impact on developing solutions to protect other digital content as a result of interoperability constraints.

The other aspect to consider is the significant implication of several major information technology players in the DRM technologies. The investments and technological and commercial announcements of Microsoft, IBM or Sony may result in them playing a central role as regards these technologies. In particular, these players may agree between themselves on particular techniques that they would then impose on the market. It is therefore necessary to monitor this possibility closely in order to avoid a non-transparent technical agreement replacing an international standardisation process that has just begun.

Impact on the prevention of digital counterfeiting

In this context, it is not surprising that the measurable impact of these techniques on digital counterfeiting has not been pointed out. This is not only because of a lack of statistical data, but is mainly the result of the infrequent use of these security tools in most of the e-commerce market segments in digital goods.

This lack of a measurable impact does not mean that announcing the launch of new technologies will not have a dissuasive effect on some consumers. It will prepare people for a progressive change in the digital landscape. One can imagine that the media coverage regarding several counterfeiting methods (in particular concerning the music files via the P2P networks), and the prospect of a greater use of stricter security technologies, may prepare consumers to adapt to fee-paying and more secure online distribution software.

However, it seems clear that the potential significant impacts on the prevention of digital counterfeiting require the use, on a large scale, of standardised and interoperable DRM systems. From this point of view, the current state of the market and the technological offer seem below that required. One can hope at most that the transposition in all the Member States of the requirements stated in the directive of 22 May 2001 will play a leading role in clarifying the challenges and the means to achieve them.

Analysis of the technical and economic situation, and of the transposition process already under way, led us therefore to make recommendations for the European institutions and Community policy in this area.

However, it is necessary to wait until the complete transposition of the directive in the Member States' legal systems and until its practical use is achieved in order to evaluate the situation.

3. Recommendations

The recommendations outlined at the end of the study are, in part, similar to those presented in our previous study on this subject in 2001 (F. Leprévost and B. Warusfel, 'Technologies de sécurité pour les médias digitaux', report for STOA, EP/IV/A/STOA/2000/06/01, May 2001).

Certain recommendations of a legal nature take into account the projects of transposition that we studied and the questions they raised.

Political recommendations

The main political European action in this sector has been the adoption of the directive of 22 May 2001 itself (and in particular Articles 6 and 7 thereof). Now it appears that the European authorities may consider, as a major political objective, promoting standardisation for security technologies and DRM.

We would therefore like to repeat the recommendation set out in our previous report:

- The promotion of an active standardisation policy of security technologies at the European level, taking into account the concrete proposals of representatives of academia, industry and consumers.

However, with regard to the expansion of online counterfeiting and to the reactions of people regarding the protection of intellectual rights in a digital world, we recommend that the European authorities adopt a two-step initiative:

- conduct a sociological study on consumers' perceptions of intellectual property rights for digital content (and on their elasticity with regard to commercial aspects, such as the price of digital works);
- using the results of this study and the contributions of several experts, promote information campaigns and/or promotional campaigns on the economic, societal and legal issues of intellectual property rights and counterfeiting in the digital world.

Technical recommendations

Despite the technological developments in the last two years, most of the recommendations stated in our 2001 report are still relevant, as follows:

- Bring the standards and the global secured management models of digital content on the Internet up to date
- Distinguish, if necessary, between the pure industrial standards, which may lead to a monopoly situation, and the standards issued from a general agreement between representatives of industry, academia and national bodies
- Promote solutions allowing for interoperability between distinct systems
- Identify the owners of 'essential patents', and check whether they intend to negotiate licences
- Propose technical studies on the security of existing or planned systems, and distinguish between open and closed approaches
- In connection with the proposal for a European normalisation, consider the setting up of a 'challenge' to the protocols considered as potential norms at this level
- Observe technological developments in the area of security techniques for digital media
- Evaluate the feasibility of compatible computer viruses' filters with processed data formats
- Study the conditions ensuring the convergence between DRM and PKI systems.

In addition, it appears that one of the requirements of the market — to accept the setting up and use of the DRM — concerns the relative continuity of these tools and their ease of use. Therefore, we should encourage, as a matter of priority, systems that would offer a sufficient level of progress and ease of use (i.e. systems whose technical components can be modified or updated — namely to deal with threats or to correct faults — and that could be made in a modular manner and updated without disrupting the use of the established software or challenging the protection of works that have already been exploited).

1.

1.1. Legal recommendations

On the legal side, the essential short-term issues are linked with setting up the transposed provisions of the 22 May 2001 directive in the Member States.

With regard to the transpositions already carried out or under way, it appears that three areas require particular treatment and should be monitored.

First of all, it is essential to ensure the coherence of the national decisions taken to enable certain technological measures to be compatible with the exemptions of copyright law. In fact, it would be very difficult to imagine, for the producers as well as for the consumers, that certain measures or facilities recognised in one Member State would not be recognised in another. As those decisions are taken by mediators (usually) or by a ministry-level authority, or even by a jurisdiction, the risks of divergence could be substantial. Therefore, the Community authorities have a two-fold responsibility:

- firstly, to constantly follow up the decisions relative to the application of Article 6.4 of the directive and to evaluate, case by case, the coherence of those decisions in relation to each other;
- secondly, to encourage cooperation between the different national entities and to set up a permanent dialogue, in order to elaborate a common 'doctrine'.

A second concern relates to the potential negative effect, on the cryptological and security research, of implementing the directive's provisions regarding the protection of technological measures. Protecting European interests in the field of security technology (and related economic, social, political or even military consequences) demands that European expertise in this matter should not be affected by the fear of abusive legal actions. We will also have to keep testing the reliability of our technologies to ensure the security of the information society and e-commerce.

> *Therefore, it is necessary — in the absence of clear dispositions in the majority of the transposed texts — that the Community authorities ensure that protecting the technological measures does not necessarily mean an interruption in the legitimate and necessary research activities regarding cryptology and systems security.*

The eventual recourse to technological measures may lead to progressively lighter financial withdrawals, such as 'fair compensations' (namely on the price of blank digital supports). In fact, it is not possible to imagine that this compensation, aimed at counterbalancing the negative effects of the inevitable abuses linked to private copying, will continue without the creation of effective measures to limit or suppress the likelihood of such abuses.

1.1.1. It could be useful and also politically interesting to study, along with the parties involved (producers, author societies, rights holders, representatives of Internet users), how it might be possible to replace 'fair compensation' procedures by technological measures.

In the end, it still appears necessary, as recommended in our previous report, to prepare in-depth legal studies on the new contractual models that might result from the secure commerce of digital content.

EUROPEAN PARLIAMENT

Directorate-General for Research
Division for Industry, Research and Energy

Study n°IV/STOA/2002/13/02

Protection et implémentation des droits de propriété intellectuelle dans les technologies de sécurité dédiées aux médias numériques

Prof. Dr. Franck LEPREVOST
(Université Joseph Fourier Grenoble 1 – Centre universitaire du Luxembourg)
& Prof. Dr. Bertrand WARUSFEL
(Université René Descartes Paris 5 – Avocat au barreau de Paris)

Le présent rapport constitue le document final de l'étude qui nous a été commandée par le STOA à la demande de la Commission de la Culture, de la Jeunesse, de l'Éducation, des médias et du Sport du Parlement européen (tender n° 116741, 22 juillet 2002)..

Il se base notamment sur des éléments précédemment étudiés dans le rapport que nous avions réalisé en mai 2001 pour le STOA sur le thème "Technologies de sécurité pour les médias digitaux" (EP/IV/A/STOA/2000/06/01, Mai 2001).

La Partie A de ce rapport est consacrée aux technologies de sécurité et aux architectures de gestion des droits actuellement proposées,

La Partie B de ce rapport est consacrée au contexte juridique et économique du déploiement de ces technologies de sécurité et des systèmes de gestion des droits.

La Partie C propose différents compléments technologiques utiles à la compréhension du rapport tandis que la partie D présente les conclusions et les recommandations que nous formulons à l'issue de cette étude.

TABLES DES MATIÈRES

PARTIE A : LES TECHNOLOGIES DE SÉCURITÉ ET LES ARCHITECTURES DE GESTION DES DROITS

A.1.- La problématique des DRM

L'utilisation de technologies de sécurité pour protéger les droits de propriété intellectuelle dans le contexte numérique a amené les industriels et les producteurs de contenus (textes, images animées ou inanimées, musique, logiciels, services interactifs, …) à concevoir de véritables systèmes techniques permettant le contrôle et la gestion des droits intellectuels tout au long de la chaîne de distribution et d'utilisation de ces contenus.

On dénomme usuellement ces systèmes sous le terme générique de "Digital Rights Management" (DRM), même si d'autres terminologies ont été également (ou sont encore parfois) employées (comme par exemple Electronic Copyright Management Systems – ECMS, ou encore Intellectual Property Management and Protection - IPMP, …..). Par souci de cohérence, nous retiendrons uniformément dans cette étude le terme de DRM qui est aujourd'hui largement reconnu.

A.1.1. Définition du concept de DRM

Selon le National Institute of Standards and Technology (NIST, organisme national de normalisation américain) le DRM est

> *"A system of information technology components and services, along with corresponding law, policies and business models, which strive to distribute and control intellectual property and its rights. ..."*

De leurs côtés, l'Institut IDC et l'association DWS définissent le DRM comme

> *"the chain of hardware and software services and technologies confining the use of digital content to authorized use and users and managing any consequences of that use throughout the entire life cycle of the content."* [7]

Enfin, l'IFPI et la FEP retiennent plutôt la définition suivante :

> *"Digital rights management refers to the technologies and/or processes that are applied to digital content to describe and identify it and/or to define, apply and enforce usage rules in a secure manner".*

Mais quelle que soit la définition retenue, on peut convenir que deux aspects fonctionnels coexistent et se complètent dans le concept de DRM :

- La gestion des droits numériques, qui consiste en l'activité d'identifier et de décrire la propriété intellectuelle et poser les règles d'usages.
- La gestion numérique des droits, qui elle consiste en la sécurisation des contenus et en la mise en place de moyens numériques permettant leur usage légal.

Pour réaliser ces deux fonctions successives (en amont identifier et décrire les droits, et en aval les gérer de manière sécurisée), les différents systèmes de DRM font appel à diverses technologies.

A.1.2. Les composantes techniques et fonctionnelles des systèmes de gestion électronique des droits

Pour décrire ces différentes technologies, on peut, là aussi, se référer à des typologies établies dans la littérature, tant sur le plan technique que fonctionnel.

a) les différents types de technologies potentiellement mises en oeuvre

Dans leur note pour l'Organisation mondiale de la propriété intellectuelle (OMPI) en novembre 1999 [147]., Alain Strowel et Séverine Dusollier distinguent quatre niveaux de technologies complémentaires pouvant être associées pour constituer des systèmes techniques de protection des droits :

- des mesures techniques protégeant les droits des auteurs, qui empêchent l'accomplissement de tout acte ou usage soumis aux droits exclusifs des ayants droit, tels que l'impression ou la copie. Par exemple, le *dongle* équipement physique utilisé pour préserver les droits sur les logiciels, ou encore différents dispositifs empêchant soit le ré-enregistrement soit la lecture de contenus audio ou vidéo (comme par exemple, le système *Content Scrambling System* protégeant les DVD) ;

- des systèmes d'accès, qui restreignent et contrôlent l'accès aux contenus protégés, à la fois dans le but de garantir le paiement d'une rémunération et pour protéger les droits d'auteur sur l'œuvre. Des technologies plus ou moins sophistiquées peuvent remplir cette fonction : cryptographie, mots de passe, signatures digitales, enveloppe numérique, … ;

- des outils de marquage et de tatouage qui peuvent remplir plusieurs fonctions. Tout d'abord, insérer des données relatives à l'œuvre, qu'il s'agisse du titre de l'œuvre, de l'identité de son créateur et du titulaire de droits, ainsi que des conditions d'utilisation (ce que le traité de l'OMPI sur le droit d'auteur et la directive du 22 mai 2001 dénomment les "informations sur le régime des droits"). Cela peut aussi permettre un marquage apparent (souvent dénommé "*fingerprinting*") empêchant la ré-utilisation commerciale du contenu. On peut aussi utiliser de tels moyens pour garantir le respect de l'intégrité de l'œuvre, ou pour assurer le suivi et la traçabilité du contenu (le

marquage comporte alors un numéro de série) qui peut faciliter la preuve de la contrefaçon ;

- enfin - au plus haut niveau – des logiciels de gestion capables d'agir sur les différents outils technologiques précédemment cités peuvent permettre la conclusion de licences d'utilisation *on-line* et le contrôle de l'utilisation des œuvres. D'autres fonctions peuvent également être prises en charge par ces outils : la répartition des droits perçus, la perception des paiements, l'envoi de factures, la réalisation de données de profilage des utilisateurs, etc …

Pour sa part, Leonardo Chiariglione (qui fut le directeur technique du projet SDMI, cf. infra) proposait dans son rapport au Conseil Supérieur de la Propriété Littéraire et Artistique français une liste des principales technologies-clés nécessaires à la mise en œuvre des DRM :

> *"- l'identification des Digital Items (il s'agit de l'équivalent virtuel du code SBN qui doit être compatible avec un grand nombre d'exigences), la norme sera approuvée en mars 2002 ;*
>
> *- la description des Digital Items (le terme " description " est un terme très large qui est parfois défini comme " métadonnées "), dans ce cas, il faut se référer aux descriptions très spécifiques associées à l'identification, la norme sera approuvée en mars 2002 en même temps que celle de l' "identification " ;*
>
> *- " l'association persistante " (il s'agit d'une technologie qui permet le trafic des données telles que l'identification de manière à ce que le numéro d'identification et le contenu identifié ne puissent être séparés) ;*
>
> *- le " langage des droits " (il s'agit d'un langage lu par les machines qui permet aux utilisateurs de la norme MPEG-21 de déclarer des droits vis-à-vis des contenus), la norme sera approuvée en mars 2003 ;*
>
> *- la " gestion et protection de la propriété intellectuelle " (il s'agit d'une technologie qui assure la protection des contenus de manière à ce qu'un utilisateur ayant acquis un droit vis-à-vis de ces contenus puisse y accéder dans la transparence sans être obligé d'utiliser un dispositif imposé par le fournisseur des contenus en questions), la norme sera approuvée en mars 2002. D'autres technologies sont en cours de développement dans le cadre du projet MPEG-21."*[70].

b) les principales fonctions assurées par un système de DRM

Dans son article relatif aux architectures de RDM publié en juin 2001 [102]. Renato Iannella propose un schéma général des différentes fonctions exercées dans un système de DRM. Il les classe en trois stades successifs :

- <u>la création</u> des actifs intellectuels, fonction qui correspondrait à la mise en œuvre de trois fonctions complémentaires
    - la création de droits sur de nouveaux contenus créés,

- la validation des droits attribués sur les contenus créés,
- la circulation (workflow) des droits (notamment aux fins de validation)

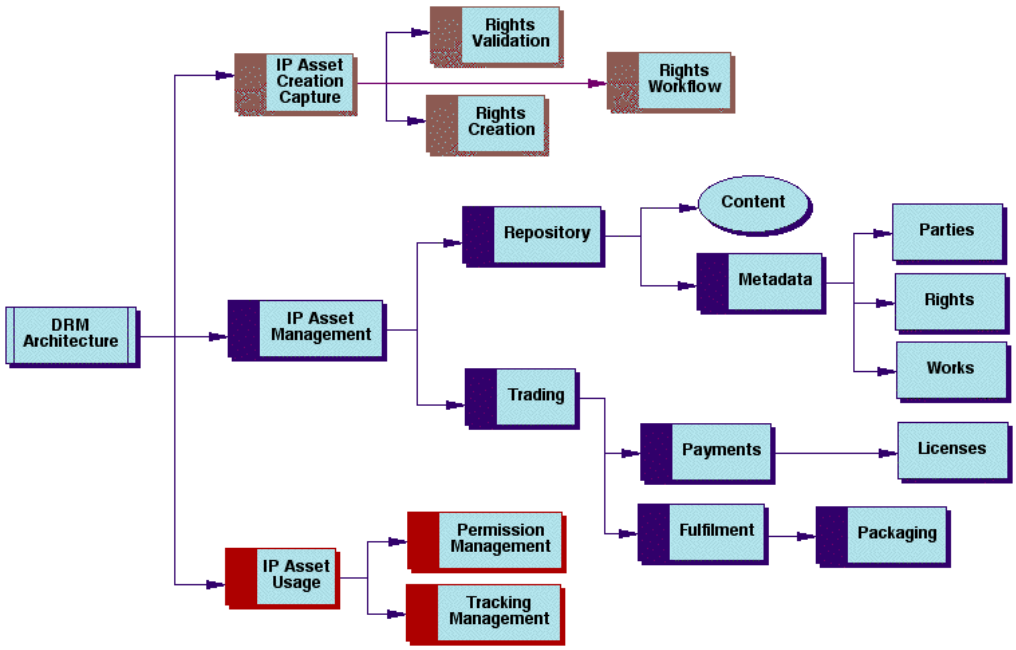
- la gestion de ces actifs intellectuels, qui mettrait en œuvre :

  - la conservation-archivage des droits (dans des bases de données qui conservent les "metadatas" associés aux contenus et qui sont interrogées lors de toute transaction),
  - la commercialisation des droits sous la forme de licences et donnant lieu aux payements associés,

- l'utilisation de ces actifs intellectuels, qui est encadrée par les deux fonctions suivantes :

  - l'autorisation (qui permet à l'utilisateur de réaliser un acte – par exemple, une reproduction, l'écoute ou l'impression, …),
  - le suivi (pour s'assurer du respect des droits accordés).

Il regroupe ces différentes fonctions de base dans le schéma suivant :



(source : R. Iannella, D-Lib Magazine, 6-01)

A.2. Des technologies et des architectures disponibles sur le marché

Dans cette partie, nous décrivons tout d'abord les propositions d'approches globales de la gestion des droits numériques, puis les approches plus spécifiques.

A.2.1.- Les différentes approches globales actuellement proposées

Nous traitons en premier lieu certaines des approches globales proposées, c'est-à-dire qui ne se focalisent pas sur un média particulier, mais qui sont a priori prévues pour traiter des données multimédia.

A.2.1.1.- CPSA : Content Protection System Architecture

L'architecture CPSA ([49]) s'appuie sur des axiomes, qui décrivent comment les appareils compatibles avec CPSA abordent la gestion du contenu de l'information.

Le possesseur du contenu sélectionne le mode d'information de gestion du contenu (CMI: Content Management Information), à partir des différentes options. Cela peut par exemple contenir des informations relatives au nombre de copies possibles (CCI: Copy Control Information), ou d'autres informations. Il est nécessaire d'assurer l'intégrité des données CMI, ce qui se fait à l'aide de différentes méthodes cryptographiques. Le CMI peut également être inclus dans le contenu sous forme d'un watermark. Le contrôle d'accès s'appuie sur d'autres axiomes. Ainsi, tout contenu CPSA est stocké sous forme cryptée. Ainsi, l'on prévient des lectures non autorisées. En outre, toutes les copies de contenu CPSA sont cryptées, sauf si un accord spécifique et différent a été établi. Les appareils compatibles CPSA détectent le watermark CMI sur les données non cryptées qu'ils reçoivent. Ainsi, si un watermark CMI est trouvé sur un contenu numérique non crypté, l'appareil n'autorise pas la diffusion de ce contenu. La protection cryptée de contenu CPSA doit se poursuivre tout au long de la transmission. Les appareils compatibles CPSA se doivent également d'examiner le statut de CCI avant de faire une quelconque copie. La copie n'est faite que si le CCI l'autorise. Il est alors nécessaire d'actualiser le CCI selon qu'une ou des copies sont effectuées.

Nous décrivons ci-dessous succinctement deux technologies de protection des contenus consistantes avec l'approche CPSA.

A.2.1.2.- *CPRM : Content Protection for Recordable Media*

Il s'agit de l'approche développée par le groupe 4C, composé d'Intel, IBM, Matsushita et Toshiba. Cette protection tend à empêcher la copie de certains fichiers d'un disque dur à l'autre. Un disque dur équipé de ce système CPRM possède un identifiant unique. En d'autres termes, il intègre dans ses dispositifs de stockage une clef, calculée à partir de son numéro de série. Un fichier CPRM qui arrive sur le disque dur est immédiatement reconnu, et codé à l'aide de la clef. Les données stockées sur le disque ne sont alors lisibles qu'à la condition de disposer d'un numéro d'authentification. L'accès à ce numéro se fait via un serveur central, et ce numéro est calculé en fonction de la clef de numérisation du disque dur.

Cette approche se différencie de la plupart des autres systèmes proposés par le fait qu'elle place la sécurité au niveau des équipements eux-mêmes (hardware) et non pas uniquement au niveau des contenus et des logiciels applicatifs. Si cela est supposé lui donner une capacité accrue à résister contre différentes de contournement, il paraît aussi qu'il s'agit d'une conception maximaliste susceptible de susciter des craintes fortes (notamment en ce qui concerne le respect de la vie privée). Cela vient de se vérifier avec la décision du NCITS (National Committee on Information Technology Standards) américain qui a rejeté le 2 avril 2001 la proposition CPRM. Ainsi, il apparait qu'il n'y a pas à l'heure actuelle de consensus entre les différents acteurs intervenant au niveau de

cet organisme de standardisation, pour accepter une solution de contrôle anti-copie poussée jusqu'au niveau de l'intégration dans les équipements.

A.2.1.3.- *DTCP : Digital Transmission Content Protection*

Cette approche a été développée par le groupe 5C, qui est composé cette fois de Intel, Toshiba, Hitachi, Sony et Panasonic. Les spécifications visent principalement les connexions IEEE 1394/FireWire, mais peuvent être adaptées à d'autres modes (NRSS Smart Card, USB, PCI, etc). Sony développe en particulier une puce DTCP. L'idée est que les appareils connectés et maniant des données numériques, comme les lecteurs de DVD, les téléviseurs numériques, les magnétoscopes numériques, etc., échangent des clefs et des certificats d'authentifications afin d'établir des liaisons sécurisées. Le lecteur de DVD chiffre le signal audio/vidéo en l'envoyant à l'appareil de réception, qui doit bien entendu le décrypter. Ainsi des appareils connectés, mais non-authentifiés, ne peuvent pas voler le signal. La phase de chiffrement n'est bien entendu nécessaire que pour les programmes qui ne sont pas protégés contre la copie.

Plus généralement, il est à noter que les technologies de protection CPRM, CPPM (Content Protection for Pre-recorded Media), CSS, DTCP et HDCP (High-bandwidth Digital Content Protection), les accès conditionnels pour la distribution protégée de contenus via le câble ou par voie de satellite, la méthode 4C/Verance d'écriture et de lecture de watermark CMI dans le domaine audio (qui a pour but de spécifier si un contenu est phase I au sens SDMI), ou encore un schéma de watermark vidéo sélectionné par le DVD CCA sont compatibles avec l'approche CPSA.

A.2.1.4.- *XCA : Extended Conditional Access*

L'approche développée par Thomson est similaire à CPSA, mais peut fonctionner avec des interfaces à sens unique (voir le standard EIA-762 RF), et utilise des appareils d'authentification amovibles, comme une carte à puce par exemple, avant de déchiffrer les données. Dans cette perspective, cette approche fournit une sécurité davantage du type end-to-end que celle développée dans CPSA. En outre, dans le cas de XCA, il semble qu'il n'y ait pas de chiffrement et déchiffrements successifs au long de la chaîne, à la différence de CPSA. La XCA-LA (Licensing Authority) est l'entité en charge de l'administration des systèmes de protection du contenu. Elle aura également pour fonction de gérer les licences des spécifications XCA aux fabricants de matériel, aux distributeurs de contenu, suivant des règles précises. En outre, elle aura la charge de la création et de la distribution des clefs requises par les appareils en conformité avec l'approche XCA.

