Rapport n° 2003-02 — (I)

MESURES TECHNIQUES DE PROTECTION

DES OEUVRES & DRMS

1ERE PARTIE : UN ETAT DES LIEUX — JANVIER 2003

Étude établie par Philippe CHANTEPIE

Chargé de mission à l'Inspection Générale de l'Administration des Affaires Culturelles

Marc HERUBEL

Chef du Bureau du Multimédia et de la Sécurité à la Direction Générale de l'Industrie des technologies de l'Information et des Postes

Franck TARRIER

Adjoint au Chef du Bureau des Techniques et des réseaux de communication à la Direction du Développement des Médias

8 janvier 2003

LETTRE DE MISSION

MESURES TECHNIQUES ET SYSTEMES NUMERIQUES DE GESTION DE DROITS
(sont mis en gras les éléments relatifs à cette 1re partie de l'étude)

Dans le contexte de la transposition de la directive n° 2001/29 CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, **il convient de réaliser un état des lieux des mesures d'identification et de protection technique des œuvres et des droits.**

Celui-ci s'attachera à apprécier **l'impact des mesures techniques, leur utilité pratique pour la lutte contre la contrefaçon, et leur faculté à satisfaire le respect d'accords contractuels conclu par les titulaires de droits, s'agissant de mesures volontaires mises en œuvre par les titulaires de droits.** Il pourra, à titre d'exemple, prendre en compte les domaines prévus par les articles 5.2. et 6.4 de la directive.

i. **L'étude visera à <u>présenter l'état de l'art des protections techniques</u> en distinguant notamment les techniques de protection des œuvres mêmes (standards d'encodage, *watermarking*, cryptage, etc.), les techniques de protection des supports de stockage et de reproduction (CD Audio, DVD, etc.), les techniques de protection logicielle, les techniques de protection des interfaces de diffusion (décodeurs), mais aussi des techniques de protection au sein des réseaux de communication (protection du signal, protection à partir des protocoles de réseaux, etc.).**

ii. **À partir évolutions technologiques réalisées, notamment depuis l'adoption du traité de l'OMPI de 1996, il conviendra de <u>chercher à apprécier et anticiper la robustesse et la pertinence des mesures de protection technique à moyen terme</u> (trois ans). Deux catégories d'œuvres pourront être privilégiées dans le cadre de cette étude : les œuvres musicales et les œuvres audiovisuelles ou cinématographiques. À cet effet, l'étude devra s'appuyer sur les travaux en cours menés notamment à l'échelon national, qu'il s'agisse de R&D publique (INRIA, ENST, ENS, etc.), ou mixte (RIAM, RNRT), voire de développements menés par les industriels (*Canal+ Technologies*, *Thomson Multimédia*, *Philips*, *Sony France*, *Microsoft France*, etc.). Elle examinera aussi les travaux et les attentes des bénéficiaires des protections qu'ils soient titulaires de droits d'auteur ou de droits voisins. Elle aura enfin, à présenter et à apprécier autant que possible les travaux menés à l'échelon international, notamment sous la forme de consortium (*SDMI*, *MPEG-21*, *W3C*, etc.) et leur impact sur le plan national.**

iii. Au regard de l'importance stratégique et des implications juridiques que revêtent désormais les systèmes de protection technique et d'identification des œuvres, l'étude pourra **<u>le cas échéant, faire des propositions en faveur d'un usage informé, efficace et respectueux des droits et libertés</u>**.

SYNTHÈSE

Les mesures techniques de protection et les Systèmes numériques de gestion des droits (*Digital Rights Management Systems*) constituent un ensemble de protections en cours de développement rapide, du fait de la forte convergence d'intérêts économiques des acteurs industriels et culturels : les industries culturelles, en vue d'assurer la protection des contenus numériques pour de nouvelles formes de distribution et d'exploitation ; les industries de l'électronique grand public comme de l'informatique, de l'édition des logiciels et des systèmes d'exploitation en vue de la croissance de leurs marchés.