A.2.1.5.- InterTrust

L'architecture de la plate-forme DRM de InterTrust s'articule sur quatre points :

- Les InterRights Points, qui opèrent sur des PC et serveurs, et aux niveaux desquels le processus de gestion des droits opère. Chaque telle entité agit comme une machine virtuelle sécurisée, qui est en mesure de gérer les droits de chaque partie. Elle crée une base de donnée locale sécurisée, qui stocke les droits de l'usager, les identités, les transactions, les clefs.

- Les informations protégées sont cryptées et stockées dans des containers. Ces informations peuvent éventuellement circuler sous manière cryptée, mais seul un InterRight Point peut, dans un certain cadre, accéder aux informations non cryptées.

- Des règles d'utilisation gouvernent les contenus. Les ayant-droits peuvent créer et changer les règles. Les règles peuvent circuler avec le contenu ou séparément.

- Un système de contrôle des communications collecte les fichiers de transactions des différents InterRights Points, les renvoie selon les directives autorisées par les règles d'utilisation, et gère également les questions de sauvegarde, de détection des fraudes, etc.

Une des particularités du système est de permettre une fonctionnalité de distribution de type peer-to-peer, dans un environnement légitime.

Des variantes de ces approches ont été proposées, par exemple dans [114], [115]).

Notons que la société InterTrust a été rachetée en novembre 2002 par une joint-venture Sony-Philips et qu'InterTrust a engagé une action en contrefaçon de brevet à l'encotnre de Microsoft accusant cette entreprise d'avoir violé certains de ses brevets décrivant son architecture DRM.

A.2.2.- Les approches plus spécifiques proposées

Dans cette partie, nous traitons certaines initiatives (sans prétention d'exhaustivité) de protection des droits orientées sur des supports Médias précis.

A.2.2.1.- *Domaine musical*

La Secure Digital Music Initiative, SDMI ([49]) avait tenté de développer entre 1999 et 2001 un système ayant pour but de limiter le piratage des contenus musicaux. Ce groupe, rassemblant plus de 190 compagnies et organisations impliquées dans les contenus musicaux, en particulier la RIAA, l'IFPI, et la RIJA, avait initié deux phases.

Dans la première (qui a donné lieu à la mise sur le marché de produits conformes à cette spécification), un watermark est créé (basé sur la technologie Verance), qui a pour but de spécifier si un fichier musical est « nouveau » ou pas. Les appareils compatibles avec le standard SDMI doivent pouvoir jouer, sans limitation, les « vieux » contenus (l'idée est de permettre l'utilisation sur les appareils compatibles SDMI des 10 milliards de CD vendus au cours des 17 dernières années).

Dans la phase deux, il devait s'agir de proposer une technologie pour décider du statut (légitime ou non) du nouveau contenu. Si le nouveau contenu n'était pas jugé légitime, il n'était pas lu par l'appareil de lecture compatible SDMI. Bien entendu, les appareils compatibles SDMI seront en mesure de lire les fichiers MP3 (ou éventuellement des fichiers de musique compressés sous d'autres formats). La spécification 1.0 actuelle permet de lire les

fichiers musicaux sur une grande variété de plate-formes, en particulier sur les PC (voir [152] pour des réactions sur ces initiatives).

Un autre exemple significatif d'implication d'un acteur important du secteur des télécommunications est celui de Deutsche Telekom avec le produit Music on Demand. L'architecture globale est classique, et fait usage de communications et transactions protégées par des modules cryptographiques (avec notamment l'utilisation d'une connexion sécurisée SSL). L'intérêt est surtout au niveau des fonctionnalités, comme la possibilité de super distribution, et la flexibilité au niveau des modes de paiement, qui peuvent se faire par carte de crédit, mais aussi directement sur la facture téléphonique. L'approche dite de streaming est également développée dans la plate-forme MusicNet (qui regroupe Bertelsmann, EMI, Warner, l'autre gros consortium étant Pressplay, qui alliait Vivendi-Universal à Sony et qui a été récemment racheté en 2003 par l'éditeur de logiciel Roxio), mais pas exclusivement, puisque cette plateforme permet également de télécharger des morceaux de musique.

Un autre exemple important est celui de l'EMMS (Electronic Media Management System) de IBM, qui fournit une suite de 5 produits softwares. Le système est en mesure d'intégrer les progrès technologiques faits dans le domaine de la cryptographie, du watermarking, de la compression, etc., à l'aide de plug-ins.

L'approche Windows Media Technologies 9 de Microsoft, compatible SDMI, traite plus généralement les données audio-visuelles (cf. infra). Elle se distingue de l'approche CPRM, dans le sens où le système de gestion des droits (DRM) est intégré dans le système d'exploitation, alors que la démarche CPRM s'affranchit a priori du système d'exploitation considéré. Toutefois, la sécurité va également jusqu'au niveau hardware, par exemple avec le Secure Audio Path, qui stocke une clef secrète unique, utilisée pour la phase d'authentification et d'accès au contenu (qui est d'ailleurs lui-même crypté).

Des tentatives dans le sens de l'interopérabilité des systèmes de distribution de musique existent, comme l'initiative EMD (Electronic Music Distribution), qui regroupe, entre autres, InterTrust, Microsoft Media, Liquid Audio, ou IBM EMSS.

A.2.2.2.- *Le secteur du logiciel*

Dans le domaine de la distribution électronique de logiciels, diverses approches se sont fait jour. Ainsi, certains systèmes en usage actuellement procèdent à une dichotomie des logiciels à distribuer. Dans cette démarche, il s'agit dans un premier temps d'exporter une partie du code d'une application sur un serveur contrôlé par le distributeur. Lorsque l'internaute télécharge, depuis un site web, le logiciel correspondant, son exécution nécessite que l'internaute s'identifie auprès de ce serveur, qui débloque, selon les droits accordés, l'exécution de la partie de code nécessaire à l'exploitation du logiciel, et qui n'est pas résidente au niveau de l'internaute. Cette approche est par exemple préconisée par la société Netquartz, via son système AAS (Asymetric Application Segmentation Technology).

A.2.2.3.- *Le secteur de l'édition électronique*

Dans le secteur des documents écrits, plusieurs initiatives ont eu lieu. Ainsi, Microsoft a lancé son initiative eBook, qui propose un système client serveur, le serveur étant muni du DAS

(Digital Asset Server), qui fournit un système DRM, ayant la flexibilité voulue pour répondre à des niveaux de sécurité variés. Des extensions de ce système intègreront XrML (eXtensible Rights Markup Language, langage développé à partir des travaux de Xerox, cf. ci-dessous). Des restrictions permettent de limiter les droits de copie ou d'impression des contenus dédiés pour eBook.

Adobe a également développé un environnement de gestion sécurisée (qui utilise essentiellement de la cryptographie sur 56 bits, et des signatures électroniques sur 1024 bits selon les documents de Adobe) des droits relatifs aux documents au format pdf (Portable Document Format).

Dans ce même domaine des documents numériques, une approche très ambitieuse a été développée par les chercheurs du laboratoire de Xerox à Palo Alto. Le concept-clé de cette approche est celui des « trusted systems » (équipements de confiance) qui – comme dans l'approche CPRM – vise à sécuriser non seulement les contenus mais également les équipements intervenant dans la chaîne de production, de diffusion et de reproduction (y compris les copieurs ou les imprimantes). Dans cette approche, par exemple, une photocopieuse intégrée à un tel système de confiance doit pouvoir reconnaître qu'un document qui lui est soumis n'est pas affecté des droits permettant de réaliser une photocopie et – dans ce cas – doit refuser de réaliser la copie demandée.

Pour permettre le maniement de documents conformément à cette approche, le laboratoire de Palo Alto a mis au point un langage interprété de type XML intitulé DPRL (Digital Property Rights Language) [157]. Il s'adapte, non seulement au domaine du document, mais plus généralement aux contenus numériques, tels que la musique, les vidéos, etc. Son objet est de spécifier les conditions d'usage de ces contenus, et est intégré dans la suite logicielle que commercialise ContentGuard, la filiale spécialisée de Xerox et de Microsoft.

A.2.3.- Les spécifications OPIMA et les standards futurs MPEG-4, MPEG-7 et MPEG-21

L'OPIMA (The Open Platform Initiative for Multimedia Access, voir [132]) est une initiative du programme ITA (Industry Technical Agreement) de l'IEC (International Electrotechnical Commission). Elle a édité une spécification (OPIMA Specification 1.0), qui présente une architecture et une description des fonctions nécessaires à l'implémentation de systèmes compatibles OPIMA. Cette spécification contient également des protocoles de sécurité et une description des API (Application Programming Interface) et des fonctionnalités favorisant l'interopérabilité des systèmes. L'architecture OPIMA est de type peer-to-peer, et les protocoles OPIMA permettent la mise en place de différents systèmes IPMP (Intellectual Property Management and Protection), en particulier dans les parties 3.3.4. A ce stade, des choix spécifiques d'algorithmes de cryptographie, de signature électronique, de watermarking, de systèmes de cartes à puces, etc., ne sont pas faits, mais le but est de donner une infrastructure autorisant de puiser, selon les besoins, dans un panel d'algorithmes.

En parallèle, certaines parties de MPEG-4, MPEG-7 et MPEG-21 ont pour objectif de favoriser l'interopérabilité entre les différents modes de gestion protégée des contenus multimédias, et favoriser un usage plus transparent et productif des ressources multimédia disponibles. Les éléments de base sont :

- L'item numérique, qui désigne un objet numérique structuré avec une représentation standard compatible avec l'environnement MPEG-21.

- L'utilisateur, qui est une entité qui interagit avec l'environnement MPEG-21 en maniant des items numériques de type MPEG-21.

L'une des neuf technologies prévues à ce stade au programme de travail de MPEG-21 concerne directement la gestion des droits et la protection des données, et s'intitule IPMP (Intellectual Property Management and Protection, Part 4). Il s'agit de fournir une architecture compatible avec les différentes approches développées, afin de faciliter, pour l'usager, l'utilisation des ressources, et pour l'ayant-droit, la bonne gestion de ses produits. Il s'agit d'exploiter dans cette approche les standards existants, ou de favoriser l'émergence de groupes de travail pour traiter les nouveaux problèmes qui pourraient émerger. Le projet inclut des moyens standardisés de récupérer des outils IPMP de sites délocalisés, d'échanger des messages entre des outils IPMP, et entre ces outils et le terminal. Il concerne également l'authentification de ces outils IPMP, et offre la possibilité d'intégrer des expressions de droit (Rights Expressions) selon le dictionnaire des données juridiques (Rights Data Dictionnary) et le langage d'expression des droits (Rights Expression Language), aspects également traités dans MPEG-21 dans la partie 5 et 6.

La première étape consiste à mettre en place un standard de déclaration d'item numérique. Il semble naturel qu'il s'appuie sur des standards existants, comme ISBN pour les livres physiques, ISWC pour les compositions musicales, ISRC pour les enregistrements audio, ou encore ISAN pour les films, mais il devrait également comporter des identifiant pour les e-books ([131]) par exemple, etc. (voir également [51]). Il est à noter que certaines des propositions décrites plus haut peuvent éventuellement répondre aux réquisitions demandées dans les appels d'offre de MPEG-21.

A.3. Des moyens cependant encore peu exploités

Une rapide analyse de la situation (en particulier dans l'Union européenne) nous montre que si la volonté de plusieurs acteurs majeurs du marché de s'engager dans la voie de l'utilisation de mesures techniques est clairement affichée, les chiffres et les prévisions économiques concernant le secteur des DRM et de la diffusion des contenus protégés demeurent très faibles. De l'avis même de l'industrie ([106]), et même si nous venons de décrire plusieurs propositions technologiques de gestion des droits numériques actuellement disponibles sur le marché, il existe, en effet, plusieurs facteurs contribuant à l'actuelle faible acceptance des systèmes de DRM actuels.

A.3.1. La volonté affichée de plusieurs acteurs majeurs du marché

A.3.1.1. Les initiatives de Microsoft

Première société mondiale dans le domaine des technologies de l'information, Microsoft a multiplié depuis 1999 les annonces et les initiatives en faveur de l'adoption de techniques de protection des droits sur les contenus numériques. Et ce à plusieurs niveaux :

1°) en tant qu'éditeur de logiciels, Microsoft a renforcé significativement les moyens techniques visant à empêcher ou à dissuader la copie et l'utilisation non autorisées de ses propres créations logicielles et en particulier de ses systèmes d'exploitation.

2°) en tant que fournisseur d'un environnement informatique largement répandu sur les plates-formes numériques (PC, mais aussi désormais les PDA de type Pocket PC, voire bientôt certains "smartphones"), Microsoft propose également des instruments de sécurité susceptibles d'être utilisés par des fournisseurs de services ou des producteurs de contenu voulant mettre en œuvre des solutions de type DRM.

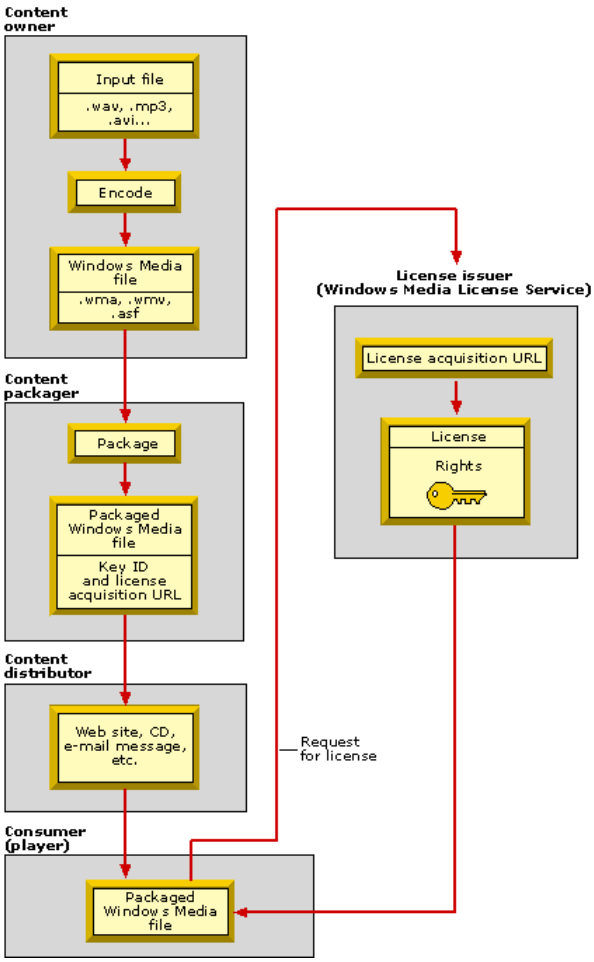
Après l'intégration dans Windows XP du système PassPort (dénommé désormais .Net Passport) Microsoft peut proposer à des fournisseurs de service d'utiliser les informations d'identité recueillies par ce biais afin d'authentifier leurs utilisateurs, voire de les utiliser pour des applications de paiement en ligne (un accord en ce sens a, par exemple été passé en juillet 2002 entre Microsoft et la société de logiciel pour télépaiement Arcot System [130]). On dénombre en effet déjà plus de 200 millions de comptes Passport gérés par Microsoft. L'Union européenne a du, d'ailleurs, intervenir pour obtenir de Microsoft différentes modifications de son système afin de renforcer sa sécurité et de le rendre compatible avec les exigences de la réglementation européenne en matière de données personnelles [77].

A plus long terme, Microsoft prépare une architecture logicielle censée être totalement sécurisée. Connu à l'origine sous le nom de "Palladium", ce projet s'appelle désormais NGSCB (*Next-Generation Secure Computing Base for Windows*). Et s'il ne se positionne pas en lui-même comme un système de DRM, Microsoft reconnaît que la complémentarité peut être forte puisque NGSCB peut servir de plate-forme sécurisée sur laquelle un logiciel de DRM pourra facilement s'appuyer :

> *While DRM and "Palladium" are both supportive of Trustworthy Computing, neither is absolutely required for the other to work. DRM can be deployed on non-"Palladium" machines, and "Palladium" can provide users with benefits independent of DRM. They are separate technologies. That said, the current software-based DRM technologies can be rendered stronger when deployed on "Palladium"-based computers."* [128].

3°) enfin, Microsoft a progressivement développé son propre système de DRM à partir de son logiciel multimédia gratuit, Windows Media Player (aujourd'hui proposé dans sa version 9). Son format de fichier WMA comprend désormais une option sécurisée (c'est-à-dire

encryptée) dont la lecture sur un disque dur ou dans un lecteur multimédia (compatible SDMI) nécessite la récupération d'une clé auprès d'un serveur extérieur (par exemple, celui du fournisseur de services). Le schéma suivant résume ce concept DRM classique :



(source : www. microsoft.com)

Désormais, Microsoft propose aux fournisseurs de contenus et aux diffuseurs son logiciel Windows Media Rights Manager SDK lequel permet de créer des fichiers WMA sécurisés puis de délivrer aux utilisateurs des licences individuelles permettant de lire et/ou de copier les fichiers sécurisés.

D'ores et déjà différents fournisseurs de contenus en ligne utilisent le système Windows Media Rights comme logiciel de DRM pour commercialiser leur offre (à titre d'exemple, on peut citer dans le domaine musical, le service en ligne OD2 de musique "on demand" (Cf. Stanislas Hintzy , directeur général d'OD2 France, mai 2003).

Par ailleurs, le format WMA encrypté a été retenu par plusieurs sytèmes de protection des CD-Audio (cf. ci-dessous) et Microsoft propose désormais aux maisons de disques un nouveau système de protection – dénommé Windows Media Data Session Toolkit - qui devrait leur permettre de commercialiser des disques lisibles à la fois dans des lecteurs audio standards et sur des PC (où leur lecture pourra donner accès à un complément multimédia).

On peut donc considérer que l'engagement de Microsoft en faveur des solutions de type DRM est devenu l'un des axes de son développement futur. Et ce d'autant que Microsoft a engagé une nouvelle stratégie largement fondée sur la location d'applications en ligne (de type ASP – Application Service Provider) et que les systèmes ASP devraient devenir des utilisateurs importants des systèmes de DRM (pour gérer l'accès aux applications et la location de leurs temps d 'utilisation).

A.3.1.2. L'implication de l'industrie phonographique dans la protection des CD-Audio

Outre Microsoft, on peut considérer que les industriels du secteur phonographique sont actuellement les acteurs du marché les plus nettement engagés dans une logique de développement de mesures techniques pour la protection des droits et – à terme – de déploiement de véritables systèmes de DRM.

Il faut savoir, tout d'abord, que dans le souci permanent de lutter contre la contrefaçon de leurs disques CD-Audio, la plupart des entreprises assurant le pressage des CD utilisent déjà le système d'identification dénommé "SID Code" (Source Identification Code) mis au point par la firme Philips et devenu un standard soutenu et géré par l'association internationale de l'industrie phonographique (IFPI) [12]. Ce code inscrit de manière indélébile sur le CD permet d'identifier le lieu de pressage du support et son numéro de série. Ce système est aujourd'hui extensible au pressage de DVD.

Mais au-delà de ce moyen physique permettant de distinguer une copie pirate d'un exemplaire original d'un CD (ainsi que de suivre la trace des éventuelles importations parallèles d'exemplaires originaux), les industriels du disque se sont engagés depuis ces récentes années dans la mise en œuvre de systèmes de protection numérique des œuvres, et ce avec un double objectif :

- limiter la reproduction sauvage des CD-Audio (notamment depuis la banalisation des graveurs de CD),
- limiter la rediffusion en ligne (notamment au travers de systèmes peer-to-peer) de fichiers numériques (par exemple au format MP3) issus des CD-Audio disponibles dans le commerce.

Après plusieurs échecs (dont celui essuyé par Sony Music, dont une première protection des CD-Audio contre la copie pouvait être contournée, apparemment, par un simple coup de crayon sur le bord du disque [155]), les compagnies ont eu recours à des techniques plus sophistiquées qui commencent à être utilisées sur le marché.

L'une des premières technologies commercialisées a été celle de la société israélienne Midbar utilisée par plusieurs grandes entreprises du secteur comme BMG, EMI-Virgin et Universal Music, mais dont les premières versions CDS200 ne permettaient pas de lire le CD sur toutes les sortes de lecteur (comme par exemple les lecteurs de voiture).

Midbar a depuis été rachetée en décembre 2002 par Macrovision, le leader des systèmes de protection pour cassettes video et DVD. Celui-ci revendique désormais la commercialisation en Europe et en Asie de près de 100 millions de CD protégés par la nouvelle version CDS300 de son système.

De son côté, la filiale BMG du groupe Bertelsmann a annoncé en juin 2003 qu'elle testait aux Etats-Unis la solution concurrente MediaMax CD-3 développée par la société SunnComm. Et Sony a adopté son système propriétaire Key2Audio mis au point par sa filiale DADC (tout en développant en parallèle un véritable logiciel de DRM adapté au téléchargement en ligne – concurrent de Windows Media – l'Open MG X).

Tous ces systèmes reposent sur un concept commun : l'enregistrement de deux sessions des mêmes morceaux sur les CD. La première est lisible uniquement sur les platines CD de salon. Un système de protection interdit sa lecture — donc sa duplication — depuis un ordinateur. La deuxième session comporte les mêmes morceaux de musique accessible depuis un ordinateur sous une forme sécurisée (telle WMA de Microsoft ou Real Audio). Un logiciel de DRM contrôle ainsi la lecture du CD depuis un PC et limite les conditions dans lesquelles peut s'effectuer son enregistrement sur disque dur.

Mais outre les difficultés techniques de jeunesse (non-reconnaissance de certaines platines, incompatibilités, dégradation éventuelle de la qualité audio en cas d'utilisation sur ordinateur), ce déploiement annoncé des systèmes de protection technique sur les CD-Audio suscite déjà une vive réaction parmi certaines associations de défense des consommateurs et des internautes.

En France, une association de consommateurs a profité des incompatibilités de lecture apparus sur un CD mis en vente pour obtenir une première condamnation judiciaire de la maison de disque pour "tromperie" [74]. Et, la confédération Que Choisir a engagé plusieurs actions en justice contre les maisons de disque [138].

De son côté, l'association britannique Campaign for Digital Rights a engagé une action de protestation et de boycott à l'encontre de ces nouvelles pratiques de verrouillage des CD-Audio [64], relayée par plusieurs associations européennes.

Anticipant ces difficultés, l'IFPI a adopté en mai 2002 des recommandations à l'intention de ses membres relatives au bon usage des systèmes de protection des CD-Audio [13].

A.3.2. Des perspectives économiques qui demeurent encore modestes

Malgré l'engagement significatif de l'industrie phonographique et de quelques acteurs majeurs du secteur des NTIC (Microsoft – ainsi que nous l'avons décrit – mais aussi notamment Sony, qui est sans doute la seule entreprise internationale à être à la fois impliqué dans la production phonographique, la micro-informatique et ses périphériques, ainsi que les produits électroniques grand public), le déploiement des systèmes de protection technique et de DRM demeure encore très limité.

Et bien que l'on dispose de peu de statistiques précises ou même d'études prospectives spécialisées, il apparaît que les prévisions initiales concernant le développement du marché des technologies de sécurité et des DRM sont toutes revues à la baisse.

En 2001 encore, les rares études sur le sujet tablaient sur une progression rapide du marché des DRM entre 2000 et 2005. Une étude IDC annonçait un marché mondial de 96 M$ en 2000 et prévoyait une hausse de 106,1% par an qui permettrait d'atteindre un chiffre mondial de 3,7 Milliards $ à cet horizon [8].

A la même époque, l'institut Gartner estimait que ces technologies entraient dans la seconde phase de leur adoption par le marché, phase dans laquelle leur intérêt économique n'était pas encore clairement établi pour la majorité des entreprises mais où déjà certaines d'entre elles souhaitaient les adopter pour en tirer des avantages stratégiques et prendre de l'avance sur le marché. Selon cette analyse, l'année 2003 devait constituer une année-charnière durant laquelle les principaux fournisseurs de contenus devraient comprendre et identifier l'apport économique que représentent les DRM. Et Gartner fixait alors à 2006 la date à laquelle le marché des DRM arriverait à maturité et où des solutions standards commenceraient à s'imposer [66].

Deux ans plus tard ce relatif optimisme n'est plus de mise et les récentes études sont nettement plus en retrait.

Le même Gartner Group, par exemple, estimait déjà en 2002 que ces technologies de gestion des droits paraissaient se développer plus lentement que prévu, que peu d'entreprises semblaient déjà leur accorder de l'intérêt et que le domaine des DRM ne paraissait pas encore constituer un marché autonome distinct de celui des autres domaine du logiciel [92].

Ce relatif pessimisme s'est confirmé depuis lors. Selon une étude de l'Institut In-Stat/MDR rendue publique en mai 2003, le déploiement des systèmes de DRM aurait été largement freiné par les tensions qui opposent actuellement les producteurs de contenus et les fournisseurs et distributeurs de dispositifs numériques, ce qui ralentit d'autant le développement de ce marché [89]. Et ce malgré la publicité dont ces moyens font l'objet. D'un côté, les producteurs de contenus sont dans l'ensemble très favorables à la mise en œuvre de dispositifs de protection des créations numériques, de l'autre les industriels ne souhaitent pas financer de telles infrastructures ni être obligés d'y adapter leurs équipements (au risque de perdre en interopérabilité).

Cet avis paraît conforme avec le taux de pénétration (et donc d'acceptation) encore faible des services en ligne payants. Selon une enquête américaine de 2001, seuls 13% du grand public et 22% des professionnels acceptaient de recourir à de tels services [145]. Et une étude plus récente estime que dans le domaine particulièrement sensible du téléchargement de musique en ligne, la part des services payants (et donc généralement mettant en oeuvre des moyens de sécurité et de contrôle) s'établirait en 2003 à 19% contre 16% en 2002 (avec une prévision à 25% pour 2005 [75].

Le taux de pénétration des technologies de sécurité pour la protection des droits demeure donc assez faible, en particulier en Europe. Et si l'on peut y voir pour partie une conséquence du ralentissement économique global (particulièrement fort dans le secteur des NTIC), cette situation économique fragile tient sans doute aussi aux difficultés propres qu'éprouvent ces technologies de sécurité et les DRM a convaincre les entreprises et les usagers.

A.3.3. Des facteurs de résistance qui demeurent importants

Dans son étude de 2001 citée plus haut, le Gartner Group indiquait déjà que le développement du marché des DRM dépendrait de différents facteurs et principalement :

- de l'acceptation par les consommateurs de l'encadrement des droits sur les contenus numériques,
- de la capacité de l'industrie d'établir des outils standards, en particulier en ce qui concerne les langages de description et de gestion des droits,
- de l'équilibre économique entre les coûts et les gains liés à la mise en œuvre d'une solution DRM.

Cette analyse demeure pleinement justifiée et l'on peut considérer que le relatif sous-équipement et sous-investissement actuel dans ce domaine tient à ce que certains de ces préalables n'ont pas encore été satisfaits et à ce que des facteurs de résistance, que l'on avait peut-être sous-estimés, demeurent.

Du point de vue technique, l'un des freins réside sans doute dans le manque d'outils assurant la confiance, dont le comportement est défini, compris, et acceptable par les parties dans une transaction numérique. D'un côté, les détenteurs de contenu numérique ne distribueront certainement pas leurs travaux sur des plate-formes étant, à leurs yeux, potentiellement hostiles. De l'autre, les usagers sont très réticents pour diffuser des informations privées à des systèmes distants. Chaque détenteur de droits doit être persuadé que le système distant recevant son information se comportera comme prévu. L'idée actuelle (notamment chez des acteurs comme Microsoft – avec son projet NGSCB évoqué plus haut, mais aussi dans le monde des logiciels ouverts) est de proposer :

- Une base de calcul de confiance ouverte, que l'on peut auditer, et qui soit compréhensible (TCB, Trusted Computing Base).
- Les moyens de prouver la possession et l'opération d'un tel TCB à distance à une autre partie.

Le TCB doit également permettre de garantir un accès conditionnel aux ressources nécessaires, ce qui conduit au concept de moteur de gestion de confiance qui serait, par exemple, en charge de l'attribution dynamique d'autorisations aux différentes pièces d'un code exécutable chargé dans un processus. Ce concept est tiraillé entre la nécessité de le rendre aussi puissant et sophistiqué que souhaitable (pour gérer les différents types d'autorisations), et celle d'en faire un outil ouvert, compréhensible, et que l'on puisse auditionner. Les technologies auront besoin d'un langage commun d'expression des droits, qui soit suffisamment général et qui ira d'ailleurs au-delà des DRMs.

Une autre limite tient également au fait qu'à ce jour les différents systèmes mis en œuvre présentent tous des limites et des failles, ce qui est normal en matière de sécurité des systèmes mais qui fragilise l'acceptation par le marché et par les consommateurs de ces types de solution.

Dès lors – et comme nous l'indiquions déjà dans notre rapport précédent de mai 2001 [125], le déploiement commercial opérationnel des technologies de protection des droits demeure encore globalement incertain et va dépendre des progrès éventuels à plusieurs niveaux :

Du point de vue industriel, un préalable essentiel demeure le besoin d'une normalisation internationale à grande échelle. Il est évident, en effet, que ces dispositifs ne seront efficaces que s'ils peuvent se déployer tout au long de la chaîne de production, de diffusion et d'utilisation des contenus numériques, ce qui impose que les formats de données et que les fonctionnalités de sécurité nécessaires soient implémentés et reconnus aux différents stades et par les différents outils mis en œuvre (pour simplifier, depuis les logiciels de numérisation ou de création de contenus, jusqu'aux lecteurs dédiés – type lecteurs MP3 – ou aux navigateurs Web, en passant par les logiciels serveurs). Cette interopérabilité des outils de sécurité tout au long de la chaîne (voire, sans doute, interopérabilité entre plusieurs formats qui coexisteront en parallèle) oblige à un accord entre les principaux groupes d'intervenants industriels et commerciaux du marché : fournisseurs de logiciels, fournisseurs de contenus et industriels fabricants des équipements numériques spécialisés. Tous les systèmes actuellement proposés ou testés sont candidats à une future standardisation. Mais on voit bien que tous ne seront pas compatibles entre eux et que, du point de vue de la méthode d'élaboration, il existe une compétition (comme dans d'autres domaines) entre des solutions émergeant dans le cadre de groupes officiels de normalisation (à l'ISO ou à l'IEEE par exemple) et des offres de systèmes propriétaires proposées par des consortiums industriels et technologiques (souvent sectoriels). De la manière dont se feront les choix de standards et de la nature de ceux qui seront retenus (puis plébiscités par le marché) dépendra en partie la physionomie du futur marché des contenus numériques et les droits et obligations réciproques des consommateurs et des diffuseurs et producteurs.

D'un point de vue économique, le choix des modes d'implémentation des technologies de protection et de contrôle des droits ne va pas non plus être neutre. Suivant les solutions mises en œuvre, pourront être privilégiés certains modèles économiques et relationnels entre les acteurs du marché. Pour prendre quelques exemples simples, nous pouvons avoir des architectures qui favoriseront la diffusion et la rémunération des contenus « à la demande » (c'est-à-dire qui privilégieront le droit d'accès au droit d'usage). C'est d'ailleurs dans ce sens que la directive du 22 mai 2001 inclut une disposition spécifique préservant le droit des diffuseurs de mettre en œuvre des mesures techniques restreignant la copie au profit de systèmes de diffusion à la demande (cf. art. 6.4 de la directive, avec toutes les difficultés d'application que cela va sans doute entraîner. De même, on peut facilement concevoir que le déploiement de systèmes de gestion électronique des droits suffisamment performants pourrait permettre de remettre en cause dans certains domaines les pratiques de « gestion collective » des droits et de leur substituer une gestion individualisée – œuvre par œuvre et titulaire par titulaire. Enfin, on voit bien également que l'un des freins conjoncturels au développement des DRM tient au fait que ni les producteurs de contenus, ni les industriels de l'informatique et de l'électronique, ni a fortiori les utilisateurs finaux ne veulent payer seuls le coût de la sécurité. La recherche de modèles économiques consensuels est donc directement lié au succès des technologies de protection des droits numériques.

Enfin, sur le plan juridique, si le recours à de telles « mesures techniques » pour la protection des droits est aujourd'hui en passe d'être reconnue dans la plupart des États (suite à la transposition progressive des dispositions du Traité OMPI de 1996, comme par exemple dans la nouvelle directive communautaire sur le droit d'auteur, ou dans la loi américaine DCMA de 1998), il reste à apprécier dans quelles conditions pratiques les exploitants de ces technologies

et les utilisateurs des contenus protégés vont pouvoir faire valoir leurs droits. En témoignent déjà, la controverse engagée aux États-Unis autour du procès relatif au « déplombage » DeCSS ou encore les débats qui ont entouré en Europe l'adoption des dispositions de la nouvelle directive relatives à l'utilisation des mesures techniques et aux éventuelles limites qui pourraient leur être apportées en vue de préserver les exceptions au droit d'auteur.

Une étude plus approfondi du contexte juridique et économique dans lequel s'inscrit désormais en Europe le développement des technologies de sécurité et des DRM est donc nécessaire (cf. partie suivante).

PARTIE B : LE CONTEXTE JURIDIQUE ET ÉCONOMIQUE

DU DÉPLOIEMENT DES TECHNOLOGIES DE SÉCURITÉ

ET DES SYSTÈMES DE GESTION DES DROITS

B.1.- La directive du 22 mai 2001 et le nouveau cadre juridique de l'emploi des mesures techniques et de protection des droits

La directive communautaire sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information du 22 mai 2001 comporte, en ses articles 6 et 7 des dispositions qui vont exercer une influence certaine sur les modalités de recours à des dispositifs de protection électronique des droits intellectuels sur les contenus numériques.

B.1.1. Des dispositions issues des Traités de l'OMPI de décembre 1996 et couvrant les moyens techniques de sécurité actuels

En premier lieu, il faut signaler que ces dispositions mettent en application les dispositions des articles 11 et 12 du traité de l'OMPI sur le droit d'auteur du 20 décembre 1996, ainsi que des articles 18 et 19 du traité de l'OMPI de la même date sur les interprétations et exécutions et les phonogrammes.

Il faut, en effet, relever que son article 6.3. définit les *"mesures techniques"* (visées à l'article 11 du traité de l'OMPI) comme

> *"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 oeuvres ou autres objets protégés, les actes non autorisés par le titulaire d'un droit d'auteur ou d'un droit voisin du droit d'auteur prévu par la loi, ou du droit sui generis prévu au chapitre III de la directive 96/9/CE. Les mesures techniques sont réputées efficaces lorsque l'utilisation d'une oeuvre protégée, ou celle d'un autre objet protégé, est contrôlée par les titulaires du droit grâce à l'application d'un code d'accès ou d'un procédé de protection, tel que le cryptage, le brouillage ou toute autre transformation de l'œuvre ou de l'objet protégé ou d'un mécanisme de contrôle de copie qui atteint cet objectif de protection."*

Cette définition paraît couvrir les différentes voies technologiques actuellement développées et expérimentées sur le marché, à savoir la cryptographie (assimilable au "cryptage" et au "brouillage" visé dans cet article), le watermarking (que l'on peut rattacher aux autres transformations de l'œuvre ou de l'objet protégé") et les différents mécanisme de protection contre les copies illicites (qui sont visés sous la dénomination générique de "mécanisme de contrôle de copie").

De même, l'article 7.2 de la directive définit ce que le Traité de l'OMPI appelle dans son article 12 *"information sur le régime des droits"* comme

> *"toute information fournie par des titulaires de droits qui permet d'identifier l'œuvre ou autre objet protégé visé par la présente directive ou couvert par le droit sui generis prévu au chapitre III de la directive 96/9/CE, l'auteur ou tout autre titulaire de droits"* ainsi que *"les informations sur les conditions et modalités d'utilisation de l'œuvre ou autre objet protégé ainsi que tout numéro ou code représentant ces informations"*.

Là aussi, cette définition paraît à la fois suffisamment générale pour ne pas se limiter à un type particulier de technique de marquage ou à une forme particulière de données, tout en étant cohérente avec les mécanismes techniques actuellement développés ou expérimentés pour associer électroniquement à un contenu protégé les informations relatives aux droits qui lui sont attachés. Cela paraît être le cas pour les procédés de watermarking ou pour l'usage d'une "signature électronique" (elle-même définie par la directive 1999/93/CE du 13 décembre 1999 comme *"une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification"*), puisque dans les deux cas, on a bien adjonction au fichier numérique représentant l'œuvre d'un élément également numérique permettant l'identification (conformément au dernier alinéa de l'article 7 qui indique que cet élément d'information doit être *"joint à la copie ou apparaît en relation avec la communication au public"* de l'œuvre).

On peut donc considérer que ces deux articles protègent le recours aux principaux composants techniques d'un système de gestion électronique des droits de type DRM (puisque tout système de DRM implique à la fois – comme nous l'avons vu – une identification des contenus et des droits accordés ainsi des moyens techniques visant à empêcher les utilisateurs d'outrepasser l'usage de ces droits).

B.1.2. Des dispositions qui consacrent et protègent le recours aux moyens techniques de sécurité par les ayant-droits

L'application et la transposition des articles 6 et 7 de la directive du 22 mai 2001 devraient donner un cadre juridique cohérent et favorable au déploiement en Europe des technologies de sécurité et des DRM par les fournisseurs de contenus et de services.

En effet, même si rien dans les lois de propriété intellectuelle des différents États-membres, n'interdisait aux ayants-droits de protéger techniquement leurs œuvres numériques, certains pouvaient s'inquiéter des risques de litiges et de contestations qu'auraient pu rencontrer la mise en œuvre de ces moyens (ne serait-ce que parce qu'un certain flou demeurait sur la compatibilité de l'usage de ces instruments avec le respect des prérogatives généralement reconnues aux usagers, et notamment celles de la copie à usage privé). Et cela pouvait expliquer les réticences observées jusqu'à présent sur le marché (dont nous avons rendu compte précédemment).

Indiscutablement, l'entrée en vigueur en Europe des dispositions prévues par les articles 6 et 7 de la directive modifie la situation et inverse la perspective. Désormais, il est clairement établi que le recours à des moyens techniques et à l'identification des œuvres et des droits fait partie des pratiques légitimes des ayant-droits. Et ce ne sera que par exception que – dans certains

cas (notamment évoqués à l'article 6.4 de la directive) – les ayant-droits devront limiter leur liberté de recourir à de tels moyens de sécurité.

Les considérants de la directive sont assez explicites sur cette orientation favorable à la libre utilisation des moyens de sécurité par les ayant-droits et les diffuseurs :

> *(47) L'évolution technologique permettra aux titulaires de droits de recourir à des mesures techniques destinées à empêcher ou à limiter les actes non autorisés par les titulaires d'un droit d'auteur, de droits voisins ou du droit sui generis sur une base de données. Le risque existe, toutefois, de voir se développer des activités illicites visant à permettre ou à faciliter le contournement de la protection technique fournie par ces mesures. (...)*
>
> *(53) La protection des mesures techniques devrait garantir un environnement sûr pour la fourniture de services interactifs à la demande, et ce de telle manière que le public puisse avoir accès à des oeuvres ou à d'autres objets dans un endroit et à un moment choisis par lui. (...)*
>
> *(55) L'évolution technologique facilitera la distribution d'œuvres, notamment sur les réseaux, et il sera par conséquent nécessaire pour les titulaires de droits de mieux identifier l'œuvre ou autre objet protégé, l'auteur ou tout autre titulaire de droits, et de fournir des informations sur les conditions et modalités d'utilisation de l'œuvre ou autre objet protégé, afin de faciliter la gestion des droits y afférents. Les titulaires de droits doivent être encouragés à utiliser des signes indiquant notamment, outre les informations visées ci-dessus, leur autorisation lorsque des oeuvres ou d'autres objets protégés sont distribués sur les réseaux.*

Mais l'adoption des dispositions de la directive n'a pas permis de lever toutes les difficultés juridiques qui s'attacheront nécessairement à la mise en œuvre de ces moyens de sécurité.

L'enjeu de sa transposition et de son application dans les différents États-membres réside en particulier dans la manière dont l'usage des systèmes de type DRM (qui sont désormais protégés contre le contournement, au titre de la directive) pourra se concilier avec le respect des différentes prérogatives dont les utilisateurs des services en ligne peuvent également se réclamer (en particulier, par application de l'article 5 de la même directive).

1. B.1.3. Des dispositions dont l'articulation avec les exceptions aux droits intellectuels peut s'avérer délicate

Dans un souci de rester en cohérence avec les principes classiques du droit d'auteur, l'article 5 de la directive a redéfini une listes des exceptions aux droits exclusifs de l'auteur sur les contenus numériques. L'article 5.1 institue, notamment, une nouvelle exception relative aux copies techniques en ligne *"transitoires ou accessoires* (…)*, et qui n'ont pas de signification économique indépendante* " (copies en mémoire cache et sur les serveurs proxy, notamment), tandis que les articles 5.2. et 5.3. offrent au choix des États membres la possibilité de consacrer plusieurs exceptions supplémentaires. Parmi celles-ci, on retiendra particulièrement les *"reproductions effectuées sur tout support, pour l'usage privé d'une personne physique et à des fins non commerciales, à condition que les titulaires de droits reçoivent une*

compensation équitable" (art. 5.2b, qui reprend – sous des termes légèrement différents l'exception connue, notamment, en droit français au travers de l'article L.122-5 2° du Code de la propriété intellectuelle), le droit de citation (art. 5.3 c-d, déjà consacré en droit français par l'article L.122-5 3°) ainsi que les "*reproductions effectuées sur papier ou sur support similaire au moyen de toute technique photographique ou de tout autre procédé ayant des effets similaires, à l'exception des partitions, à condition que les titulaires de droits reçoivent une compensation*" (art. 5.2a).

Dès lors, il convient d'examiner dans quelle mesure la mise en œuvre par les diffuseurs et les ayant-droits de mesures techniques pour la sécurisation des contenus numériques ne risque pas de rendre caduque l'exercice de certaines des exceptions proposées à l'article 5.

Dans notre rapport de mai 2001 [125], rédigé durant le processus d'adoption de la directive, nous avions déjà évoquée cette question et nous recommandions au Parlement européen de

> *"veiller à ce que la reconnaissance du rôle des "mesures techniques"(par l'article 6) ne puisse entraîner des effets pratiques qui entreraient en contradiction avec la reconnaissance des exceptions obligatoires ou facultatives aux droits de reproduction et de communication prévues à l'article 5."*

Il est vrai que la logique des Traités OMPI de 1996 (dont sont issus les articles 6 et 7 de la directive) veut que ne soient protégées que "les mesures techniques efficaces qui sont mises en œuvre 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 œuvres, d'actes qui ne sont pas autorisés par les auteurs concernés ou permis par la loi." (article 11 du Traité sur le droit d'auteur). Dès lors, les auteurs estiment dans leur grande majorité que la protection juridique qu'accorde la nouvelle directive aux mesures techniques ne devrait s'appliquer que lorsque celles-ci sont mises en œuvre aux fins d'assurer la protection des droits d'auteurs, ce qui sous-entend que cette protection juridique cesserait de produire ses effets dès lors qu'une mesure technique serait utilisée pour imposer à l'utilisateur une contrainte non justifiée par le droit d'auteur (cf. notamment le Pr André Lucas [126] ainsi que le Pr Alain Strowel in [51]). Mais la rédaction finale de l'article 6 de la directive n'est pas aussi explicite et l'exemple du Digital Millenium Copyright Act (DMCA de 1998) américain nous montre qu'il est possible de concevoir deux catégories de mesures techniques : celles qui se limitent à interdire les actes portant atteinte aux droits de l'auteur et celles qui permettent de restreindre toute forme d'accès à un contenu indépendamment des règles du droit d'auteur.

De plus, on sait que l'effet de certains des dispositifs techniques de protection des droits et, particulièrement, des systèmes de contrôle des copies, peut être d'empêcher techniquement la réalisation de certaines formes de citations, de copies ou d'impression, même à usage privé (on en prendra comme exemple que la pratique des éditeurs de documents électroniques de type "e-book", qui ne permettent pas l'impression des textes mais uniquement la lecture à l'écran, supprimant ainsi par un simple paramétrage technique la possibilité de réaliser une copie sur support papier à usage privé). C'est pourquoi certains juristes s'inquiètent d'une dérive possible qui conduirait à passer d'un système de protection et de gestion des droits de propriété intellectuelle à un système de gestion des droits d'accès à l'information.

Au cours des entretiens et des réunions préalables au présent rapport, nous avons – par exemple – recueilli auprès d'une association professionnelle représentatrice d'un ensemble d'usagers avertis des nouvelles technologies de l'information (en l'occurrence, l'Association

française des documentalistes et bibliothécaires spécialisés) une liste de sujets d'inquiétude et de questions non résolus, qui nous semblent assez caractéristiques des interrogations légitimes que suscitent la transposition de la directive du 22 mai 2001 :

1. *"Le droit d'auteur français ne permet pas un contrôle de l'accès aux œuvres mais un droit d'exploitation opposable non au public mais à ses exploitants. Le public, par les exceptions qui sont tolérées, peut échapper dans certains cas (citation, copie privée, etc.) à des actions en contrefaçon. Or la technologie numérique permet un contrôle de l'accès à l'œuvre et permet une dérive qui implique que chaque usage puisse donner lieu à une demande d'autorisation.*
2. *Les mesures techniques menacent les exceptions au droit d'auteur lorsqu'elles empêchent l'accès à des œuvres qui ne sont pas ou ne sont plus protégées ou l'exercice normal d'une exception reconnue par la loi sur le droit d'auteur.*
3. *La violation de ces mesures par ceux qui ne bénéficient pas des exceptions implique deux sanctions, l'une au nom du droit d'auteur, l'autre pour avoir neutralisé ces systèmes. Cette même violation, par ceux qui ont droit à ces exceptions, leur fait encourir des sanctions pour avoir voulu bénéficier de leurs droits.*
4. *Il sera difficile aux exploitants de démontrer l' »efficacité » d'une protection technique en raison de la rapidité de l'évolution qui la rend rapidement obsolète. Lorsque cette protection peut être violée, le contournement deviendrait-il licite? Et puisque la recherche dans ce domaine doit pouvoir se poursuivre, des dérogations devraient-elles être instaurées ?*
5. *Il devrait être impossible de cumuler une compensation équitable, à l'image de celle qui est prévue pour les copies privées, et une protection technique empêchant d'accéder à une œuvre sans autorisation.*
6. *Ces protections faciliteraient la mise en œuvre d'une cybersurveillance par les producteurs, les employeurs ou d'autres entités, portant atteinte à la vie privée des citoyens ou aux activités des entreprises par le contrôle des usages attribuables à un utilisateur ou un groupe d'utilisateurs donné.*
7. *L'utilité même d'une protection juridique spécifique n'est pas évidente puisque il semble que des dispositifs légaux permettaient déjà de sanctionner ceux qui les auraient neutralisées (comme la loi sur la fraude informatique en France)."*

Au cœur de ces interrogations (et de celles exprimées – avec plus de vigueur – par des associations très critiques, tels l'initiative "EUCD.info") il y a notamment la façon dont va être transposée puis appliquée l'article 6.4 de la directive qui prévoit un processus complexe qui doit tout à la fois inciter les ayant-droits à promouvoir des "mesures volontaires" conciliant leurs mesures techniques avec le respect des exceptions prévus à l'article et donner une possibilité d'intervention aux pouvoirs publics en cas d'abus :

> ***"les États membres prennent des mesures appropriées pour assurer que les bénéficiaires des exceptions ou limitations prévues par le droit national conformément à l'article 5, paragraphe 2, points a), c), d) et e), et à l'article 5, paragraphe 3, points a), b) ou e), puissent bénéficier desdites exceptions ou limitations dans la mesure nécessaire pour en bénéficier lorsque le bénéficiaire a un accès licite à l'œuvre protégée ou à l'objet protégé en question."***

et ce tout en laissant, d'autre part, une entière liberté contractuelle aux diffuseurs lorsqu'ils diffusent des

> ***"œuvres ou autres objets protégés qui sont mis à la disposition du public à la demande selon les dispositions contractuelles convenues entre les parties de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit individuellement."***

Comme on va le voir en étudiant rapidement les différents projets de loi ou textes de transposition déjà adoptés, il en résulte pour chaque État-membre certains choix juridiques et technico-politiques à effectuer, parmi lesquels les deux principaux paraissent être à ce jour :

1°) **la loi doit-elle se contenter d'inciter les ayant-droits et les diffuseurs à faire des propositions de "mesures volontaires", ou doit-elle les y obliger ?**

2°) **de quelle nature doit être le mécanisme de recours en cas de contestations entre les parties en présence concernant la conciliation entre l'usage d'une mesure technique et celui d'une des exceptions au droit d'auteur (recours à un juge, à un médiateur, à un conciliateur, ….?)**

Le risque est donc important que chaque État-membre gère ces questions sensibles selon des modes qui ne s'avèreraient finalement pas compatibles entre eux et qui, créant ainsi des incertitudes juridiques et des aléas techniques (en particulier pour les fournisseurs de contenus et les diffuseurs), rendraient plus difficiles (et peut-être moins intéressant économiquement) la mise en œuvre de mesures techniques pour la protection des droits. L'enjeu de la transposition dans les États-membres est donc important.