Cette convergence d'intérêts économiques se concentre sur la mise en œuvre de mesures techniques de plus en plus combinées qui empruntent à la cryptographie et aux technologies du *watermarking.* Elle se déploie à travers la constitution de consortiums industriels mondiaux, à la fois rivaux et complémentaires pour atteindre des cibles de sécurité sur l'ensemble de la chaîne de la distribution de contenus numériques : production et gestion numérique des droits, distribution par réseaux ou supports optiques, lecture, etc.

La convergence de la recherche et du déploiement des mesures techniques tend à se concentrer sur les techniques d'encodage, les interfaces et les outils de lecture, mais aussi sur les passerelles d'accès entre trois univers principaux : l'univers des supports physiques, l'univers de l'informatique ouvert aux réseaux eux-mêmes ouverts, l'univers de l'électronique grand public.

i. Des techniques de plus en plus adaptées à l'univers de protection des contenus.

Le contrôle des accès entre ces univers apparaît ainsi comme la clé de voûte de la protection des contenus numériques et le cœur de la compétition industrielle mondiale entre l'ensemble de ces secteurs.

Dans ces conditions, la distinction juridique entre les mesures de protection et les mesures de contrôle d'accès s'estompe très largement. Car, derrière la mise en œuvre des mesures techniques de protection, se joue surtout l'offre de Systèmes numériques de gestion de droits (*Digital Rights Management Systems*), donc des formes intégrées de distribution numérique protégée techniquement qui emploient toutes les mesures techniques et présentent, à travers les langages de description de droits une assez grande souplesse pour s'adapter à la diversité des droits nationaux :

– les technologies de cryptographie applicables autant pour la protection de supports physiques que pour le contrôle d'accès et l'utilisation des contenus numériques ;

– les technologies de *watermarking*, utilisables pour la reconnaissance des droits, mais aussi la traçabilité, l'analyse d'audience ou la lutte contre la contrefaçon, etc.

– des combinaisons variables en fonction de cibles de sécurité par catégories d'œuvres, de modes de distribution des contenus numérique (supports, réseaux), d'économie des secteurs concernés, de publics visés.

– l'application dans des systèmes numériques de gestion de droits de l'ensemble de ces éléments, à nouveau avec des qualités de sécurité variées.

L'efficacité et la robustesse de ces techniques dépendent de trois facteurs principaux :

– la mise en place d'éléments de sécurité matériels (composants électroniques), plus robustes que des éléments logiciels ;

– la renouvelabilité, car la difficulté du contexte de sécurité et la forte valeur des contenus amènent de façon quasi certaine au piratage des protections, dans un délai généralement plus court que le cycle de vie des matériels de lecture utilisés ; la carte à puce est une solution qui répond bien à ces deux premiers critères ;

– la connexion permanente, qui permet d'éviter de stocker chez l'utilisateur des données de sécurité critiques

Nombreuses parmi ces techniques sont celles qui sont déjà à l'œuvre, parfois bien au-delà d'un stade expérimental. Leur déploiement devrait s'accélérer au cours des années présentes. **Dans ce contexte, la mise en œuvre de ces mesures semble moins dépendre de la robustesse des mesures et des systèmes, nécessairement relative aux cibles de sécurité assignées, que de l'acceptation par les utilisateurs, et notamment, ceux du domaine informatique, des limites techniques posées – artificiellement – à un environnement numérique – techniquement – ouvert et homogène, en fonction de leur transparence, de leur simplicité et finalement de leur faculté à rendre plus commodes les usages d'accès aux œuvres.**

ii. Des enjeux juridiques et sociaux.