B.2. L'état de la transposition des articles 6 et 7 de la directive du 22 mai 2001

La directive du 22 mai 2001 devait être transposée dans les législations des états-membres au plus tard le 22 décembre 2002. Mais à cette date seuls la Grèce et le Danemark avaient achevé leurs processus législatifs en ce sens.

Plus d'un semestre plus tard, la situation n'a que peu progressé. Seule la nouvelle loi autrichienne est entrée en vigueur le 1er juillet 2003 tandis que l'Allemagne paraît avoir voté définitivement un projet de texte mais qui n'est toujours pas officiellement promulgué à ce jour.

Par ailleurs, plusieurs autres États ont établi un projet de texte et ont engagé les travaux législatifs en vue de son approbation. Nous avons ainsi pu prendre connaissance des projets actuellement en discussion en Belgique, au Luxembourg, en France et en Grande-Bretagne.

Sous réserve de la disponibilité des textes, de leur éventuelle traduction et des modifications que pourront encore subir ceux qui n'ont pas encore été définitivement adoptés, on peut établir un premier bilan de la situation législative dans les États-membres ci-dessus mentionnés s'agissant de la transposition des articles 6 et 7 de la directive du 22 mai 2001.

B.2.1. La transposition réalisée en Grèce

La Grèce a choisi un mode de transposition extrêmement fidèle au texte même de la directive. L'article 66A de sa loi sur le droit d'auteur reprend donc très largement les dispositions de l'article 6 de la directive du 22 mai 2001, tandis que son nouvel article 66B reprend celles de l'article 7 de la directive.

Les seuls choix juridiques effectués par la Grèce concerne la mise en œuvre de l'article 6.4 et plus particulièrement deux de ses principaux aspects, à savoir, d'une part, les "mesures volontaires" prises par les ayant-droits pour assurer aux usagers le bénéfice des exceptions ou limitations au droit d'auteur, et d'autre part, le mécanisme par lequel la puissance publique peut prendre les "mesures appropriées" en cas de besoin :

- sur le premier point, le paragraphe 5 de l'article 66A de la nouvelle loi grecque impose aux ayants-droits une obligation de prendre des mesures volontaires au profit des prérogatives des bénéficiaires :
  "the rightholders should have the obligation to give to the beneficiaries the measures to ensure the benefit of the exeption"

- sur le second point, la Grèce a choisi le recours à une médiation qui sera assurée par un médiateur choisi sur une liste tenu par l'administration en charge des questions de propriété intellectuelle, avec en cas d'échec une action contentieuse de premier et dernier ressort devant la Cour d'appel d'Athènes :
  "the rightholders and third parties benefiting from the exception may request the assistance of one or more mediators selected from the list of mediators drawn up by the Copyright Organization"
  et *"if no party objects within one month from the forwarding of the recommendation, all parties are considered to have accepted the recommendation. Otherwise, the dispute is settled by the Court of Appeal of Athens trying at first and last instance."*

B.1.2. La transposition réalisée au Danemark

La transposition danoise effectuée par la loi n° 1051 du 17 décembre 2002 consiste, du point de vue qui nous intéresse, dans les articles 75c à 75e, 76(1)iii et 78 introduits dans la loi danoise sur le droit d'auteur.

Si l'on met de côté les articles 76(1)iii et 78 qui édictent les sanctions pénales applicables aux actes prohibés définis à l'article 75, l'essentiel de la transposition tient à la rédaction des quatre paragraphes (c à e) de ce dernier article.*

Il s'agit d'une transposition assez concise qui ne rentre pas très profondément dans le contenu des définitions posées par la directive. Par exemple, l'article 75c(4) qui définit les mesures techniques faisant l'objet de la protection ne définit pas le qualificatif "efficace" ("effective" dans la traduction anglaise que nous avons consultée) contrairement à ce que propose la directive elle-même. De même, la loi se contente de préciser que les mesures techniques concernées ont pour objectif de "protéger" les œuvres (on peut dès lors considérer que la définition communautaire servira en cas de besoin à interpréter le sens de ce qualificatif dans la loi danoise).

Les choix juridiques effectués concernent, comme en Grèce, l'application de l'article 6.4, à savoir :

- d'une part, l'absence d'obligation imposée aux ayants-droits de proposer des "mesures volontaires",

- d'autre part, le recours à une juridiction (en l'espèce, le *"Copyright Licence Tribunal"* mentionné à l'article 75d(1)) pour imposer en cas de litige avec les usagers le respect des exceptions dont les usagers doivent pouvoir bénéficier.

mais la loi danoise prévoit également dans son article 75c(6) une exception explicite aux interdictions de contournement des mesures techniques aux fins de la recherche cryptographique :

> *"The provisions of subsections (1)-(4) shall not prevent research into cryptography*"

B.1.3. La transposition réalisée en Autriche

La nouvelle loi sur le droit d'auteur en Autriche comporte deux articles 90b et 90c qui transposent respectivement les dispositions des articles 6 et 7 de la directive.

Il s'agit d'une transposition très concise qui se limite à énoncer les actes prohibés portant atteinte d'une part aux mesures techniques (article 90b) et d'autre part aux informations sur le régime des droits (article 90c).

Il ne semble pas que les mécanismes prévus par l'article 6.4 de la directive pour pallier les éventuels conflits entre une mesure technique et l'exercice des exceptions au droit d'auteur et aux droits voisins aient été explicitement établis.

B.1.4. La transposition réalisée en Allemagne

Le parlement allemand ayant approuvé en juillet 2003 une version amendée du texte proposé en 2001 par le gouvernement fédéral, la loi allemande transposant la directive du 22 mai 2001 a été publiée le 12 septembre 2003.*(Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft)*.

Ce texte comporte plusieurs articles spécifiquement consacrés à la protection des mesures et des informations sur le régime des droits.

Son article 95a décrit les mesures techniques protégées par la loi et conformément à la directive et énonce les différents actes de contournement de ces mesures ou qui y sont associés. Son dernier paragraphe indique expressément que ces prohibitions ne sont pas opposables aux autorités publiques agissant dans le cadre de leurs missions de sécurité et de répression pénale. Quant à lui, l'article 108b prévoit les sanctions pénales applicables aux actes de contournement.

Son article 95b est consacré, pour sa part, à la nécessaire conciliation entre l'usage des mesures techniques et les exceptions aux droits d'auteur prévus par la directive. Le législateur allemand a fait le choix d'obliger les ayant-droits à fournir aux usagers légitimes les moyens nécessaires pour qu'ils puissent jouir des prérogatives qui leur sont reconnues au titre de différentes exceptions dont en particulier :

- l'exception pour des motifs de sécurité publique,
- l'exception en faveur des personnes handicapées,
- l'exception à des fins pédagogiques,
- l'exception à des fins de recherche,
- l'exception de copie privée

Dans le cas où l'ayant droit ne permet pas aux usagers de bénéficier de ces différentes exceptions, le paragraphe (2) de cet article 95b prévoit que l'usager peut agir pour en obtenir le bénéfice sauf dans deux cas (conforme à l'article 6.4. de la directive) :

- si des accords volontaires ont été conclus entre ayant-droits et usagers,
- si l'usager a accédé au contenu protégé dans le cadre d'un service "à la demande" et selon des conditions contractuelles convenues.

Mais l'interprétation de l'article 108b semble faire ressortir que le contournement direct d'une mesure technique par l'utilisateur légitime lui-même en vue de profiter de l'une des exceptions qui lui sont reconnues ne serait pas sanctionné pénalement.

L'article 95c du projet reprend, lui, les dispositions de l'article 7 de la directive relative à la protection des informations sur le régime des droits.

Plus original et plus remarquable (car ne découlant pas explicitement de la directive, même s'il en constitue une conséquence logique) nous paraît être l'article 95d. Il impose à celui qui met en œuvre des mesures techniques de le mentionner aux usagers, d'en indiquer la nature et de préciser ses coordonnées (nom, entreprise, adresse) afin que les usagers puissent le contacter en cas de difficulté pour rendre compatible la mesure technique concerné avec le respect des exceptions rappelées à l'article 95b(2). :

§ 95d Kennzeichnungspflichten

(1) Werke und andere Schutzgegenstände, die mit technischen Maßnahmen geschützt werden, sind deutlich sichtbar mit Angaben über die Eigenschaften der technischen Maßnahmen zu kennzeichnen.

(2) Wer Werke und andere Schutzgegenstände mit technischen Maßnahmen schützt, hat diese zur Ermöglichung der Geltendmachung von Ansprüchen nach § 95b Abs. 2 mit seinem Namen oder seiner Firma und der zustellungsfähigen Anschrift zu kennzeichnen. Satz 1 findet in den Fällen des § 95b Abs. 3 keine Anwendung.

B.1.5. La transposition en cours en Belgique

A notre connaissance le projet de loi belge transposant la directive du 22 mai 2001 a fait l'objet dans son dernier état d'amendements proposés par le Sénat le 18 octobre 2002.

A la lecture de ce texte amendé, on constate que la Belgique a choisi de transposer de manière assez fidèle les termes de la directive. Possédant une loi distincte régissant les bases de données, elle se propose donc d'introduire des modifications d'une part dans la loi la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins, et d'autre part, dans la loi du 31 août 1998 transposant en droit belge la directive européenne du 11 mars 1996 concernant la protection juridique des bases de données.

Les choix juridiques effectués dans ce projet belge se limitent – comme dans d'autres États-membres – aux conditions d'application des dispositions de l'article 6.4. de la directive :

- l'adoption de mesures volontaires par les titulaires est présentée comme une obligation à la charge de ceux-ci, dans le projet d'article 79bis §2 qui indique :
  "Les titulaires de droits prennent des mesures volontaires, y compris des accords avec les autres parties concernées, afin de fournir à l'utilisateur d'une œuvre ou d'autres objets protégés, les moyens nécessaires pour pouvoir bénéficier des exceptions ...".
  et ce n'est qu'en cas de défaillance des titulaires en la matière que la puissance publique interviendra :
  "§ 3. Si dans le délai d'un an à compter de l'entrée en vigueur de la présente loi, aucune mesure volontaire adéquate au sens du § 2 n'a été communiquée par les titulaires de droits au délégué du ministre visé à l'article 76, le Roi prend dans l'intérêt général les dispositions appropriées imposant aux titulaires de droits concernés, de fournir à l'utilisateur d'une œuvre ou d'autres objets protégés, les moyens nécessaires pour pouvoir bénéficier des exceptions ...."

- Comme on peut le constater à la lecture du §3 ci-dessus rappelé, le seul recours organisé en cas de conflits entre mesures techniques et exceptions consistera en une intervention contraignante de l'Administration ("Le Roi"), ce qui différencie la voie belge de celles suivies par plusieurs des autres états-membres (qui privilégie plutôt soit la voie juridictionnelle, soit celle de la médiation).

Ces deux remarques valent dans les mêmes conditions pour l'application des mesures techniques aux bases de données, le projet d'article 6bis de la loi du 31 août 1998 étant identique sur ces points à celui de l'article 79bis ci-dessus.

B.1.6. La transposition en cours au Luxembourg

Le projet de loi luxembourgeois a été déposé devant le Parlement le 14 mai 2002. Il modifie les dispositions de la loi du 18 avril 2001 relative à la protection des droits d'auteur.

Proche du texte et des définitions données par la directive, le projet luxembourgeois a choisi comme en Belgique d'imposer aux titulaires de droits l'adoption des mesures destinés à permettre la mise en œuvre des exceptions aux droits qui sont reconnus au profit des usagers. L'Article 71-2 de ce projet indique bien que

> *"Nonobstant la protection juridique des mesures techniques, les titulaires de droits doivent prendre les mesures nécessaires, notamment par la voie contractuelle, afin de garantir aux bénéficiaires des exceptions ..."*

En revanche, le mécanisme de règlement qui devrait être mis en œuvre en cas de défaut d'adoption de ces mesures nécessaires, paraît se limiter en la possibilité pour l'usager concerné "d'intenter une action en cessation conformément à l'article 81 de la présente loi afin de faire cesser l'application des mesures techniques qui entravent

l'exercice desdites exceptions." On se rattache donc là à un pur mécanisme juridictionnel.

B.1.7. La transposition prévue en France

En France, le Conseil supérieur de la propriété littéraire et artistique (CSPLA) siégeant auprès du ministère de la Culture a été chargé de préparer l'avant-projet de loi de transposition. Bien que cet avant-projet ait subi différentes modifications lors de son examen par les différents ministères avant d'être présenté au Parlement (sans doute au 4ème trimestre 2003), une version intermédiaire non officielle a été diffusée en ligne (en avril 2003).

Ce texte présente une transposition assez détaillée des dispositions des articles 6 et 7 de la directive et propose une modification des dispositions du Code de la propriété intellectuelle, concernant tout à la fois le droit d'auteur, les droits voisins et les prérogatives reconnues aux producteurs de base de données.

Les définitions des mesures techniques et des informations sur le régime des droits (qui seraient dénommées *"informations sous forme électronique concernant le régime des droits"*) sont très proches de celles données par les articles 6 et 7 de la directive.

Les actes qui seraient prohibés pour assurer la protection de l'un ou l'autre de ces éléments font l'objet d'une énumération assez détaillées. Mais s'agissant des actes concernant les mesures techniques, on peut s'étonner que le projet d'article L335-3 sanctionne d'une manière générale

> *"Le fait pour une personne de porter atteinte en connaissance de cause, ou en ayant des raisons valables de penser porter atteinte, à toute mesure technique"*

alors que la directive ne prévoit une protection qu'à l'encontre du seul *"contournement"* des mesures techniques.

On note également que, concernant l'article 6.4 de la directive, ce projet français semble avoir fait le choix d'imposer aux ayants-droits une obligation de prendre ("dans un délai raisonnable") des "mesures volontaires" (projet d'article L.331-6). De même, ce texte se rallie comme d'autres à la possibilité de recourir à des médiateurs. Un collège de trois médiateurs serait en effet institué par le projet d'article L331-7, lequel aurait la possibilité d'enjoindre éventuellement aux ayant-droits de prendre les *"mesures appropriées pour permettre le bénéfice effectif de l'exception"*.

B.1.8. La transposition prévue en Grande-Bretagne

On ne connaît actuellement que l'avant-projet diffusé l'an dernier pour consultation par l'UK Patent Office. Ce texte comporte notamment deux sections assez complètes et détaillées proposant des amendements à la loi britannique de 1998 sur le copyright sur la base des articles 6 et 7 de la directive.

S'agissant des mesures techniques, cet avant-projet a fait le choix de régler la question de la conciliation entre leur mise en œuvre et les exceptions aux droits d'auteur, en prévoyant la possibilité pour l'usager d'émettre une plainte auprès du Secrétaire d'État (section intitulée *"Remedy when effective technological measures prevent permitted acts"*), lequel ministre serait alors chargé de délivrer le cas échéant à l'ayant droit ou à son licencié une injonction. Il s'agirait donc là du choix d'un mécanisme administratif.

Concernant tant la protection des mesures techniques que celle des informations sur le régime des droits, on peut noter également que le projet britannique précise (sans doute dans un but d'efficacité répressive) que le droit d'engager une action à l'encontre des actes illicites reviendrait concurremment aux titulaires des droits et à la personne assurant la communication au public des contenus protégés (article 296ZA(2)-(3), 296ZC(2)-(3) et 296ZE(3)-(4)).

B.3. L'exposition différente des États-membres aux risques de contrefaçon numérique

Les effets de la mise en œuvre des moyens de sécurité dans les États-membres vont dépendre non seulement du cadre juridique résultant de la transposition de la directive du 22 mai 2001, mais aussi de la plus grande exposition de ces États aux risques de contrefaçon numérique.

Il existe, en effet, à côté de la contrefaçon traditionnelle d'objets matériels une nouvelle forme de contrefaçon en plein développement qui consiste à reproduire des éléments immatériels existant sous forme purement numérique et à les redistribuer, le cas échéant, par la voie des réseaux en ligne [153].

Le volume de cette contrefaçon numérique est encore plus difficile à apprécier que celui de la contrefaçon traditionnelle (pour laquelle, les saisies douanières et policières constituent une base de calcul et de comparaison sur longue période). De plus, le développement de nouvelles technologies de reproduction (disponibilité de moyens de stockage de grande capacité, de graveurs de CD et de DVD) et de transmission (techniques de compression, logiciels peer-to-peer) favorisent son accroissement et sa décentralisation (décentralisation qui est, depuis l'origine, l'une des caractéristiques de la contrefaçon liée à l'Internet, cf. [151]).

Quelques éléments globaux concernant des domaines particulièrement touchés permettent néanmoins de se faire une idée des volumes et de l'évolution générale de la contrefaçon numérique :

- concernant les industries phonographiques, l'IFPI
    - considère qu'en 2002 le volume des ventes de disques aurait diminué de 8% en volume et de 9% en valeur (ce qui constituerait un indice de l'accroissement du volume mondial de la contrefaçon des œuvres phonographiques) ;
    - constate une numérisation croissante de cette contrefaçon, car les supports informatiques comme le CD-R (CD-Rom enregistrable) représentent une part croissante des saisies effectuées (de 9% en 2000 à 28% en 2002) alors qu'au contraire les cassettes audio perdent leur positions (de 65% en 2000 à 40% en 2002) ;
    - évalue à 700 millions le nombre de fichiers pirates en circulation ou 99% de la musique en ligne, et estime à 500 millions les fichiers disponibles sur des plates-formes d'échange *peer to peer*.

- concernant les industries cinématographiques,
    - les industriels américains du secteur estimaient avoir subi pour l'année 2002 des pertes comprises entre 1,3 et 4 Mds $ [89],
    - une étude a évalué l'accroissement très soutenu du nombre de sites proposant des téléchargements de films en streaming[2] a considérablement augmenté, passant de 78.000 en juin 2001 à 400.000 en juin 2002,
    - le nombre de films téléchargés illégalement chaque jour dans le monde est passé de 300.000/500.000 en 2001 à 400.000/600.000 en 2002,
    - le nombre de films disponible illégalement sur le réseau aurait augmenté de 20% sur la même période. [156].

- concernant les logiciels professionnels, BSA (Business Software Alliance)
    - a enregistré en 2002 une légère baisse
    - mais évalue encore le coût économique du piratage de logiciel à plus de 13 milliards de dollars [63].

Les parts et la répartition de cette contrefaçon touchant les contenus numériques en Europe ne peuvent pas non plus être facilement évalués. On retiendra cependant quelques éléments qui semblent refléter la situation présente.

B.3.1. Une contrefaçon plus faible dans l'Union européenne que dans d'autres parties du monde

Les chiffres collectés par l'industrie phonographique sont là encore l'une des sources principales d'évaluation. Selon l'IFPI, l'Union européenne serait moins touchée par la contrefaçon de musique que la moyenne du reste du monde, puisque le recul des ventes de CD ne serait en 2002 qu'environ 3% (mais 4% si l'on étend l'Europe à ses nouveaux entrants) contre 8% au niveau mondial.

De même, les évaluations de piratage en matière de logiciel fournies par l'association BSA montrent que l'Europe occidentale demeure une zone modérément touchée avec un taux de contrefaçon qui serait autour de 35% (ce qui demeure cependant encore élevé dans l'absolu, mais qui témoigne d'un recul de 17 points sur les huit dernières années) [63].

Cette situation d'exposition limitée de l'espace communautaire aux risques de contrefaçon doit cependant être pondérée dans la mesure où :

- certains États-membres présentent des taux nationaux de contrefaçon élevés (cf. infra B.3.2.),
- le développement des réseaux numériques haut-débit va décloisonner la situation européenne de la situation mondiale (puisque les sources de contenus piratés seront de plus en plus accessibles depuis le continent européen),
- les nouveaux entrants (en particulier les pays d'Europe centrale et orientale, comme la Pologne ou la Tchéquie) devraient, dans un premier temps, renforcer les statistiques de contrefaçon de l'Union, puisqu'ils sont encore aujourd'hui des pays très exposés à ce risque.

B.3.2. Une contrefaçon qui touche néanmoins plus fortement certains pays européens sensibles

Trois États-membres sont généralement considérés comme particulièrement sensibles aux différentes formes de contrefaçon, en particulier dans le domaine numérique. Il s'agit de :

- l'Italie,
- l'Espagne, et de
- la Grèce

pays qui tous les trois cumulent à la fois une forte présence de la contrefaçon de musique et de logiciels (cf. le tableau ci-dessous publié par BSA).

Évolution du taux de piratage
des logiciels professionnels en Europe Occidentale

	2001	2002
Allemagne	34 %	32 %
Autriche	33 %	30 %
Belgique/Luxembourg	33 %	31 %
Danemark	26 %	24 %
Espagne	49 %	47 %
Finlande	27 %	25 %
France	46 %	43 %
Grèce	64 %	63 %
Irlande	42 %	42 %
Italie	45 %	47 %
Norvège	34 %	32 %
Pays-Bas	39 %	36 %
Portugal	43 %	42 %
Royaume-Uni	25 %	26 %
Suède	31 %	29 %
Suisse	33 %	32 %

TOTAL EUROPE OCC.	37 %	35 %

(source BSA, rapport annuel, 2003)

Ces statistiques montrent d'ailleurs que d'autres pays sont en matière de logiciels dans une situation proches des leurs (notamment le Portugal, l'Irlande et la France).

En Italie, la contrefaçon de produits couverts par les droits d'auteur et les droits voisins (dont une partie croissante sont distribués ou copié sous forme numérique) s'élèveraient – d'après les estimations de l'IIPA – à :

- 20% du marché local en ce qui concerne les films (vidéo et DVD)
- 23% du marché local en ce qui concerne la musique (27% selon les derniers chiffres de l'IFPI),
- 45% du marché local en ce qui concerne les logiciels professionnels, et
- 74% du marché local en ce qui concerne les jeux vidéos

Concernant particulièrement le domaine phonographique, l'IFPI rapporte une augmentation assez nette des saisies de CD-R pirates en 2001 et 2002 et le démantèlement de nombreux sites clandestins de reproduction de CD, la copie sur CD enregistrables représentant dorénavant 82% des contrefaçons de musique effectuées en Italie.

Un renforcement de la loi réprimant la contrefaçon de droits d'auteur a déjà été réalisé en août 2000. Mais ses effets pourraient être accrus ensuite avec l'entrée en vigueur des dispositions issus de la directive du 22 mai 2001.

Quant à l'Espagne et à la Grèce, il s'agit de deux pays dans lesquels la croissance de la copie pirate de CD-audio (là aussi sur support CD-R) a été très importante sur ces dernières années. On estime d'ailleurs qu'en Grèce, la moitié du marché des CD commercialisés dans le pays relève de la contrefaçon.

Mais à côté de ces pays européens sensibles, la contrefaçon numérique touche progressivement d'autres États-membres qui n'ont pas d'antécédents liés à la contrefaçon traditionnelle.

On peut s'en apercevoir en évoquant les résultats d'une étude nationale qu'a fait réalisé l'IFPI par l'institut GFK en 1982 concernant l'Allemagne.

L'enquête dénombre 1,.1 million de personnes qui copient des fichiers musicaux sur des CD vierges, ce qui a pour conséquence (avouée dans 17,5% des cas) de diminuer les achats de CD d'origine De même, elle évalue à 4.9 millions le nombre de personnes qui téléchargent gratuitement (et généralement sur des sites pirates) de la musique numérisée (ce qui induit chez près de 20% de ces personnes un moindre besoin d'acquérir des CD commerciaux..

En France le phénomène ne semble pas substantiellement différent, mais s'y ajoute les taux traditionnellement élevés (bien qu'en baisse progressive) de piratage de logiciels commerciaux (évalués encore à 43%, malgrè une baisse tendancielle depuis plusieurs années).

L'arrivée progressive (et semble t'il, plus lente que prévue) des technologies de sécurité et des architectures de DRM s'effectue donc dans un contexte économique et commercial marqué par une banalisation progressive de la contrefaçon numérique en Europe. Cette situation peut avoir des effets ambivalents sur l'avenir de ces moyens de sécurité.

D'un côté, le maintien ou un accroissement régulier des faits de contrefaçon inciteront les professionnels de l'industrie et les pouvoirs publics à recourir à des solutions innovantes et efficaces pour enrayer l'évolution. Et dans cette hypothèse, on ne peut exclure que l'opinion publique et les consommateurs finissent par adhérer aux objectifs de lutte contre la contrefaçon numérique et comprennent qu'il convient de préserver les industries culturelles et d'éviter une dégradation trop rapide de leurs sources de revenus.

Mais de l'autre côté, on peut aussi envisager que la persistance d'un niveau structurel de contrefaçon numérique et que les difficultés (techniques, juridiques et commerciales) à imposer les DRM fassent finalement opter l'opinion publique et les principaux acteurs du marché pour des modèles économiques et techniques différents.

Là encore, les suites de l'application des dispositions issues de la transposition de la directive du 22 mai 2001 nous donneront certains indices sur cette évolution possible à moyen terme.

PARTIE C : COMPLEMENTS TECHNOLOGIQUES

Cette partie complète et précise, sans prétendre à aucune exhaustivité, certains aspects technologiques utilisés ou invoqués dans la partie A. Plus précisément, après un bref historique retraçant le passage du monde analogique au monde numérique (C.1), il nous a semblé utile de rappeler dans la première partie certains éléments concernant l'unité de mesure utilisée dans le monde numérique, à savoir le bit (C.2).

Nous poursuivons en décrivant les supports de stockage de données numériques du type CD/DVD (C.3). Et comme les informations numériques, (photos, vidéos, sons, fichiers de données ou même modules logiciels) sont le plus souvent compressées avant un envoi via, ou une mise à disposition sur Internet, ou sur les supports physiques déjà décrits, nous évoquons donc ensuite la question des techniques de compression, principalement dans le domaine des images et dans le domaine audio (C.4). La cryptographie à clef secrète, à clef publique et les signatures électroniques sont des éléments essentiels de la gestion des droits, et nous décrivons ici certains standards (C.5.1). Cela ne saurait suffire pour la gestion des droits dans le domaine des données numériques, comme la musique, les photos, ou les vidéos, pour lesquelles il est fait appel à la notion de filigrane (ou encore de watermarking), notion que nous illustrons dans la partie C.5.2.

Enfin, dans la partie C.5.3, nous traitons des mesures dites de codes régionaux et des mesures intégrées de protection contre la copie des CD/DVD.

C.1.- Monde analogue et monde numérique : du phonographe au lecteur de DVD

L'histoire attribue à l'année 1877 et à Thomas Edison la construction du premier appareil capable d'enregistrer et reproduire des sons. Dans son approche originale du phonographe, un diaphragme contrôlait une aiguille, et celle-ci « grattait » un signal analogique sur une feuille d'étain cylindrique. Ainsi, on parlait dans l'appareil, en même temps que l'on faisait tourner le cylindre, et l'aiguille enregistrait les paroles sur la feuille, en reproduisant les vibrations recueillies par le diaphragme. Pour la reproduction des sons, l'aiguille n'avait qu'à suivre l'impression présente sur la feuille : en effet, les vibrations ainsi éprouvées par l'aiguille étaient transmises au diaphragme, qui reproduisait ainsi les sons.

Le système a connu une amélioration importante due à Emil Berliner en 1887, avec la mise au point du gramophone, et des disques plats avec une rainure en spirale, ce qui a permis une production industrielle de ces disques plus aisée. Parmi les problèmes de l'approche analogique, on compte celui de la fidélité (adéquation entre le signal enregistré et celui émis), et celui de l'altération, à chaque reproduction, du signal enregistré. L'objet des supports de type Compact Disc (CD, voir plus bas) est précisément de remédier à ces inconvénients. En pratique, l'enregistrement digital convertit les ondes analogiques en un flux de nombres, et enregistre ces nombres en lieu et place de l'onde, à l'aide d'un convertisseur analogue vers digital. Inversement, pour reproduire les sons (par exemple), on utilise un convertisseur digital vers analogue (DAC : digital-to-analog converter), et les ondes sont au besoin

amplifiées afin de rendre le son enregistré. Aussi longtemps que le flux de nombres enregistré n'est pas modifié, les ondes produites par le DAC seront les mêmes.

L'enregistrement et la reproduction seront donc d'autant plus fidèles que le convertisseur analogue vers digital a opéré avec un échantillonnage à haut taux, et à produit des nombres appropriés. Pour un CD-Audio (voir plus bas), le taux d'échantillonnage est de 44100 échantillons par seconde (44,1 kHz), avec un nombre de graduations de 65536 (sur 16 bits). Un DVD-Audio a des capacités encore plus importantes (192000 échantillons par seconde, soit un taux de 192 kHz, et une précision sur 24 bits). Dans le monde numérique, comme on vient de le voir, l'information n'est plus représentée par des données continues (ondes), mais discrètes, dont l'unité de mesure élémentaire est le bit

C.2.- L'unité atomique d'information numérique

Les informations numériques sont, comme le nom l'indique, représentées par des nombres. Ces nombres à leur tour, admettent des représentations dans des bases quelconques. Ainsi, le système décimal n'est autre que le fait de représenter les nombres en base 10. Notre représentation des heures fait, elle, appel à la représentation en base 60. Pour un ordinateur, la représentation la plus commode (et pour l'usager la plus économique) se fait en base 2, et l'unité élémentaire d'information est le bit, abréviation debinary digit. Un bit est donc une quantité valant 0 ou 1, et un nombre de représenté, par exemple, par 11 bits, avec le bit de plus fort poids à gauche correspond, approximativement, à un nombre de l'ordre de 1000 en système décimal. Par exemple, 1000000000 est l'écriture binaire du nombre décimal 1024. Les bits sont usuellement regroupés en paquets de 8, appelés octets ou bytes. Enfin, les capacités des ordinateurs, ou des mémoires se déclinent en Kilobytes, Mégabytes, Gigabytes, Terabytes, etc. La table suivante montre les correspondances pour les quatre préfixes cités :

Nom	Abréviation	Taille
Kilo	K	$2^{10} = 1024$
Mega	M	$2^{20} = 1048576$
Giga	G	$2^{30} = 1073741824$
Tera	T	$2^{40} = 1099511627776$

On constate que un kilo est approximativement égal à mille, un méga à un million, un Giga à un milliard, etc. On parle alors de Kilo-octets ou Kilo-Bytes (Ko ou KB), de Méga-octets ou Méga-Bytes (Mo ou MB), etc.

C.3.- Les supports de stockage et les lecteurs/graveurs de CD/DVD

Les données numériques sont stockées sur différents supports. Nous en évoquons quelques-uns dans cette partie, en commençant par les CD (Compact Disc) et DVD (Digital Versatile Disc). L'aspect extérieur de ces objets est identique depuis 1982, année de leur apparition : il s'agit de disques optiques de 12 cm de diamètre, et de 1,2 mm d'épaisseur. Ils sont constitués de matière plastique (polycarbonate), recouvert d'une fine pellicule métallique sur (au moins) l'une des faces. Cette matière plastique est gravée en une longue spirale d'information, représentée sous forme d'alvéoles d'une certaine profondeur, séparées par des espacements, formant ainsi un code binaire : une alvéole correspond à un 0, et un espace à un 1. Par

exemple, une séquence du type 11001010 se matérialise sous la forme de deux espaces, deux trous, un espace, un trou, un espace, un trou. La spirale débute au centre du CD, et se déroule vers l'extérieur (de par la petitesse de l'épaisseur de la spirale, sa longueur est de plusieurs kilomètres). Enfin, les capacités de stockage sont fonction du type considéré : simple/double face, simple/double couche.

Bien que les caractéristiques globales des CD et DVD soient similaires, ils se déclinent sous une douzaine de formats, dépendants des types d'utilisation ou des fonctionnalités d'enregistrement.

C.3.1.- Les CD-Audio

Dans le cas des CD, les alvéoles dont il est fait mention ci-dessus ont une profondeur de 0,83 µ, et les espaces une longueur de 1,6 µ. Schématiquement, la première génération de CD concerne les CD-Audio et les CD-ROM.

Un CD-Audio (parfois seulement appelé CD), est une mémoire stockant des données audio (en pratique, jusqu'à 74 minutes de musique). Un CD-ROM (Read Only Memory) est une mémoire stockant des données multimédia : audio (musique), texte (programmes informatiques écrits en langage C par exemple), ou encore de la vidéo, des jeux ou des programmes éducatifs.

A contrario, les CD-R et les CD-RW sont des disques optiques gravables. Ainsi un CD-R est un disque a priori vierge au départ, qui peut être gravé une fois, en enregistrant tous types de données. Un CD-RW offre la souplesse d'être réenregistrable, et supporte tous types de données. En pratique, il peut être regravé jusqu'à 1000 fois sans détérioration patente des données.

C.3.2.- Les DVD

Les DVD ont des capacités largement plus grandes que celles des CD. En effet, les alvéoles ont dans ce cas une taille de 0,4 µ et les espacements de 0,74 µ. Les formats reconnus actuellement par le DVD-Forum sont au nombre de six.

Les DVD-Vidéo sont des DVD où sont enregistrés en règle générale des films, destinés à être visionnés sur des appareils " de salon ". La technologie sous-jacente aux DVD-ROMs est la même que celle des DVD-Vidéos, mais peut également stocker d'autres formats. C'est l'analogue du CD-ROM.

Le DVD-R est l'analogue du CD-R, et est enregistrable une fois. Le DVD-RAM fait du DVD un disque dur virtuel, qui peut être réenregistré jusqu'à 100.000 fois. Le DVD-RW est également un DVD réenregistrable (jusqu'à 1.000 fois), avec quelques particularités techniques par rapport au DVD-RAM. Un autre format existant de DVD réenregistrable est le DVD-RW+, mais n'est pas à l'heure actuelle approuvé par le DVD-Forum. En revanche, le DVD-Audio l'est, et est destiné à la musique de très haute fidélité.

Les DVD permettent de nombreuses fonctionnalités : ils permettent par exemple de stocker jusqu'à 3 heures de vidéo compressée au format MPEG-2 (voir plus bas), avec un taux de

compression de 40:1, et une qualité de son de type CD-Audio, ou encore d'offrir des sous-titres en 32 langues, ou encore de permettre des visionnements des films dans des formats variés (format TV standard ou format letterbox).

C.3.3.- D'autres supports de mémoire

Les supports précédents co-existent avec d'autres, dont nous citons quelques-uns ci-dessous, sans entrer davantage dans les détails.

- Disques durs : le support est ici magnétique. C'est évidemment un support important de stockage, et nous reviendrons sur cet aspect en connexion avec la gestion des droits sur Internet.

- Flash Memory : A la différence d'un CD et DVD, qui sont des mémoires optiques, ce support est une mémoire solide (de type EEPROM, donc ROM). Parmi les exemples les plus adaptés à la présente étude, citons les CompactFlash, les SmartMedia, les Memory Stick, utilisés en particulier dans les caméras numériques.

- D'autres supports sont par exemple magnéto-optiques, comme le MiniDisc de Sony (qui est représenté sous la forme d'un objet carré de 7 cm de côté). Un Mini-Disc se comporte de manière analogue à un Floppy-Disc, à ceci près que sa capacité de stockage est environ 100 fois plus importante. Sous sa forme pré-enregistrée, un MiniDisc est comme un CD, mais plus petit, et stocke environ 5 fois moins de données. Cependant, en mode Audio, le MiniDisc utilise une technique de compression numérique, ATRAC (Adaptive Transform Acoustic Coding), qui compresse par un facteur 5 les données audio, avec une déperdition d'information (schématiquement, la musique est modifiée lors de la décompression), si bien que les capacités de stockage audio du MiniDisc sont similaires à celles d'un CD pour lequel aucun mode de compression n'aurait été utilisé. Nous reviendrons dans la section suivante sur les techniques de compression des données multimédia. Un MiniDisc peut également être vierge a priori et enregistrable. En outre, l'enregistrement et le réenregistrement de musique se fait de manière beaucoup plus souple que sur une cassette usuelle.

C.3.4.- Les capacités comparées de stockage

Le tableau suivant permet de se faire une idée sur les performances de stockage des différents supports respectifs de type CD et DVD (*sf* est mis pour simple face, *df* pour double face, *sc* pour simple couche et *dc* pour double couche). Dans l'estimation de temps musical correspondant, les données sont supposées ne pas être compressées (avec des modes de compression, dont nous parlerons dans la partie suivante, on atteint des capacités de stockage en équivalent de temps de musique beaucoup plus important). On aurait pu procéder de la même manière par équivalence en temps vidéo de stockage et prendre comme base de comparaison le CD-ROM.

Type de support	Capacité	Temps musical équivalent	Nombre de CD équivalent
CD	650 Mo	1h14mn	1
DVD sf/sc	4,7 Go	9h30mn	7
DVD sf/dc	8,5 Go	17h30mn	13

DVD df/sc	9,4 Go	19h	14
DVD df/dc	17 Go	35h	26

C.3.5.- Les lecteurs et graveurs de CD et de DVD

Les lecteurs de CD et DVD fonctionnent sur le même principe. Un rayon laser parcourt la surface du disque lorsque celui-ci tourne, pour rendre compte des alvéoles et espacements (il suit la spirale allant vers l'extérieur). Dans le cas d'un lecteur DVD, celui décode de surcroît la vidéo stockée en format MPEG-2, et retourne un signal vidéo standard. La longueur d'onde du laser du lecteur DVD est toutefois plus petite (640 nanomètres) que celle du lecteur CD (780 nanomètres).

Les graveurs de CD et DVD ont pour objet de permettre l'enregistrement de données sur ces supports, et fonctionnent en créant les alvéoles et espacements sur les CD ou DVD. Au delà des versions destinées à l'industrie, des modèles grand public se sont fait jour (tel par exemple le DVR-A03 de Pioneer, qui arrivera sur le marché européen en mai 2001), qui permettent le montage de discothèques et vidéothèques personnelles.

C.4.- Les techniques de compression et les standards correspondants

Afin de permettre de stocker beaucoup d'information sur un support de capacité limitée, ou encore de transmettre beaucoup d'information via Internet, il est fait usage de techniques de compression, faisant appel à des approches perceptives (e. g. on ne voit pas ou on n'entend pas les modifications). Celles-ci concernent aussi bien les images fixes, que les vidéos ou la musique.

C.4.1.- Codage des images fixes : JPEG 2000 et al.

Un fichier numérique stockant une image doit définir la couleur exacte de chaque pixel. Typiquement, sur Internet, une photo est représentée par 400 fois 400 pixels. Afin de définir parfaitement l'image, il est nécessaire d'attribuer des valeurs à 24 bits par pixel, ce qui représente environ 460 Ko. C'est donc pour des raisons de gestion de tels fichiers que des méthodes de compression d'image ont été étudiées. En particulier, sous l'impulsion du Joint Photographic Experts Group (abrégé en JPEG, et désignant précisément le groupe de travail de normalisation ISO/IEC/JTC1 SC29/WG1, qui se réunit trois fois par an, voir le site Internet officiel [12]), plusieurs standards ont été mis au point. A l'heure actuelle, parmi les formats de représentation des images, on compte (les formats suivants ne sont pas tous dus à JPEG) le format GIF, JPEG ([119]), MPEG-4 Visual Texture Coding (VTC, [13], voir également le paragraphe suivant sur les standards MPEG), JPEG-LS ([14]), ou encore PNG ([15]). En pratique, le choix de telle ou telle méthode dépend fortement de l'application visée, et un point d'équilibre est à trouver entre le degré de sophistication que l'on s'autorise au regard du but visé.

Plus précisément, JPEG ([119]) désigne un standard depuis le début des années 1980 (ISO/ITU-T 10918-1), qui se décline en plusieurs modes, dits « baseline », « lossless », « progressive » et « hierarchical ». Le premier mode, et le plus populaire, se concrétise schématiquement comme suit : l'image est divisée en 8x8 blocs, et on fait agir une DCT

(Discrete Cosine Transform) sur chacun. Les blocs ainsi transformés subissent encore quelques opérations (scannage en zig-zag, entropie via le code de Huffman, etc.).

MPEG-4 VTC ([13]) désigne l'algorithme utilisé dans MPEG-4 pour comprimer les images fixes. L'approche est basée sur DWT (Discrete Wavelet Transform), et sur des codes arithmétiques. Il peut en outre encoder des objets façonnés de manière arbitraire. Des objets différents peuvent être traités séparément, éventuellement avec des qualités de traitement différentes, et être recomposée au niveau du décodeur pour fournir l'image finale décodée.

JPEG-LS ([14]) est un standard ISO-ITU-T pour l'encodage « lossless » des images fixes. Il fournit également une compression dite « near-lossless » Le code adopté ici est celui de Golomb.

PNG ([15]) est une recommandation W3C, destinée à remplacer GIF (et ne serait pas protégée par des brevets), en incorporant davantage de fonctionnalités que GIF. L'algorithme est basé sur un schéma prédictif et un code d'entropie (analogue à celui de l'utilitaire de compression Zip, qui est basé sur LZ77 couplé avec un code de Huffman). PNG (tout comme GIF) ne supporte que la compression de type « lossless ».

Dans la version la plus récente, JPEG 2000 (dont la partie 1 est déjà un standard qui va être publié sous l'appellation ISO/IEC 15444-1:2000, un travail ayant débuté en 1996, voir [10], [11]), la technique de compression proposée est basée sur la théorie mathématique des ondelettes (DWT), mais c'est essentiellement en ce qui concerne les fonctionnalités proposées que ce standard est riche. Par exemple, l'une d'entre elles consiste en la possibilité de coder des photos avec des régions d'intérêt (ROI: Region Of Interest). Cela permet, à l'aide d'autres fonctionnalités inclues dans JPEG-2000, de sélectionner des parties de l'image qui seront envoyées avant les autres vers le décodeur. Ce dont à besoin le décodeur est essentiellement une indication des emplacements (en pratique les décalages dans le flux des informations) que devront avoir ces différents objets dans la photo finale. L'une des applications de ces fonctionnalités, sur Internet, consiste, lorsque l'on récupère une page Web comportant des photos, de pouvoir se faire une idée très rapidement du contenu de la photo, qui s'affiche à l'écran avec une précision de plus en plus grande. Dans des approches différents, la récupération d'une telle photo peut se faire ligne à ligne, et un temps non négligeable peut s'avérer nécessaire avant que l'on ait idée du contenu.

Le document final IS 15444 est en outre doté des parties (complètes ou quasi-complètes) 2 (extensions), 3 (Motion JPEG 2000), 4 (Conformance) et 5 (Reference software) et 6 (Compound image file format). Quatre nouvelles parties sont en cours de développement, en particulier la partie 4 (JPSEC, security aspects) très importante pour cette étude, à laquelle se rajoute la partie 9 (JPIP, interactive protocols and API), 10 (JP3D, volumetric imaging) et 11 (JPWL, wireless applications)

Les mérites comparés de ces différents standards ([128], [129], [67]) font ressortir que JPEG-2000 constitue un véritable progrès davantage sur le plan des fonctionnalités, que sur celui de la compression proprement dite. Sur ce plan, même si les techniques de compression des nouveaux standards sont (à l'exception de JPEG-LS) très sensiblement plus élaborés que dans JPEG, les gains ne paraissent pas substantiels.

C.4.2.- MPEG

Le Moving Picture Expert Group (abrégé en MPEG, et désignant le groupe de travail de normalisation ISO/IEC/JTC1 SC29/WG11, qui se réunit également trois fois par an à des dates souvent compatibles avec les réunion JPEG, car l'intersection entre les deux groupes n'est pas vide, voir le site MPEG officiel [16]), s'attache à définir les standards concernant le codage compressé d'informations audio-visuelles (e. g. films, vidéos, musique). A l'heure actuelle, le groupe de travail a produit les standards suivants :

- MPEG-1 : concerne les domaines vidéo et audio (approuvé en novembre 1992, voir [17], [18], [19], [20], [21], [22], [23], [24], [25], [26]),

- MPEG-2 : standard pour la télévision numérique (approuvé en novembre 1994, voir [27], [28], [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44]),

- MPEG-4 : le standard des applications multimédia (approuvé dans sa version 1 en octobre 1998, et dans sa version 2 en décembre 1999, voir [74]).

MPEG développe conjointement

- MPEG-4 : versions 3, 4, 5,

- MPEG-7 : le standard de représentation du contenu pour la recherche d'information multimédia, le filtrage, la gestion (approuvé en septembre 2001).

Enfin, MPEG a initié MPEG-21, destiné à produire une architecture multimédia. Les algorithmes définis par la communauté MPEG sont également confrontés à des standards propriétaires. Il semble adéquat pour la clarté de ce rapport - même si cette approche est très simplificatrice et comme on va le voir la démarche des organismes de standardisation ne suit pas cette séparation - de séparer les approches selon le domaine considéré (Audio, ou Vidéo/Multimédia), ce qui permet par la même occasion de définir clairement le format MP3.

C.4.3.- Le domaine Audio

Au 27/3/2001, selon http://www.searchterms.com, le terme « MP3 » est le huitième mot le plus recherché sur Internet (il était en première position au début de 1999). En réalité, ce terme désigne « MPEG 1 Layer 3 », autrement dit [23] et [24]. Celui-ci a été défini en 1991 ([23], [24]), et permet des compressions pour des fréquences de 32 kHz, 44,1 kHz et 48 kHz, pour un taux standard de 32 kbit/s, et utilise la DCT déjà vue dans le cadre de JPEG (les différentes couches 1 à 3 correspondent à des degrés de sophistication et de performance croissants). La recherche dans le domaine ayant connu depuis 1991 d'importants progrès, le successeur MPEG 2 Advanced Audio Coding (AAC, voir [29] et [59]) a été mis au point. Il permet de traiter des fréquences de taille deux fois plus petites, à des taux de allant de 8 kbit/s à 320 kbit/s, en utilisant une variante de DCT (MDCT: Modified Discrete Cosine Transform). MPEG-4 Audio concerne, lui, davantage les fonctionnalités (à ce niveau, l'apport de ce standard est très important) que la compression, pour laquelle est fait de nouveau usage de la technologie AAC. D'autres algorithmes de compression, propriétaires, ont été mis au point et inclus dans certains produits, parmi lesquels Liquid Audio, Windows Media Audio, RealAudio, le format BlueMatter de Universal, ou encore le format MP3Pro, annoncé par Thomson Multimédia pour mi-2001, certains affirmant permettre des performances meilleures

que leurs pendants MPEG. Le projet Vorbis, émanant de la communauté du logiciel libre, porte sur le format .ogg, alternatif au format MP3.