C'est pourquoi, au-delà de « l'état de l'art » des mesures techniques de protection et du contrôle de la distribution de contenus numériques, de la robustesse relative de celles-ci, de l'appréciation du temps nécessaire à leur déploiement, **les véritables enjeux des mesures techniques sont de nature juridique et sociale : ils ont affaire au champ de protection juridique de ces mesures techniques et aux conséquences pratiques qui en résulteront pour les utilisateurs, en fonction de la puissance de la convergence des intérêts industriels.**

Ces enjeux se manifestent bien pour chacun dans la faculté d'usage licite de l'environnement numérique et de l'accès aux contenus numériques, véritable ressort de la société de l'information. Ils dépendront pour beaucoup de l'intermédiation que pourront effectuer les distributeurs, passerelle nécessaire entre les attentes des consommateurs, le monde de l'industrie des technologies de l'information et le monde de l'industrie culturelle. Cette intermédiation aura à vaincre des écueils et à participer à un défi **en favorisant une concurrence attractive d'offres licites de contenus** :

– **réduire l'attraction pour les usages illicites des réseaux de distribution de contenus en pair à pair** qui sont paradoxalement l'un des plus puissants facteurs d'accélération de la mise en œuvre des mesures techniques et de contrôle d'accès ;

– **faciliter l'intégration de l'ensemble de la chaîne de distribution de contenus numériques**, notamment sur ses maillons faibles : la gestion numérique des droits, la facilité d'usage des utilisateurs.

Au plan européen, une grande part des débats relatifs aux *DRMS* et aux mesures techniques, a trait aux nouveaux équilibres que leur déploiement créera en ce qui concerne la copie privée, notamment du fait de l'existence d'un « système de rémunération » pour copie privée. De l'analyse des mesures techniques comme de la présentation synthétique des *DRMS*, ressortent les éléments suivants :

– **le champ de l'exception pour copie privée, fondée historiquement sur une tolérance contingente à l'environnement technique, va subir une mutation très profonde** ;
– les mesures techniques de protection et plus encore les *DRMS* sont à l'œuvre d'une part pour **fixer dans le code les conditions précises d'une ligne de partage entre copie numérique de contrefaçon et copie privée** ;

– les mesures techniques de protection et plus encore les *DRMS* sont constituées pour **permettre un retour à l'exercice intégral des droits exclusifs** des auteurs, des producteurs et des artistes et interprètes, d'autoriser ou d'interdire la reproduction des œuvres, y compris les copies privées numériques ;

– les *DRMS*, associés ou non à des protections techniques des supports, sont en mesure de **favoriser un nouveau champ d'« exploitation normale » de la copie numérique, principalement rémunérée** dans le cadre du commerce électronique des contenus, par une chaîne électronique de valeur dans laquelle chaque copie privée numérique peut donner lieu à une compensation ;

– les *DRMS*, associés ou non à des protections techniques des supports, facilite donc pour l'exercice des droits exclusifs **la transition progressive du système actuel de rémunération forfaitaire vers une rémunération proportionnelle**.

Pour chacune de ces évolutions, les utilisateurs auront à jouer un rôle central, qu'il s'agisse du choix des offres et des systèmes de facturation associés, plus ou moins forfaitaires (achat, location, avec ou sans possibilité de copie, abonnement, paiement à l'acte,…), qu'il s'agisse de l'appréciation du rapport entre confort d'utilisation et fermeture de l'environnement numérique.

iii. Des enjeux industriels et culturels.

En deçà des résultats de l'état de l'art des mesures techniques et des *DRMS*, il apparaît que ces questions sont au centre d'une compétition internationale de grande ampleur entre différents secteurs industriels. Elle se joue avec un arrière-fond constitué par l'impact des réseaux *P2P*, utilisés à la fois comme moyen de développement (informatique, télécommunications), élément de blocage (industries culturelles) ou de prudence sur l'ouverture aux réseaux (électronique grand public), mais surtout levier de compétition et de négociation. Cette compétition peut se décliner ainsi :

– entre **industries culturelles**, désireuses de profiter des opportunités présentées par de nouveaux modes de distribution et soucieuses d'éviter les risques liés à la prolifération de la contrefaçon, et **industries de l'électronique, de l'informatique et**

des télécommunications, désireuses de bénéficier de l'attraction des utilisateurs pour les contenus numériques.