C.4.4.- Le domaine Vidéo/Multimédia/Metadata

Les premiers standards MPEG-1 et MPEG-2 disposent également de parties (Part 2, [20], [21], [22], [28]) dévolues à la vidéo. Comme précédemment, d'autres formats de compression propriétaires (comme ceux développés dans QuickTime, AVI, ou RealVideo) ont été mis au point. L'approche de MPEG-4, qui est davantage orienté objet que ses prédécesseurs, permet des passerelles entre ces différents formats. Il s'adapte en outre aussi bien aux appareils à faible débit (et permet ainsi de récupérer de la vidéo sur GSM), qu'aux appareils à haute définition.

L'objet de MPEG-7 est de standardiser la description des contenus. Ce standard permet, ente autres, d'avoir des informations sur les données, par exemple de savoir qui a créé le bitstream, à quelle heure, etc. Les domaines d'application concernent, entre autres, la recherche, le filtrage, etc.

La sécurité au sens large des données audio et vidéo est devenue un aspect important au sein de la communauté MPEG à partir de MPEG-4. Dans la partie suivante, nous précisons les concepts sous-jacents à la sécurité des systèmes d'information.

C.5.- Les techniques de sécurité et les standards correspondants

La protection des données numériques, que ce soit de la musique, de la vidéo, etc., utilise de manière essentielle les méthodes cryptographiques ou de tatouage d'information. Ces protections procurent des éléments de réponse à plusieurs impératifs (voir [113] pour les aspects ayant trait à Echelon). Nous décrivons ci-dessous ces deux approches, qui ne sont d'ailleurs pas exclusives l'une de l'autre, en précisant le degré de standardisation et les limites de sécurité technologiques connues, ainsi que les méthodes existantes de protection contre les copies illicites.

C.5.1.- Cryptographie

L'objet de la cryptographie est l'étude des techniques ayant pour but d'assurer la confidentialité, l'intégrité et l'authenticité des informations ou de leur origine. Elle se caractérise, schématiquement, par deux approches principales, qui, pour nombre d'applications, ne s'excluent pas mutuellement, mais peuvent souvent être combinées harmonieusement entre elles : cryptographie à clef secrète et cryptographie à clef publique (voir [112] et [109] pour un rapport succinct sur les standards AES et IEEE P1363).

C.5.1.1.- *Cryptographie à clef secrète*

La cryptographie à clef secrète de nouveau se subdivise en deux écoles : celle dite des « stream ciphers » et celle des « blocks ciphers ». Concernant les « stream ciphers », nous dirons seulement ici qu'ils codent un message bit à bit. Les "blocks ciphers" traitent

l'information par blocs. Ils utilisent la même clef pour chiffrer un bloc que pour le déchiffrer. Le plus célèbre de ces algorithmes est le DES (Data Encryption Standard, [5]), estampillé FIPS (Federal Information Processing Standard) 46-2 du NIST (National Institute of Standard and Technology) en 1977. Dans cette partie, nous le décrivons de manière succinte.

La longueur de la clef secrète du DES est de 56 bits (64 avec le padding), et traite des blocs de 64 bits. En pratique, DES fonctionne de la manière suivante : le chiffrement se fait sur 16 tours ; à partir de la clef K de 56 bits, on construit 16 clefs $(K_i)_{1=i=16}$ de 48 bits (une par tour). Pour chaque tour, on construit des S-boxes $S=(S_1, \ldots, S_8)$. Les S_j sont des applications de substitution qui prennent 6 bits en entrée et renvoient 4 bits en sortie. Le bloc initial de 64 bits est divisé en deux moitiés de 32 bits : L_0 (L=left=gauche) et R_0 (R=right=droite). Chaque tour suit le même schéma : il prend en entrée 32 bits : L_{i-1} et R_{i-1} du tour précédent et produit de nouveau 32 bits L_i et R_i de la manière suivante :

$$L_i = R_{i-1}, \qquad R_i = L_{i-1} \oplus f(R_{i-1}, K_i),$$

où $\oplus$ désigne XOR (l'exclusive-OR, qui obéit aux règles suivantes : $0 \oplus 1 = 1 \oplus 0 = 1$ et $0 \oplus 0 = 1 \oplus 1 = 0$), et $f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$. Ici E est une fonction fixée qui étend R_{i-1} de 32 bits à 48 bits, et P une permutation fixée sur 32 bits. Une permutation initiale IP des bits précède le premier tour. Après le dernier tour, les moitiés gauche et droite sont échangées et le texte est permuté bit-à-bit par IP^{-1}. Le déchiffrement suit le même algorithme avec la même clef K, mais simplement les sous-clefs sont appliquées dans le sens inverse.

Il est apparu ces dernières années que le DES n'offrait plus une sécurité suivante ([80]), et le NIST a demandé à la communauté cryptographique mondiale de réfléchir et proposer de nouveaux algorithmes répondant à des critères publics, afin de définir l'AES (Advanced Encryption Standard, [1]). Le lauréat de ce concours est l'algorithme RIJNDAEL, une proposition belge due à Joan Daemen et Vincent Rijmen, désormais désigné également comme le FIPS 197. L'AES traite des blocs de taille 128 bits, avec des clefs de longueurs variables (128, 192, 256 bits). En fait, il est suffisamment souple pour traiter des blocs de taille 64 bits, et sera efficace sur des plate-formes variées (processeurs à 8 bits, réseaux ATM, communications de satellites, HDTV, B-ISDN, etc.).

Bien entendu, l'AES doit résister à toute une batterie d'attaques, allant de la cryptanalyse différentielle ou linéaire aux attaques par recherche exhaustive. C'est d'ailleurs ce type d'attaque par « brute-force » à laquelle a été confronté le DES ces dernières années ([80]), et qui a motivé la recherche d'un successeur.

L'un des problèmes de la cryptographie à clef secrète concerne la gestion des clefs. En effet, il est nécessaire d'avoir autant de clefs secrètes que de correspondants, ce qui devient très rapidement très complexe. Une réponse à ce problème est fournie par la cryptographie à clef publique.

C.5.1.2.- *Cryptographie à clef publique*

Dans cette approche, chaque correspondant possède non pas une, mais deux clefs. L'une est secrète (on la qualifie généralement de « privée »), l'autre est publique. Par exemple, si Alice et Bob (ces noms sont standards en cryptographie) souhaitent communiquer, Alice dispose d'une clef privée x_A et d'une clef publique y_A, mutatis mutandis pour Bob. Si Alice souhaite envoyer un message à Bob, elle cherche la clef publique y_B de Bob, chiffre son message avec cette elle, et envoie le message ainsi crypté à Bob. Les clefs publiques et privées sont reliées

par une certaine fonction, et seul Bob, avec sa clef secrète x_B est en mesure de déchiffrer le message d'Alice. La sécurité de ces protocoles repose sur des problèmes mathématiques.

Le projet P1363 ([7]), commencé en 1993 et achevé en août 2000, a, sous l'égide du comité de standardisation de l'IEEE (Institute of Electrical and Electronical Engineers), standardisé un certain nombre d'algorithmes, de schémas et de protocoles de cryptographie à clef publique.

La sécurité des algorithmes à clef publique décrits dans le standard IEEE-P1363 ([7]) repose sur les problèmes mathématiques suivants (voir [110]) :

- Factorisation de grands entiers : RSA (Rivest-Shamir-Adleman) et Rabin-Williams

- Problème du logarithme discret : DSA (Digital Signature Algorithm, [2], [6])), échange de clefs de Diffie-Hellman, chiffrement et signature électronique de El Gamal, de Schnorr et de Nyberg-Rueppel.

- Problème du logarithme discret pour les courbes elliptiques : les analogues des algorithmes ci-dessus pour les courbes elliptiques, considérées sur des corps finis de cardinalité un grand nombre premier ou une puissance première de deux (e.g. [4]).

Les cryptosystèmes à clef publique sont naturellement également sujet à des attaques, que l'on peut qualifier dans une certaine mesure. En effet, mis à part des choix malheureux des paramètres où les attaques sont polynomiales, les meilleurs algorithmes classiques connus (la cryptanalyse classique est entendue ici par opposition à la cryptanalyse quantique, voir [111]) de résolution du problème de la factorisation ou du logarithme discret dans le groupe multiplicatif d'un corps fini sont sous-exponentiels. En revanche, à ce jour, aucun algorithme sous-exponentiel (avec les précautions mentionnées sur le choix des paramètres, où il faut éviter les courbes elliptiques super singulières, les courbes elliptiques anormales, ou celles sujettes à une descente de Weil efficace) n'a été mis au point pour résoudre le problème du logarithme discret formulé dans le groupe des points rationnels d'une courbe elliptique sur un corps fini. En pratique, cela signifie concrètement qu'il est très souhaitable d'utiliser RSA ou DLP avec des modules de taille 1024 bits et plus, et d'utiliser ECDLP avec des modules de taille 163 bits et plus (la sécurité de ECDLP avec 163 bits équivaut à celle offerte par RSA ou DLP avec 1024 bits).

C.5.1.3.- *Signatures électroniques*

Les signatures électroniques (ou digitales) sont utilisées pour prouver l'authenticité et l'intégrité des données. A la différence d'une signature manuelle, elles dépendent du document à signer (pour des détails techniques, voir la partie C).

En pratique, pour des raisons de rapidité, on ne signe pas (au sens strict du mot) un fichier, mais le résultat donné par l'application d'une fonction de hachage à ce fichier. Une fonction de hachage est une fonction qui prend en entrée (input) un fichier de n'importe quelle taille et génère une sortie (output) de taille fixée. Pour les besoins de la cause, nous prenons l'exemple de la fonction (européenne) RIPEMD-160, pour laquelle la taille en sortie est de 160 bits. Une bonne fonction de hachage doit satisfaire à diverses propriétés (impossibilité technique de

fabriquer une pré-image ou encore one-way function, résistance aux collisions, etc.). En l'état actuel des connaissances, c'est le cas de RIPEMD-160.

Les différentes étapes typiques de constitution de la signature électronique d'un document peuvent être décrites comme suit (il y a d'autres choix possibles) :

- Une paire unique de clefs cryptographiques (pour la technologie à clef publique) est fournie à Alice (ou générée par elle).

- Avec RIPEMD-160, Alice hache son message *M* et récupère un output *MD* (comme Message Digest).

- Alice signe *MD* avec sa clef secrète, via un algorithme de signature électronique. La signature électronique *S* consiste en le résultat de cette opération.

- Alice ajoute *S* au message *M* et envoie le tout électroniquement à Bob.

De son côté, Bob reçoit le message *M* + *S* de Alice. Il veut vérifier l'authenticité de l'origine de ce message.

- Bob sépare *M* de *S*. Il applique de nouveau RIPEMD-160 à *M* et récupère un output *MD*.

- Bob utilise la clef publique d'Alice pour vérifier que *S* est bien la signature électronique de *MD* émanant de Alice. S'il n'y a aucune altération (tous les bits sont égaux), alors il sait que les données n'ont pas été altérées après la signature.

- Bob reçoit un certificat d'une autorité de certification (ou de Alice elle-même). Ce certificat confirme la signature digitale sur les données de Alice. Le certificat contient la clef publique, le nom (ou pseudonyme) d'Alice (éventuellement d'autres informations), et le tout est signé numériquement par l'autorité de certification.

En pratique, on utilise rarement la cryptographie à clef publique toute seule, mais plutôt en la combinant avec la cryptographie à clef secrète. En effet, les protocoles à clef publique, s'ils permettent des échanges sécurisés sur des canaux qui ne le sont pas, sont en règle générale 1.000 fois plus lents pour le chiffrement/déchiffrement que les protocoles à clef secrète. La solution consiste à initier une communication sécurisée à l'aide d'un protocole à clef publique, transférer une information disons de 128 bits, ce qui est parfaitement raisonnable sur le plan du temps de calcul, et d'utiliser ensuite cette information commune aux deux correspondants comme clef secrète d'un protocole à clef secrète. Le protocole à clef publique cède alors la place au protocole à clef secrète, et la communication se poursuit à l'aide de celui-ci. C'est par exemple ce que fait le produit PGP de Phil Zimmerman, qui combine un algorithme à clef publique, en l'occurrence RSA, avec un protocole à clef secrète nommé IDEA, et plus généralement dans les architectures PKI (Public-Key Infrastructure) avec autorités de certification (CA, voir par exemple [3], [8]), qui impliquent en particulier les technologies de signature électronique.

C.5.1.4.- *Autorités de certification*

La tâche centrale du CA est d'authentifier le possédant et les caractéristiques d'une clef publique de sorte à ce qu'elles soient considérées comme de confiance. Une fois que le CA est persuadé que ces critères sont satisfaits, un certificat est généré contenant cette clef et d'autres détails. Ce certificat est lui-même signé numériquement par le CA (et donc avec la clef secrète du CA) pour établir la corrélation avec le possesseur de la clef. Si le CA publie sa clef publique, alors une vérification automatique est possible par tout récipiendaire. Cependant, il est nécessaire que le récipiendaire du certificat fasse confiance au CA. Toutes les parties doivent donc faire confiance au CA. Il résulte de cela que plusieurs catégories de certificats peuvent être conçus. Par exemple la clef publique d'un CA peut être signée numériquement par un autre CA, et donner naissance ainsi à une hiérarchie de CA. Une clef publique peut aussi être certifiée par plusieurs CA.

Un exemple de certificat est donné ci-dessous:

- Nom ou pseudonyme du signataire.
- Nom du CA.
- Clef publique du signataire.
- Algorithme, type de clef.
- Profession, position dans une organisation, qualifications, documents officiels relatifs au signataire.
- Limites juridiques.
- Confirmation de la révélation des vrais interlocuteurs (en cas de pseudonymes) en cas de conflit.
- Date d'expiration du certificat.

Il est particulièrement notable que ces standards AES ou IEEE-P1363 aient fait l'objet d'un débat scientifique ouvert et international. Il est donc très invraisemblable qu'il y ait au sein même de ces algorithmes des « trap-doors ». De plus, l'évaluation des propositions a été faite sur de longues années, dans le souci de pérennité des nouveaux standards.

L'une des applications possibles de ces architectures de signature et de certification électronique pourrait être la gestion électronique des droits, puisque l'authentification du contenu et de l'utilisateur qui y accède pourrait se réaliser par le biais de signatures utilisant les technologies à clé publique. C'est pourquoi nous proposons que l'on étudie les perspectives que cela pourrait offrir dans les prochaines années.

C.5.2.- Tatouage de données/Watermarking

Le double objet de la sténographie concerne, d'une part, la faculté de « cacher » de l'information dans de l'information et ainsi de communiquer de manière confidentielle (information hiding), d'autre part, le tatouage des informations numériques (watermarking). Nous ne nous étendons pas ici davantage sur le premier aspect (voir [49], [78], [108], [120]). Le second aspect est devenu crucial dans le domaine de la protection des droits et des contenus, de l'authentification et de la vérification d'intégrité, le traçage de documents (éventuellement de Meta-informations, metadatas), de contrôle, etc. (voir [63], [88], [100], [101], [133], [131], [126], [91]), et se décline sur des modes variés selon les applications

visées (on pourra se réfèrer notamment, pour avoir une vision d'ensemble des tendances de cette technologie, au forum d'échange animé conjointement par des représentants des mondes industriels et académiques : *http://www.watermarkingword.org*).

C.5.2.1.- *Fonctionnalités et mesures de la sécurité*

Les grandes classes de watermarks (ce terme technique s'est imposé pour désigner ce qui suit) sont :

- Perceptible par l'humain
- Non-perceptible par l'humain : cela signifie invisible, si l'objet d'application est visuel (e.g. une photo, une vidéo), ou inaudible, s'ils s'agit d'un objet audio (e.g. musique).

    - Fragile : le watermark peut être altéré/enlevé par des modifications simples du support (photo, vidéo, musique, etc.)

    - Robuste : le watermark résiste aux manipulations importantes que subit le support. Cet aspect est particulièrement important lorsque des techniques de compression, qui sont considérées comme des modifications importantes de l'original, sont mises en oeuvre.

        - Privé : la détection du watermark nécessite le support original (e.g. la photo originale)

        - Public : la détection du watermark ne nécessite pas le support original.

Un aspect crucial, lors de la mise en oeuvre d'un système de watermark robuste, est que le coût (financier, technologique, etc.) pour contrecarrer les mesures de protection (par exemple, enlever le watermark, ou le rendre inutilisable, etc.) doit être supérieur à celui payé pour utiliser le produit de la manière dont on l'a conçu. En d'autres termes, si pour contourner une mesure de protection (que cela soit dans le contexte des techniques de watermarking, ou de la sécurité des données plus généralement), il est nécessaire de détruire la valeur économique ou commerciale de l'objet visé, alors la mesure de protection est parfaitement adaptée aux besoins. Dans un cadre différent mais similaire, et illustrant bien la problématique, s'il est nécessaire d'investir 2 M Euros pour casser une clef de session d'un cryptosystème et détourner des fonds se montant à strictement moins que cette valeur, il sera légitime d'estimer que la protection est relativement dissuasive.

Les applications concernant la propriété intellectuelle, telles celles développées à travers le projet européen MENHIR, se sont concentrées sur le concept de « licence plate » (standards IS 10918-3 et IS 10918-4), qui permettent d'attacher un label aux images, contenant des informations comme la provenance de l'image, les ayant-droits, etc. Au stade présent du développement de JPEG 2000, il n'est pas prévu de standardiser une technique de Watermarking, mais plutôt d'envisager certaines interfaces destinées à la protection des contenus.

Dans la plupart des applications, les outils de watermarking doivent être robustes, et garantir, dans une certaine mesure à évaluer, que l'information ajoutée (à l'image, la vidéo, aux sons, etc.) ne peut être enlevée, soit par des modifications accidentelles du support original (e.g. l'image originale), soit par des attaques ad-hoc. Il existe toutefois des exceptions, où l'on

demande au watermark au contraire d'être fragile, c'est-à-dire de ne pas résister aux modifications des données, même mineures.

Les modifications peuvent se faire au niveau du traitement du signal, comme par exemple, celles qui visent à changer (dans le domaine image et vidéo) les contrastes, les filtres linéaires et non-linéaires, les compressions (JPEG/MPEG). Des modifications géométriques peuvent également être appliquées aux images/vidéos, comme le changement d'échelle, ce qui a pour conséquence que les algorithmes qui ajoutent le watermark à des endroits fixes tombent sous le coup de cette attaque. Il est également possible d'ôter des parties de l'informations originale (e.g. on coupe une partie de l'image), de translater les images ou vidéos, de faire opérer des rotations, de retourner les images. Ces diverses attaques sont d'autant plus importantes qu'elles ne modifient pas sensiblement la qualité de l'information récupérée à son issue. De plus, les watermarks pré-existant dans des données ne doivent pas être modifiées par l'arrivée d'un nouveau watermark (ou alors de manière compatible, par exemple, en conservant les données relatives aux divers marquages, comme les données relatives au nouvel arrivant, l'heure des modifications, etc.).

En ce qui concerne l'évaluation des différentes technologies de watermarking proposées, différentes approches co-existent.

Dans le domaine de l'image, l'un de ces instruments est constitué par StirMark ([121], [122], [123]), qui implémente toute une batterie d'attaques, principalement sur les photos (des adaptations sont toutefois possibles dans le domaine vidéo, voir [123], bien qu'un design spécifiquement dédié aux attaques de watermarks pour la vidéo n'ait – pour l'instant - pas vu le jour).

Dans le domaine audio, l'initiative d'évaluation la plus célèbre est due au SDMI (Secure Digital Music Initiative [48], voir également [83] pour une proposition d'évaluation des performances des algorithmes de watermarking dans le domaine audio). Le SDMI a en effet proposé un challenge sur Internet de six techniques de protection des données audio (en fait musicales). Sur les six, quatre étaient directement des techniques watermarking, et deux n'étaient pas directement des techniques watermarking. Une récompense de 10000 $ était à partager entre les lauréats, sous la condition toutefois de non-divulgation des méthodes d'attaques. Enfin, les méthodes de protection utilisées n'étaient pas révélées, et les assaillants avaient trois semaines pour tenter leur chance.

Ce challenge a entraîné des réactions très diverses, et très fortes, notamment de l'Electronic Frontier Foundation, qui a même appelé au boycott pur et simple du challenge. Par ailleurs, un groupe de chercheurs des universités de Princeton, de Rice, et du centre de recherche de Xerox de Palo Alto aux Etats-Unis ([75]) ont déclaré avoir contourné les méthodes de protection proposées au challenge, sans altérer de manière notable pour le commun des mortels l'intégrité auditive et donc la valeur commerciale des morceaux de musique. La critique la plus importante à l'égard du challenge proposé par le SDMI concerne le fait que, d'une part, les techniques de protection n'ont pas été divulguées, et que d'autre part, le temps imparti pour attaquer les propositions était très court.

Dans la partie suivante, nous proposons une esquisse de classification des algorithmes de watermarking selon les finalités visées et les domaines de plongement de ces watermarking (compressé ou non).

C.5.2.2.- *Classification des algorithmes de Watermarking pour les images*

Concernant les algorithmes de watermarking pour les images, plusieurs approches co-existent, que l'on peut classifier schématiquement en trois catégories : les techniques relevant du domaine dit spatial, du domaine transformé, et les techniques hybrides.

Dans le domaine dit spatial, les valeurs de certains pixels des images sont modifiées, par exemple en ajoutant un signal dans le domaine bleu de l'image. Cela peut se faire sur la base de suites pseudo-aléatoires, dont l'initialisation (seed) dépend d'une clef secrète, que les entités autorisées utilisent également pour détecter le watermark. Par ailleurs, il est également possible de modifier des valeurs de pixels choisis eux-même de façon aléatoire. Afin de garantir la robustesse, ces modifications sont répétées. Les modifications peuvent également s'opérer sur des blocs de l'image, sélectionnés de manière aléatoire. Les blocs peuvent eux-même être davantage adaptés à tel type de modification, et être traités en conséquence. Dans ces approches, il est très utile de tirer parti du système visuel humain.

Dans le domaine transformé, les techniques utilisées traitent mathématiquement, en règle générale, l'image avant d'y inclure un watermark. En pratique, on modifie des coefficients des transformées utilisées (DCT, DFT, DWT), ce qui permet de répartir les modifications sur l'ensemble de l'image. Dans certains cas, ces techniques s'avèrent plus résistantes que les précédentes à des attaques comme les rotations par exemple (voir plus bas les questions de robustesse). Le désavantage est le coût algorithmique et la difficulté à adapter le signal watermark au contenu local de l'image.

Les techniques hybrides tentent de combiner les deux approches précédentes, et se subdivisent de nouveau en deux catégories, l'une orientée JPEG et ses variantes, notamment à base de DCT, l'autre orientée JPEG-2000 et les techniques à base d'ondelettes (DWT). Il s'agit ici de proposer des algorithmes compatibles avec les méthodes de compression en vigueur, et donc, si la robustesse est une des propriétés souhaitées (par exemple si l'on souhaite mettre l'image protégée sur Internet), résistants à des phases de compression/décompression successives. En pratique, l'image est en règle générale partitionnée en blocs, qui sont alors traités via DCT ou DWT. Certains des coefficients de ces transformations sont alors modifiés. L'avantage est que, ainsi, il est tiré un meilleur parti de l'environnement local de l'image. En revanche, il est essentiel de prêter beaucoup d'attention aux attaques de type translation, et changement d'échelle.