– entre **industries de l'électronique grand public**, traditionnellement attachées aux industries culturelles, face à un couple « nouvel » entrant : **les industries de l'informatique et des télécommunications** qui favorisent toutes les formes d'accès aux contenus numériques.

– **entre l'ensemble des acteurs sur les articulations principales de la chaîne de valeur**, soit en protégeant les contenus, soit au contraire en ne les protégeant pas, du moins provisoirement ; et surtout, en cherchant à gagner des positions en amont de la chaîne (description des droits et titularité des droits) ou en aval (édition des logiciels de lecture).

La compétition n'est pas achevée mais des perspectives de stabilisation sont en cours : multiplication des accords de standardisation, évolution de l'ensemble des modèles économiques sur des logiques économiquement soutenables, mise en œuvre désormais rapide d'accords de protection entre industries culturelles et industries des technologies de l'information. Les résultats de cette compétition ne sont pas neutres pour les industries nationales qu'elles soient celles de l'électronique grand public ou culturelles. Elles ne sont pas non plus neutres du point de vue du droit de la concurrence.

Cependant, ces enjeux industriels et culturels de moyen terme mais aux effets durables restent pour le moment relativement absents des débats actuels. Ils se concentrent sur les inconvénients parfois très réels posés aux consommateurs par les mesures techniques appliquées au support le plus ancien (CD Audio) appelé à disparaître. Ils touchent aussi le périmètre de la faculté de copie privée et ses effets juridiques et économiques relatifs à sa compensation. Ils manquent sans doute encore d'aborder les conséquences des changements profonds qu'entraîne pour les utilisateurs et les industries la mutation du droit de propriété littéraire et artistique qu'effectue la protection juridique des mesures techniques.

* * *
*

AVANT-PROPOS

La lettre de mission précise : « *dans le contexte de la transposition de la directive n° 2001/29 CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, il convient de réaliser un état des lieux des mesures d'identification et de protection technique des œuvres et des droits* ». Aussi, l'étude a-t-elle cherché à réaliser dans une période assez courte à dresser un état des lieux des mesures techniques de protection et *DRMS* en cours de commercialisation ou de développement qui puisse être à la fois aussi complet que synthétique.

Certaines techniques ne sont pas encore sur le marché mais devraient l'être au cours des deux prochaines années selon les architectures générales présentées. L'étude a aussi voulu indiquer certains enjeux soulevés par l'introduction de *Digital Rights Management Systems* (*DRMS*) et conserver un équilibre entre le caractère scientifique et technique de son objet et l'indispensable accès à l'information des lecteurs non spécialistes. La recherche de cet équilibre difficile explique certainement beaucoup d'insuffisances techniques.

Les industriels et les chercheurs doivent être particulièrement remerciés d'avoir bien voulu présenter aussi librement que possible les réalisations techniques ou l'état de leurs travaux.

Il a naturellement été proposé, d'une part à la Direction Générale de l'Industrie des technologies de l'Information et des Postes (DiGITIP) du Ministère de l'Industrie, d'autre part à la Direction du Développement des Médias, d'être pleinement associées à la préparation et la confection de cette 1re partie de l'étude sur les aspects techniques et industriels. **M. Alain SEBAN,** Directeur (Direction du Développement des Médias) et **M. Emmanuel CAQUOT,** Chef du service des technologies et de la société de l'information (DiGITIP) **doivent être particulièrement remerciés d'avoir accepté que ce travail puisse bénéficier du concours de :**

– Marc HERUBEL, Chef du Bureau du Multimédia et de la Sécurité à la Direction Générale de l'Industrie des technologies de l'Information et des Postes ;

– Franck TARRIER, Adjoint au Chef du Bureau des Techniques et des réseaux de communication à la Direction du Développement des Médias.