C.5.2.3.- *Classification des algorithmes de Watermarking pour les vidéos*

La plupart des considérations et solutions apportées dans le contexte des images se transposent dans celui des vidéos, par exemple, simplement en traitant chaque image de la vidéo comme une image fixe. Cependant l'environnement de ce média présente des caractéristiques différentes, et plus complexes, que celles des images fixes, et le watermarking de vidéos doit satisfaire souvent des contraintes très spécifiques. Deux approches sont à distinguer.

Dans la première, la vidéo n'est pas compressée. Par exemple, dans l'approche développée dans [89] (voir [132] pour d'autres approches, notamment basées sur les transformées en ondelettes, mais qui nécessitent, à la différence de celle présentée ci-dessous, la connaissance

de la vidéo originale), une suite d'informations, représentant le watermark, est répétée un certain nombre de fois (ce nombre est noté cr, et désigne le chip rate) pour obtenir une suite numérique étendue, qui est amplifiée, et modulée à l'aide d'une suite binaire de longueur cr de pseudo-bruit. Ce signal est alors ajouté à celui de la vidéo, pour former la vidéo tatouée. La détection se fait en corrélant le signal reçu et la suite binaire de pseudo-bruit.

La seconde approche privilégie une action directement au niveau du domaine compressé, en ajoutant l'information (le watermark) dans le flux binaire représentant la vidéo compressée, ce qui toutefois peut imposer des temps de calcul plus importants que l'approche précédente (voir [89], [90], ou [106] pour des travaux plus récents, qui s'appuient sur le concept DEW ou Differential Energy Watermarks, qui s'applique également dans le contexte des images fixes d'ailleurs). Ainsi, il est possible (voir [89]) d'appliquer la technique décrite plus haut au domaine compressé. Pour cela, une transformation par blocs, DCT par exemple dans le contexte JPEG, suivie d'un balayage en zig-zag, est appliqué à la suite watermarkée étendue. A son issue, chaque coefficient DCT ainsi créé est ajouté à ceux de la vidéo (en prêtant attention aux taux de traitement autorisés). Le décodage se fait également dans le domaine compressé.

C.5.2.4.- *Classification des algorithmes de Watermarking dans le domaine audio*

Dans le domaine audio, plusieurs propositions ont été faites, et la problématique est assez semblable à ce qui précède, dans le sens où l'on peut soit privilégier une action dans le domaine non-compressé, ou au contraire, dans le domaine compressé. Certaines méthodes utilisent le domaine des fréquences (voir par exemple [57], [71]). D'autres sont assez similaires à celles que l'on rencontre dans le domaine des images ([51]).

C.5.3.- Codes régionaux et méthodes intégrées de protection contre les copies pour les CD/DVD

C.5.3.1.- *Les codes régionaux des DVD Vidéo*

Afin de contrôler la sortie des films (non simultanée en général, par exemple, un film peut sortir en DVD aux Etats-Unis au moment où il fait seulement son entrée dans les salles en Europe), des productions des studios dans les différentes régions du globe, et de gérer les droits de distribution inhérents, les DVD Vidéo intègrent une protection qui a pour but de prévenir l'usage d'un DVD hors de sa zone. Chaque lecteur se voit attribuer un code régional correspondant à la zone géographique à laquelle il est destiné, le but étant qu'un lecteur acheté dans une région, et identifié comme tel via son code, ne peut lire un DVD acheté dans une autre région.

Toutefois, il existe des DVD, dits toutes zones, qui sont lisible par tous les lecteurs. Les DVD peuvent également être lisibles dans certaines régions et pas dans d'autres. La méthode utilisée n'est pas du cryptage, mais simplement un octet sur le DVD que le lecteur examine avant de lire ou pas le DVD, selon que les informations stockées sur cet octet sont compatibles ou pas avec le lecteur.

Il y a six régions (ou zones) réparties comme suit (voir [68]) :

(1) Canada, Etats-Unis et territoires rattachés
(2) Japon, Europe, Afrique du Sud, Moyen Orient (y compris l'Egypte)
(3) Asie du Sud-Est, Est de l'Asie (y compris Hong-Kong)
(4) Australie, Caraïbes, Nouvelle Zélande, Iles du Pacifique, Amérique Centrale, Amérique du Sud
(5) Ancienne Union Soviétique, Inde, Afrique, Corée du Nord, Mongolie
(6) Chine

Ces codes régionaux s'appliquent également aux lecteurs de DVD-ROM dans le cas d'utilisation d'un DVD Vidéo (mais pas pour les DVD-ROM contenant des logiciels).

Ceci étant, certains lecteurs peuvent être modifiés pour lire tous les DVD, quelles que soient leurs zones d'appartenance. Cette fonctionnalité est d'ailleurs permise par les lecteurs de DVD-ROM RPC 2, qui autorisent un nombre limité de fois (entre 5 et 9) la modification du code régional.

C.5.3.2.- *Méthodes intégrées dans le DVD de protection contre la copie*

Il existe principalement trois méthodes de protection intégrées.

La première, appelée APS (Analog Protection System), est développée par Macrovision, et est intégrée dans chaque lecteur, pour empêcher la copie analogique sur VHS. Les cartes vidéo informatiques utilisent également ce système. Les DVD informent le lecteur d'activer la protection AGC (Automatic Gain Control) avec ou sans perturbation. Les copies illicites auront ainsi une qualité très amoindrie, et ne seront pas exploitable dans des conditions favorables.

La seconde, appelée CGMS (Copy Guard Management System), est un système de gestion de niveau de génération de copies. L'information CGMS est intégrée dans le signal vidéo sortant du lecteur, et l'appareil faisant la copie doit respecter ce signal. Le standard numérique sera présent sur les connections numériques comme IEEE 1394/Firewire (voir [46]). L'équivalent Audio est appelé SCMS (Serial Copy Management System). L'objet est d'éviter les copies de copies, à l'aide d'indicateurs (flags), et d'éviter la copie en série du support (CD ou DVD) maître (voir *www.eacem.be* pour diverses illustrations, et [115] pour une description technique). Deux approches techniques existent pour permettre cette fonctionnalité :

- L'appareil enregistreur ajoute un second watermark (concept dit de remarking).

- L'enlèvement dans le contenu d'une pièce volatile d'information pendant l'enregistrement (concept dit du ticket).

L'un des problèmes avec le premier concept est que l'appareil du consommateur doit être techniquement en mesure de rajouter un watermark, ce qui signifie que le contenu doit être accessible à cette fin. Un second problème est que les pirates peuvent comparer les données avant et après le rajout du watermark, et ainsi le trouver. Le concept du ticket permet d'éviter ces écueils. Le ticket peut être plongé dans le contenu, ou transmis sur un signal à part. Si l'appareil du consommateur ne parvient pas à traiter ce ticket, il en découle une perte des droits sur le contenu. Pour assurer que le ticket est spécifique à un morceau de musique, ou

pour une fonctionnalité particulière (copie de tout par exemple), le ticket est lié de manière cryptographique avec le watermark du contenu.

Le concept de ticket peut s'expliquer sur l'exemple suivant : en pratique, on sélectionne une fonction cryptographique de type one-way, F, et on l'applique n fois au ticket. Il suffit alors de comparer la valeur du watermark W et $F^n(T)$, où T désigne le ticket. Si, par exemple, $W = F^2(T)$, alors l'appareil est autorisé à enregistrer le contenu, et le nouveau ticket $T' = F(T)$.

La troisième, appelée CSS (Content Scrambling System), est destinée à crypter les données stockées sur le DVD, de manière à interdire la lecture directe de ces informations. Les lecteurs et les décodeurs échangent des clefs d'encryptage de manière à décrypter la vidéo juste avant l'affichage. Cette protection a fait l'objet de diverses attaques technologiques (et donné naissance à divers procès), notamment DeCSS et les sept lignes rédigées en langage PERL par K. Winstein et M. Horowitz, deux chercheurs du MIT.

Dans le domaine audio, que nous plaçons également dans cette partie, un certain nombre de produits et méthodes existent pour empêcher la copie de CD. L'exemple le plus important et significatif est peut-être celui de la technologie Key2Audio placée par Sony et Universal sur leurs CD, et destinée à empêcher que ceux-ci soient copiés (gravés) sur d'autres supports (autres CD, disque dur, …). En fait, il s'est avéré qu'il était possible de contourner cette technologie en passant simplement un stylo-feutre autour du CD pour rendre cette protection inopérante.

Face aux limites de ces modes de protection et aux récentes attaques qu'ils ont subi, une partie significative de l'industrie de l'électronique grand public paraît vouloir évoluer rapidement en direction d'une protection par watermarking. C'est ainsi que Digimarc, Hitachi, Macrovision, NEC, Philips Electronics, Pioneer et Sony ont annoncé en avril 2001 la formation d'un nouveau forum commun dénommé « Video Watermarking Group ».

PARTIE D : CONCLUSIONS ET RECOMMANDATIONS

D.1.- Conclusions

Notre analyse de l'état des technologies disponibles et de leur utilisation (détaillée dans les parties A à C du présent rapport) nous conduit à la triple conclusion suivante : il existe aujourd'hui une offre technique en matière de sécurité des œuvres numériques (D.1.1.) mais ses faiblesses expliquent sans doute un taux d'utilisation encore marginal (D.1.2.) qui les rend incapables de produire déjà un effet significatif sur le volume de la contrefaçon numérique (D.1.3.).

1.

2. D.1.1. Sur l'offre technique en matière de sécurité des œuvres numériques

Les technologies essentielles pour construire et exploiter des systèmes de protection des œuvres numériques et de gestion électronique des droits (DRM) sont aujourd'hui disponibles. Elles empruntent pour une large partie aux techniques cryptographiques ainsi qu'à la stéganographie et aux différentes méthodes déjà utilisées en matière de sécurité des systèmes.

Mais ces technologies sont affectées par deux faiblesses qui en freinent apparemment la diffusion et l'utilisation.

Elles sont tout d'abord **assez peu normalisées et encore largement dépendantes de standards propriétaires**. Les efforts de normalisation engagés dans le secteur paraissent assez timides et ne devraient pas suffire à convaincre rapidement les principaux industriels du secteur à trouver un consensus. On note par exemple que la nouvelle norme MPEG4 (ISO/IEC 14496 adopté en 1999) se contente de proposer un mode de description des droits intellectuels (IPMP) et des techniques de sécurité sans pour autant normaliser ces techniques elles-mêmes. De même, le Comité européen de normalisation (CEN) n'a réussi à élaborer qu'un cadre général et très descriptif concernant les architectures de DRM et non une véritable norme européenne en la matière (cf. la version provisoire de son rapport, CEN/ISSS, février 2003). On notera toutefois l'intéressante initiative dénommée "OpenDRM" qui cherche à promouvoir un cadre de référence en la matière qui soit compatible avec les pratiques et la logique du logiciel OpenSource.

La seconde faiblesse actuelle tient au fait que **ces technologies n'ont pas encore fait la preuve de leur fiabilité**. L'échec très médiatisé du projet SDMI en 2001 dans le domaine de la musique numérique a marqué les esprits sur ce point. Bien que certaines des technologies de base utilisées paraissent isolément fiables (notamment, celles relatives à la signature numérique ou au chiffrement), d'autres demeurent encore perfectibles (en matière de

watermarking, notamment) et – surtout – il s'avère que les fragilités apparaissent essentiellement au niveau de leur implémentation et de leur combinaison dans des logiciels complexes qui sont censés assurer les différentes fonctions d'un système de DRM.

Or, tant pour les producteurs et diffuseurs que pour les usagers, la sécurité des technologies mises en œuvre constitue une exigence légitime.

Les premiers souhaitent que les investissements techniques et commerciaux à réaliser autour des DRM puissent être rentabilisés sur une période suffisamment longue et ont donc besoin que ces technologies s'avèrent efficaces et dissuasives vis-à-vis des différentes formes de contrefaçon numérique.

Les usagers-consommateurs de leur côté ont un double souci : d'une part, être assurés que leurs données personnelles (identité, coordonnées bancaires, goûts, nature des produits consommés, …) seront bien préservées et, d'autre part, que l'évolution technologie et celles des menaces ne les obligeront pas à devoir changer trop souvent leurs logiciels ou leurs équipements. Des deux côtés, l'incertitude qui demeure quant à la sécurité des technologies actuellement proposées freine leur développement et leur emploi à grande échelle.

3. D.1.2. Sur l'utilisation de ces techniques sur le marché

Ainsi que nous l'avons relevé dans le rapport, les rares données disponibles indiquent toutes que **les technologies de sécurité sont encore très peu utilisées sur le marché pour protéger les œuvres numériques**. Et les seules qui le soient actuellement sur une certaine échelle (dans le domaine du "verrouillage" des CD-Audio) engendrent des critiques et des difficultés pratiques, tout en restant souvent des technologies de premier niveau.

Le cas de l'industrie phonographique va donc devoir être suivi avec attention. Il semble, en effet, que cette industrie soit la seule qui – malgré l'échec du projet SDMI – ait officiellement exprimé sa volonté stratégique d'investir dans les moyens techniques de sécurité et d'en assumer les conséquences vis-à-vis de ses consommateurs. Si cette orientation se confirmait, la relative concentration de ce secteur d'activité (qui est largement dominé par cinq grandes firmes internationales) pourrait permettre qu'une standardisation de fait s'instaure rapidement en matière de protection des CD-audio ainsi que des téléchargements musicaux en ligne. Et une telle évolution aurait une forte influence sur la possibilité de déployer dans les autres segments du marché numérique des solutions de DRM compatibles avec celles qui seraient retenues dans le domaine musical.

L'autre élément que nous avons relevé concerne **l'implication significative de plusieurs acteurs majeurs des technologies de l'information dans les technologies DRM**. Les investissements et les annonces techniques et commerciales de Microsoft, d'IBM ou de Sony pourraient ainsi jouer un rôle important dans le futur de ces technologies, notamment en permettant à ces grands acteurs de trouver entre eux des consensus techniques qu'ils seraient en mesure d'imposer rapidement au reste du marché. Il faudra donc également suivre cet aspect de la situation pour éviter que des ententes techniques non transparentes viennent remplacer une normalisation internationale encore balbutiante.

4. D.1.3. Sur leur impact en ce qui concerne la prévention des contrefaçons numériques

Dans ce contexte, il est logique que l'on ne puisse constater **aucun impact mesurable à ce jour de l'utilisation de ces techniques sur la contrefaçon numérique**. Cette lacune ne résulte pas seulement d'une absence de données et statistiques. Elle provient surtout du manque de déploiement significatif de ces outils de sécurité sur la plupart des segments de marché du commerce électronique des produits numériques.

Cet absence d'impact mesurable ne signifie pas pour autant que l'annonce du lancement des technologies ne puisse pas exercer à terme des effets dissuasifs sur une certaine partie des consommateurs et préparer les esprits au changement progressif du paysage numérique. On peut imaginer que la médiatisation entretenue autour de différentes formes de contrefaçon numérique (notamment celle affectant les fichiers musicaux via les réseaux P2P) et la perspective du déploiement de moyens de sécurité plus contraignants ait pour but de préparer les consommateurs à s'accommoder de services de diffusion en ligne payants et mieux sécurisés.

Mais il nous semble clair que **d'éventuels effets significatifs sur la prévention de la contrefaçon numérique ne pourraient résulter que du déploiement à grande échelle de systèmes de DRM normalisés et interopérables**. De ce point de vue, l'état actuel du marché et de l'offre technologie paraît très en-deçà de ce qui serait nécessaire. Tout au plus, peut-on imaginer que l'application dans les différents États-membres des dispositions issues de la directive du 22 mai 2001 en matière de mesures techniques et d'information sur les droits pourra jouer un rôle d'entraînement et de clarification des enjeux et des moyens.

Notre analyse de cet état des lieux technique et économique ainsi que du processus de transposition actuellement en cours nous conduit donc à formuler différentes recommandations pour les institutions et la politique communautaire en la matière.

D'une manière générale, il faudra attendre l'achèvement de la transposition de la directive du 22 mai 2001 dans les États-membres et la mise en œuvre des dispositions concernées pour pouvoir apprécier l'évolution de la situation en la matière.

D.2.- Recommandations

Les recommandations que nous pouvons formuler à l'issue de cette étude sont, pour partie, similaires à celles qui avaient été présentées dans notre précédent rapport sur le même thème en 2001 (F. Leprévost & B. Warusfel : Technologies de sécurité pour les médias digitaux, rapport pour STOA, EP/IV/A/STOA/2000/06/01, mai 2001).

Certaines recommandations de nature juridique tiennent compte, par ailleurs, des perspectives de transposition telles que nous les avons étudiées et des questions qu'elles soulèvent.

1. D.2.1. Recommandations de nature politique

Le principal acte politique communautaire en la matière ayant été l'adoption de la directive du 22 mai 2001 elle-même (et, en particulier, de ses articles 6 et 7), il nous semble que le principal objectif politique que les autorités communautaires pourraient se donner à moyen terme réside dans **une incitation à promouvoir la normalisation en matière de technologies de sécurité et de DRM**.

Nous reprenons donc le libellé de notre recommandation en ce sens dans notre rapport de 2001 :

- Promouvoir une politique de standardisation active des technologies de sécurité au niveau européen, tenant compte des propositions concrètes émises par les milieux industriels et académiques, ainsi que par les organisations représentant les utilisateurs de systèmes d'information

2. Mais compte tenu de l'évolution préoccupante de la contrefaçon en ligne et des réactions de l'opinion face à la protection des droits intellectuels dans le contexte numérique, nous estimons également que les autorités communautaires devraient prendre une initiative en deux temps :

- faire réaliser **une étude sociologique sur la perception** par le public et les différentes catégories de consommateur **des droits de propriété intellectuelle en matière d'œuvres numériques** (et sur leur élasticité éventuelle à des éléments commerciaux, tels que notamment le prix des produits numériques) ;

- sur la base de cette étude et des contributions de différents experts (sociologues, psychologues, juristes, scientifiques, …), susciter l'organisation de **campagnes d'information et/ou de sensibilisation aux enjeux économiques, sociaux et juridiques des droits intellectuels et de la contrefaçon dans le domaine numérique**.

3. D.2.2. Recommandations de nature technique

Malgré les évolutions techniques intervenues depuis deux ans, les recommandations techniques formulées dans notre rapport de 2001 demeurent pour l'essentiel valables :

- Faire le point sur les standards, ainsi que sur les modèles globaux proposés de gestion sécurisée sur Internet des contenus numériques.

- Distinguer entre les standards propriétaires pouvant mener à des situations de monopole et les standards issus d'un consensus entre représentants des mondes de l'industrie, académique, et gouvernementaux et favoriser les solutions permettant l'interopérabilité entre différents systèmes.

- Identifier les détenteurs de "brevets essentiels", évaluer leur volonté de négocier les licences d'exploitation.

- Proposer des études techniques de la sécurité des systèmes existants ou des systèmes en projet et distinguer entre les approches ouvertes et les approches fermées.

- Envisager la mise en place d'un "challenge" sur les protocoles susceptibles d'être normalisés.

- Assurer une veille sur les développement des techniques de sécurité multimédia.

- Évaluer la faisabilité de filtres à virus informatiques compatibles avec les formats des données traitées.

- Étudier les conditions de "convergence" technologique entre les systèmes de gestion électronique des droits (DRM) et les infrastructures à clé publique (PKI).

Par ailleurs, il nous apparaît que l'un des impératifs du marché pour accepter la mise en place et l'utilisation des DRM concerne la relative pérennité de ces outils, et leur simplicité d'utilisation. On devrait donc **encourager en priorité les architectures et les systèmes qui présenteraient un niveau suffisant d'évolutivité tout en permettant un grand confort d'utilisation aux usagers** (c'est-à-dire dont les composants techniques susceptibles d'être modifiés ou mis à jour – notamment pour faire face à des menaces ou pour corriger des failles – seraient conçus de manière modulaire et pourraient être mis à niveau sans bouleverser l'utilisation des logiciels déjà installés ou remettre en cause la protection des œuvres déjà exploitées).

4. D.2.3. Recommandations de nature juridique

Sur le terrain du droit, les enjeux essentiels à court terme sont liés à la mise en œuvre dans les États-membres des dispositions transposées de la directive du 22 mai 2001.

Au vu des transpositions actuellement réalisées ou en cours, il nous semble que trois questions nécessiteront sans doute une surveillance et un traitement particulier.

En premier lieu, il nous apparaît essentiel que **les décisions qui seront prises nationalement pour rendre compatibles certaines mesures techniques avec les exceptions reconnues au droit d'auteur, soient cohérentes entre elles**. Il serait en effet très difficile d'imaginer, tant pour les diffuseurs que pour les consommateurs, que certaines contraintes ou certaines facilités reconnues dans un État-membre ne le soit pas dans un autre. Étant donné que ces décisions seront prises suivant les cas par des médiateurs (le plus souvent) ou par une autorité ministérielle, voire par une juridiction, les risques d'écart pourraient s'avérer importants. Il devrait donc incomber aux autorités communautaires une double charge :

- d'une part, **effectuer un suivi permanent des décisions prises** ainsi dans le cadre de l'application de l'article 6.4 de la directive et **évaluer au cas par cas la cohérence de ces décisions les unes par rapport aux autres**,

- d'autre part, **favoriser la mise en relation des différentes entités nationales** en charge et organiser leur concertation permanente, **afin que se crée une "doctrine" commune**.

Une seconde préoccupation a trait à l'interaction négative que pourrait exercer l'application des dispositions issues de la directive en matière de protection des mesures techniques sur les possibilités de recherche en cryptographie et en sécurité de l'information.

La protection des intérêts européens en matière de technologie de sécurité (avec toutes ses conséquences économiques, sociales, politiques voire militaires) impose que l'expertise européenne en la matière ne soit pas bridée par la crainte d'actions contentieuses abusives. De même, la sécurité de la société de l'information et du commerce électronique nous obligera à tester en permanence la fiabilité de nos technologies.

Il convient donc – en l'absence de dispositions explicites dans la plupart des textes de transposition – que les autorités communautaires veillent à ce que **la protection des mesures techniques ne soit pas un frein à l'exercice légitime et nécessaire des activités de recherche en matière de cryptographie et de sécurité des systèmes**.

Par ailleurs, on peut penser que l'éventuel développement du recours aux mesures techniques devrait conduire à ce que les prélèvements financiers effectués au titre des "compensations équitables" (notamment sur le prix des supports numériques vierges) soient allégés progressivement. On ne peut en effet concevoir que cette compensation prévue pour balancer les effets négatifs des inévitables abus dans la copie privée perdure si des moyens efficaces restreignent ou suppriment les possibilités de se livrer à de tels abus.

Il serait donc utile et sans doute politiquement intéressant d'**étudier avec les parties concernées** (producteurs et diffuseurs, sociétés de gestion collective, ayant-droits, représentants des usagers et des internautes, …) **dans quelle mesure pourrait s'opérer à terme une substitution entre compensation équitable et mesures techniques**.

Enfin, il nous paraît toujours aussi nécessaire de **mener des études juridiques poussées sur les nouveaux modèles contractuels qui pourraient être induits par le commerce sécurisé des contenus numériques**, ainsi que nous l'avions déjà recommandé dans notre précédent rapport.

Bibliographie

[1] *AES. Advanced Encryption Standard*. http ://csrc.nist.gov/encryption/aes/index.html

[2] *ANSI X9.30:1-1997 : Public Key Cryptography for the Financial Service Industry : Part I : The Digital Signature Algorithm (DSA)* (revision of X9.30:1-1995)

[3] *ANSI X9.57-1997 : Public Key Cryptography for the Financial Service Industry : Part I : Certificate Management*

[4] *ANSI X9.62-1998 : Public Key Cryptography for the Financial Service Industry : Part I : The Elliptic Curve Digital Signature Algorithm (ECDSA)*

[5] *FIPS 46. Data Encryption Standard. Federal Information Processing Standards Publication 46*. U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1977. (revised as FIPS 46-1 : 1988, revised as FIPS 46-2 : 1993)

[6] *FIPS 186. Digital Signature Algorithm. Federal Information Processing Standards Publication 46*. U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1994

[7] IDC, *Digital Rights Management (DRM): A Definition* - IDC #23982 - March 2001.

[8] IDC, *The DRM Landscape: Technologies, Vendors, and Markets*, #24891, June 2001.

[9] *IEEE P1363/D13 (Draft Version 13). Standard Specifications for Public Key Cryptography*, Institute of Electrical and Electronics Engineers, Inc., http ://grouper.ieee.org/groups/1363/index.html

[10] *IETF-PKIX, Public-Key Infrastructure (X.509)* : http ://www.ietf.org/html.charters/pkix-charter.html

[11] IFPI, *Défendons la culture européenne : la position des producteurs de phonogrammes sur la Position Commune du Conseil sur la Directive Droit d'auteur et droits voisins dans la Société de l'Information*, 19 octobre 2000.

[12] IFPI, *SID Code Implementation Guide*, téléchargeable sur le site www.ifpi.org

[13] *IFPI issues labelling guidelines for copy control CDs*, May 30, 2002, téléchargeable sur le site http://www.ifpi.org

[14] *ISO/IEC/SC29/WG1 : JPEG 2000 Press Release* – Rochester. ISO/IEC/SC29/WG1 N1861 (18 August 2000)

[15] *ISO/IEC/SC29/WG1 : JPEG 2000 Part I Final Committee Draft Version 1.0.* ISO/IEC/SC29/WG1 N1646R (16 March 2000)

[16] *ISO/IEC/SC29/WG1* : http://www.jpeg.org

[17] *ISO/IEC 14496-2:1999 : Information technology - Coding of audio-visual objects. Part 2: Visual*, December 1999

[18] *ISO/IEC 14495-1:1999 : Information technology - Lossless and near-lossless compression of continuous-tone still images. Baseline*, December 1999

[19] W3C, *PNG (Portable Network Graphics) Specification*. Oct. 1996, http ://www.w3.org/TR/REC-png

[20] *ISO/IEC/SC29/WG11* : http ://www.cselt.it/mpeg/

[21] *ISO/IEC 11172-1:1993 : Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s. Part 1 : Systems*

[22] *ISO/IEC 11172-1:1993/Cor 1*, 1996

[23] *ISO/IEC 11172-1:1993/Cor 2*, 1999

[24] *ISO/IEC 11172-2:1993, Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s. Part 2 : Vidéo*

[25] *ISO/IEC 11172-2:1993/Cor 1*, 1996

[26] *ISO/IEC 11172-2:1993/Cor 2*, 1999

[27] *ISO/IEC 11172-3:1993 : Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s. Part 3: Audio*

[28] *ISO/IEC 11172-3:1993/Cor 1*, 1996

[29] *ISO/IEC 11172-4:1995 : Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s. Part 4: Compliance testing*

[30] *ISO/IEC 11172-5:1993 : Information technology - Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s. Part 5: Software simulation*

[31] *ISO/IEC 13818-1:2000 : Information technology - Generic coding of moving pictures and associated audio information. Part 1: Systems*

[32] *ISO/IEC 13818-2:2000 : Information technology - Generic coding of moving pictures and associated audio information. Part 2: Vidéo*

[33] *ISO/IEC 13818-3:1998 : Information technology - Generic coding of moving pictures and associated audio information. Part 3: Audio*

[34] *ISO/IEC 13818-4:1998 : Information technology - Generic coding of moving pictures and associated audio information. Part 4 : Conformance testing*

[35] *ISO/IEC 13818-4:1998/Cor2*, 1998

[36] *ISO/IEC 13818-4:1998/Amd 1:1999 : Advanced Audio Coding (AAC) conformance testing*

[37] *ISO/IEC 13818-4:1998/Amd 2:2000 : System target decoder model*

[38] *ISO/IEC 13818-4:1998/Amd 3:2000 : Additional audio conformance bitstreams*

[39] *ISO/IEC 13818-5:1997 : Information technology - Generic coding of moving pictures and associated audio information. Part 5 : Software simulation*

[40] *ISO/IEC 13818-5:1997/Amd 1:1999 : Advanced Audio Coding (AAC)*

[41] *ISO/IEC 13818-6:1998 : Information technology - Generic coding of moving pictures and associated audio information. Part 6 : Extensions for DSM-CC*

[42] *ISO/IEC 13818-6:1998/Cor 1*, 1999

[43] *ISO/IEC 13818-6:1998/Amd 1, 2000 : Additions to support data broadcasting*

[44] *ISO/IEC 13818-6:1998/Amd 2 : 2000 : Additions to support synchronized download services, opportunistic data services and resource announcement in broadcast and interactive services*

[45] *ISO/IEC 13818-7:1997 : Information technology - Generic coding of moving pictures and associated audio information. Part 7 : Advanced Audio Coding (AAC)*

[46] *ISO/IEC 13818-7:1997/Cor 1*, 1998

[47] *ISO/IEC 13818-9:1996 : Information technology - Generic coding of moving pictures and associated audio information. Part 9 : Extension for real time interface for systems decoders*.

[48] *ISO/IEC 13818-10:1999 : Information technology - Generic coding of moving pictures and associated audio information. Part 10 : Conformance extensions for digital storage media command and control (DSM-CC)*

[49] 4C, *Content Protection System Architecture : A Comprehensive Framework for Content Protection*. http://www.lmicp.com/4centity/docs/

[50] 5C, *Digital transmission content protection white paper*, http://www.dtcp.com

[51] *DOI : Digital Object Identifiers*. http://www.doi.org

[52] *SDMI : Secure Digital Music Initiative*. http://www.sdmi.org

[53] R. Anderson, F. Petitcolas, "On the limits of steganography", *Special Issue of IEEE J-SAC* (1998)

[54] Apple Computer, "Mac OS cannot eject copy protected audio disc", *AppleCare Knowledge Base Article 106882*, April 2002

[55] P. Bassia, I. Pitas, *Robust audio watermarking in the time domain* (1996)

[56] J. Bickers, "Copy-protected CDs: Piracy defense or rip-off ?" *USA Today*, June 2002

[57] P. Biddle, P. England, M. Peinado, B. Willman, "The Darknet and the future of content distribution", *ACM DRM-2002 Workshop*

[58] M. Blaze, J. Feigenbaum, J. Lacy, "Decentralized trust management", *Proceedings 1996 IEEE Symposium on Security and Privacy*, 164-173, May 1996

[59] Julien Bœuf & Julien Stern, *An Analysis on one of the SDMI Candidates*.

[60] A. Boldyreva, M. Jacobsson, "Theft-protected proprietary certificates", *ACM DRM-2002 Workshop*

[61] L. Boney, H. Tewfik, K. N. Hamdy, "Digital Watermarks for Audio Signals", *EUSIPCO 96*, Trieste, Italy (1996)

[62] D. Boneh, M. Franklin, "An efficient public-key traitor tracing scheme", *CRYPTO 1999*

[63] BSA (Business Software Association), *Annual Report 2002*.

[64] S. Brands, *Rethinking public-key infrastructures and digital certificates – Building in privacy*, PhD Thesis, Technical University of Eindhoven 1999

[65] Bureau Européen des Unions de Consommateurs (BEUC), *Commentaires sur la Position Commune du Conseil concernant la Directive sur les Droits d' Auteur dans la Société de l'Information*, BEUC/X/051/2000, 10 Novembre 2000

[66] Michael Calvert, "Research Management Update: Content Management - Timetable for Digital Rights Management", *Gartner*, IGG-07182001-02, 18 July 2001.

[67] *Campaign for Digital Rights: Corrupt audio discs web site*. http://uk.eurorights.org/issues/cd/bad/.

[68] G. Caronni, "Assuring Ownership Rights for Digital Images", *Proceedings VIS 95*, Session "Reliable IT Systems", p. 3-11 (1995)

[69] H. Chang, M.J. Attalah, "Protecting software code by guards" proceediings *Workshop on Security and Privacy in Digital Rights Management 2001*, Association of Computing Machinery

[70] Rapport particulier de Monsieur Leonardo Chiariglione (Telecom Italia Lab, Italie) *La gestion et la protection des œuvres et de la propriété intellectuelle - État des travaux et des*

réflexions, Ministère de la Culture, Conseil supérieur de la propriété littéraire et artistique, Paris, Octobre 2001.

[71] S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot, "A White-Box DES implementation for DRM applications", *ACM DRM-2002 Workshop*

[72] Y.-H. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick, M. Strauss, "REFEREE: Trust Management for Web Applications", *6th. International World Wide Web Conference*, Santa Clara, CA, April 1997

[73] R. Clark, *An introduction to JPEG 2000 and watermarking*. http://www.jpeg.org

[74] CLCV c. EMI, Tribunal de Grande Instance de Nanterre, 24 juin 2003.

[75] "Online music sales to be muted", *CNET News.com*, July 28, 2003.

[76] Codes régionaux DVD : http://www.unik.no/~robert/hifi/dvd/world.html. Pour de nombreux liens concernant les DVD, voir http://www.unik.no/~robert/hifi/dvd/

[77] Commission européenne, Groupe de protection des données Article 29, *Document de travail concernant les services d'authentification en ligne*, 10054/03/FR, WP 68, 29 janvier 2003

[78] ContentGuard, *eXtensible Rights Markup Language (XrML) 2.1. Submission to the OASIS Rights Language Technical Committee*, May 2002.

[79] Copyright Office, "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies", *US Federal Register*, Vol. 64, No. 226 - Wednesday, November 24, 1999, p. 66139.

[80] I. J. Cox, J. Kilian,T. Leighton, T. Shamoon, "Secure spread spectrum watermarking for multimedia", Tech. Report, *NEC research institute*, 95-01

[81] S. Craver, P. McGregor, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D. S. Wallach, D. Dean, E. W. Felten, http://www.cs.princeton.edu/sip/sdmi/announcement.html

[82] I. Cox, M. Miller, J. Bloom, *Digital watermarking. Multimedia Information and Systems*. Morgan Kaufman Publishers. 2002

[83] S.A. Craver, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D.S. Wallach, D. Dean, E.W. Felten, "Reading between the lines: Lessons from the SDMI challenge", proceedings *10th. USENIX Security Symp.*, 13-17. Aug. 2001

[84] C.R.I.D., *Le droit d'auteur : un contrôle de l'accès aux œuvres ?*, Bruylant, 2000

[85] J. Dittmann, A. Behr, M. Stabenau, P. Schmitt, J. Schwenk, J. Ueberberg, "Combining digital watermarks and collusion secure fingerprinting for digital images", *Proceedings of SPIE, Vol. 3657*, pp. 171-182 (1999)

[86] Y. Dodis, N. Fazio, "Public-key broadcast encryption for stateless receivers", *ACM DRM-2002 Workshop*

[87] T. Ebrahimi, R. Erard, M. Kutter, F. Leprévost, D. Santa Cruz, "How to bypass the Wassenaar Arrangement : A new application for watermarking", *8th ACM International Multimedia Conference on Multimedia and Security* (November 2000, Los Angeles, California, USA).

[88] ECMA, *Data interchange on read-only 120 mm optical data discs (CD-ROM)*, ECMA standard 130, June 1996

[89] In-Stat/MDR, "DRM in 2003: Are We Making Any Progress?", cité in "DRM Makes Minimal Impact, Study Says", May 29, 2003, *Ecommerce News*.

[90] E. F. Foundation, *Cracking DES, Secrets of Encryption Research, Wiretap Politics & Design*, O'Reilly (1998)

[91] F. Ergun, J. Killian, R. Kumar, "A note on the limits of collusion-resistant watermarks", In *Advances in Cryptology – Eurocrypt 99*, LNCS 1592, pp. 140-149. Springer-Verlag, Berlin, Heidelberg, New York 1999

[92] Gartner Group, *Digital Rights Management Has Little Immediate Hope – Market Analysis*, 3 April 2002 ; Gartner Group, *Digital Rights Management (DRM) Software: Perspective - Strategy, Trends & Tactics*, 3 October 2002.

[93] S. Godik, T. Moses, eds. *OASIS eXtensible Access Control Marked Language (XACML). OASIS eXtensible Access Control Marked Language Technical Committee*, Working Draft, September 2002

[94] J. D. Gordy, L. T. Bruton, *Performance Evaluation of Digital Audio Watermarking Algorithms*, Preprint (2000)

[95] Lucie Guibault, "Pre-Emption Issues In The Digital Environment : Can Copyright Limitations Be Overridden By Contractual Agreements Under European Law?", *Instituut voor Informatierecht* (Institute for Information Law, Amsterdam), 1998.

[96] H. Guth, B. Pfitzmann, "Error- and collision-secure fingerprinting for digital data", in *Information Hidding 1999*, LNCS 1768, pp. 134-145, Springer-Verlag, Berlin, Heidelberg, New York, 2000

[97] J. A. Halderman, "Evaluating new copy-prevention techniques for audio CDs" *ACM DRM-2002 Workshop*

[98] P. Hallam-Baker, E. maler, eds., "Assertions and Protocols for the OASIS seccurity assertion markup language (SAML)" in *OASIS XML-based security services technical committee*, May 2002

[99] F. Hartung, M. Kutter, "Multimedia watermarking techniques", *Proceedings IEEE : Special Issue on Identification and Protection of Multimedia Information*, 87(7) :1079-1107, July 1999

[100] F. Hartung, B. Girod, "Digital watermarking of raw and compressed video", in N. Ohta, editor, *Digital compression technologies and systems for video communications*, VOl. 2952 of SPIE Proceedings Series, pp. 205-213, October 1996

[101] F. Hartung, B. Girod, "Digital watermarking of MPEG-2 coded video in the bitstream domain", *Proceedings of International Conference on Acoustic, Speech and Signal Processing* (ICASSP 97), vol. 4, pp. 2621-2624, April 1997

[102] Renato Iannella, "Digital Rights Management (DRM) Architectures", *D-Lib Magazine*, June 2001,Volume 7, Number 6.

[103] Instituut voor Informatierecht (Institute for Information Law, Amsterdam), *Privacy, Data Protection and Copyright : Their Interaction in the Context of Electronic Copyright Management Systems*, Report for the Consortium IMPRIMATUR, 1998

[104] Instituut voor Informatierecht (Institute for Information Law, Amsterdam), *Watermarking Technology for Copyright Protection : General Requirements and Interoperability*, Report for the Consortium IMPRIMATUR, 1998

[105] M. Jacob, D. Boneh, E. Felten, "Attacking an obfuscated cipher by injecting faults", *ACM DRM-2002 Workshop*

[106] M. Jacobson, M.K. Reiter, "Discouraging software piracy using software aging", pp. 1-12 in *Security and Privacy in Digital Rights Management – ACM CCS-8 Workshop DRM 2001* (LNCS 2320), Springer-Verlag, 2002

[107] R. Johnson, J. Staddon, "FAIR: Fair Audience InfeRence", *ACM DRM-2002 Workshop*

[108] A. Kiayias, M. Yung, "Breaking and repairing asymmetric public-key trator tracing", *ACM DRM-2002 Workshop*

[109] A. Kiayias, M. Yung, "On crafty pirate and foxy tracers" in *Security and Privacy in Digital Rights Management. SPDRM 2001*. LNCS 2320, pp. 22-39, Springer-Verlag, Berlin, Heidelberg, New York 2002

[110] R. Koenen, "MPEG-4, Multimedia for our time", *IEEE Spectrum*, vol. 36, No. 2, February 1999, pp. 26-33. http://www.cselt.it/mpeg/tutorials.htm

[111] L. Korba, S. Kenny, "Towards meeting the privacy challenge: Adapting DRM", *ACM DRM-2002 Workshop*

[112] M. Kutter, "Watermarking resisting to translation, rotation, and scaling", *Proceedings of SPIE International Symposium on Voice, Video, and Data Communications* (1998)

[113] M. Kutter, F. Jordan, F. Bossen, "Digital Watermarking of Color Images using Amplitude Modulation", *Journal of Electronic Imaging*, vol. 7, n°2, p. 326-332 (1998)

[114] M. Kutter, F. Leprévost, "Symbiose von Kryptographie und digitalen Wasserzeichen :

effizienter Schutz des Urheberrechtes digitaler Medien", *Tagungsband des 6. Deutschen IT-Sicherheitskongress des BSI*, 479-484 (1999)

[115] M. Kutter, F. Leprévost, T. Ebrahimi, "Efficient copyright protection of multimedia data through the combination of cryptography and digital watermarking", in progress (2000-2001)

[116] B. LaMacchia, "Key challenges in DRM: An industry perspective", *ACM DRM-2002 Workshop*

[117] B. LaMacchia, S. Lange, M. Lyons, R. Martin, K. Price, *NET Framework Security*, Addison-Wesley, April 2002, 45-119

[118] G. C. Langelaar, *Real-time Watermarking Techniques for Compressed Video Data*, PhD Thesis (2000)

[119] L. Lessig, *Code and other laws of Cyberspace*, Basic Books, New-York, 1999

[120] F. Leprévost, *Encryption and cryptosystems in electronic surveillance : A survey of the technology assessment issues*. Scientific and Technological Options Assessment of the European Parliament. Global project n° EP/IV/B/STOA/98/1401/01 (1998)

[121] F. Leprévost, "Les standards cryptographiques du XXI-eme siècle : AES et IEEE-P1363", *La Gazette des Mathématiciens*

[122] F. Leprévost, "AES und IEEE-P1363, die kryptographischen Standards des 21. Jahrhunderts", *Tagungsband des 6. Deutschen IT-Sicherheitskongresses des BSI*, 485-491 (1999)

[123] F. Leprévost, "The end of public-key cryptography or does God play dices?" *PricewaterhouseCoopers Cryptographic Centre of Excellence Quaterly Journal*, Issue 3 (1999)

[124] F. Leprévost, "AES : Round 2", *PricewaterhouseCoopers Cryptographic Centre of Excellence Quaterly Journal*, Issue 3 (1999)

[125] F. Leprévost, B. Warusfel, *Technologies de sécurité pour les médias digitaux*, rapport pour STOA, EP/IV/A/STOA/2000/06/01, mai 2001

[126] A. Lucas, *Droit d'auteur et numérique*, Litec, 1998

[127] M. Maes, T. Kalker, J.-P. M. G. Linnartz, J. Talstra, G. F. G. Depovere, J. Haitsma, "Digital watermarking for DVD video copy protection", *IEEE Signal Processing Magazine*, September 2000, pp. 47-57

[128] *Microsoft "Palladium": A Business Overview*, Août 2002, téléchargeable à http://www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp

[129] D. Mulligan, A. Burstein, "Implementing copyright limitations in rights expression languages", *ACM DRM-2002 Workshop*

[130] "Le Passport de Microsoft met un pied dans les paiements électroniques", *Net-Economie.com*, 10 juillet 2002.

[131] *Open eBook Forum* : http://www.openebook.org

[132] *OPIMA : The Open Platform Initiative for Multimedia Access*. http://www.iec.ch/opima/ + http://drogo.cselt.it/ufv/leonardo/opima/

[133] KW. B. Pennebaker, J. L. Mitchell, *JPEG, Still image data compression standard*, Van Nostrand Reinhold, New York, 1992

[134] F. A. P. Petitcolas, M. Kuhn, "Information hiding - a survey", *Proceedings of the IEEE : Special Issue on Identification and Protection of Multimedia Information*, 87 (7) :1062-1077, July 1999

[135] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, "Attacks on copyright marking systems" in David Aucsmith (Ed), *Information Hiding, Second International Workshop, IH'98*, Portland, Oregon, U.S.A., April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, pp. 219-239.

[136] F. A. P. Petitcolas, R. J. Anderson, "Evaluation of copyright marking systems", in *proceedings of IEEE Multimedia Systems (ICMCS'99)*, vol. 1, pp. 574--579, 7--11 June 1999, Florence, Italy.

[137] F. A. P. Petitcolas (http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/)

[138] "Musique : voilà pourquoi votre CD est muet ", *Que Choisir-Mensuel*, n° 405 - juin 2003 , télécheargable sur le site http://www.quechoisir.org.

[139] *Rightscom Limited*, "Digital Rights Management and the New Business Models"

[140] "CD creator burns copy-protection efforts", *Reuters*, January 17, 2002

[141] S. Roche, *Mécanismes de Sécurité liés à la Diffusion des Images : Tatouage d'Image*, Thèse, Institut Eurecom Sophia-Antipolis, Mai 1999

[142] R. Safavi-Naini, Y. Wang, "Traitor tracing for shortened and corrupted fingerprints", *ACM DRM-2002, Workshop Stanford University: Copyright and fair use web site*. http://fairuse.stanford.edu

[143] D. Santa Cruz et T. Ebrahimi, "A study of JPEG 2000 still image coding versus other standards", ISO/IEC/SC29/WG1 N1814 (July 2000), *Proceedings of EUSIPCO 2000*

[144] D. Santa Cruz, T. Ebrahimi, J. Askelöf, M. Larsson, C. Christopoulos, "An analytic study of JPEG 2000 functionalities", ISO/IEC/SC29/WG1 N1816 (July 2000), *Proceedings of SPIE*, vol 4115, of the 45th annual SPIE meeting, Applications of Digital Image Processing XXIII

[145] "Doesn't Everybody Do It? Internet Piracy Attitudes and Behaviors", *SIIA/KMPG LLP*, 2001.

[146] M. Stefik, "Shifting the Possible : How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing", *Berkeley Technology Law Journal*, 12 (1997)

[147] Alain Strowel et Séverine Dusollier, *La protection légale des systèmes techniques*, document OMPI, 1999

[148] M.D. Swanson, M. Kobayashi, A.H. Tewfik, "Multimedia Data Embedding and Watermarking Techniques", *Proceedings of the IEEE*, vol. 86, n°6, 1064-1087 (1998)

[149] M. D. Swanson, B. Zhu, A. Tewfik, "Multiresolution scene-based video watermarking using perceptual models", *Journal on selected areas in Communications*, pp. 540-550 (1998)

[150] K. Tanaka, Y. Nakamura, K. Matsui, "Embedding the Attribute Information into a Dithered Image", *Systems and Computers in Japan*, p. 1-25 (1990)

[151] L. Trotter Hardy, *Project Looking Forward : Sketching the Future of Copyright in a Networked World*, Report for the U.S. Copyright Office May 1998

[152] Vidéo et DVD archives, *The Electronic Frontier Foundation* "Intellectual Property - Video and DVD" Archive (http://www.eff.org/ip/Video), *DVD Copy Control Association* (http://www.dvdcca.org)

[153] B. Warusfel, "Internet : nouvelles problématiques face à la contrefaçon", in *L'entreprise face à la contrefaçon de droits de propriété intellectuelle*, IRPI, Ed. Litec, 2003

[154] B. Warusfel, *La propriété intellectuelle et l'Internet*, Paris, Ed. Flammarion, février 2001.

[155] Warner: "Copy-Proof CDs cracked with 99-cent marker pen.", *Reuters*, May 24, 2002

[156] *Viant Inc*, juin 2002.

[157] Xerox Corp., *The Digital Property Rights Language Manual and Tutorial - XML Edition, v2.00*, 13 nov. 1998 (http://www.contentguard.com/DPRLmanualXML.doc).

F. L. : Institut Fourier (Université de Grenoble I), UMR 5582 du CNRS, B.P. 74,
F-38402 St Martin d'Hères cedex (France), et
Centre Universitaire du Luxembourg, 162 A, Avenue de la Faïencerie, L-1511 Luxembourg
e-mail : Franck.Leprevost@ujf-grenoble.fr

B. W. : Université René Descartes Paris V – Faculté de droit, et
4, rue Saint-Florentin, F-75001 Paris (France)
e-mail : warusfel@droit.univ-paris5.fr