Ils ont l'un et l'autre très largement contribué à la réalisation de cette étude, respectivement, pour la partie relative à la cryptographie et aux enjeux industriels, et pour la partie relative au fonctionnement synthétique des *DRMS*.

* * *

INTRODUCTION

« Avec le XX° siècle, les techniques de reproduction ont atteint un tel niveau qu'elles vont être en mesure désormais, non seulement de s'appliquer à toutes les œuvres d'art du passé,… mais de s'imposer elles-mêmes comme des formes originales d'art. »

W. Benjamin, *L'œuvre d'art à l'âge de la reproductibilité technique.*

« The machine is the answer to the machine… A system must be able to identify copyright materials, to track usage, to verify users, and to record usage and appropriate compensation. In addition, the system should provide security for the integrity of the copyrighted material (freedom from tampering) and some level of confidentiality or privacy for the user. »

Charles Clark, *The Publisher in the Electronic World*

« *Ce qui compte ce n'est pas la barrière, mais l'ordinateur qui repère la position de chacun, licite ou illicite, et opère une modulation universelle.* »

Gilles Deleuze, *Post-scriptum sur les sociétés de contrôle.*

« La protection des contenus permet d'abandonner définitivement le concept de copie en tant que pierre angulaire de la protection des titulaires de droits »

L. Chiariglione, *Rapport au CSPLA sur la gestion et la protection des œuvres et de la propriété intellectuelle, 2001.*

A la croisée de ces réflexions, se ramifie puis se noue le fil des questions posées par la protection juridique des mesures techniques de protection des œuvres, elles-mêmes objet de la protection du droit de propriété littéraire et artistique. La reproductibilité technique des œuvres qui n'a cessé de progresser jusqu'à confondre l'« aura » de l'œuvre d'art et ses simulacres techniques ou d'interroger la pertinence du concept de copie, la réponse technique et utilitariste à la déstabilisation économique et juridique qui en procède, la prévention, enfin posée, au lieu d'où dérivent bien des conséquences de l'émergence des protections techniques, forment ce carrefour.

La transposition de la *Directive 2001/29 CE relative à l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information* sera sans doute l'occasion, en dépit de sa complexité, de ses équilibres propres et d'une connaissance difficile de l'état exact des techniques, d'aborder et de trancher pour un temps cet ensemble de questions, ouvertes depuis plus d'une décennie. Car, avec la vivacité des débats suscités depuis l'adoption du *Digital Millenium Copyright Act*, bien des questions relatives à la protection juridique des mesures techniques de protection des œuvres, sont connues : l'accès aux œuvres, les risques d'intrusion dans la vie privée, la limitation des usages, notamment de copie privée numérique, voire la mise en cause de la liberté de communication, etc., et bien sûr, les conditions effectives d'une économie durable de la création.

Le développement d'un droit des mesures techniques de protection des contenus numériques succède de peu à l'essor rapide de la recherche et surtout du développement industriel de ce type de technologies. Depuis l'adoption du Traité ADPIC prévoyant que chaque Etat doit établir un régime juridique protecteur des droits exclusifs des droits d'auteurs et droits voisins, et surtout depuis l'adoption des Traités OMPI de 1996, la protection juridique des mesures technique est devenue le canon intellectuel international de la protection de ces droits dans l'environnement numérique.

La *directive 2001/29 CE du 22 mai 2001 relative à certains aspects du droit d'auteur et des droits voisins dans la société de l'information* a pour fonction d'assurer l'intégration de cette norme internationale dans les droits internes des Etats membres. L'objet de la directive consiste précisément à définir une protection juridique des actes préparatoires ou de neutralisation des mesures de techniques efficaces, qu'il s'agisse de dispositifs de contrôle d'accès ou de mesures techniques de contrôle de copie. L'établissement d'une pareille protection juridique recèle, du point de vue industriel et technique, comme du point de vue juridique et culturel, un très grand nombre d'enjeux.

- **du point de vue industriel**, il paraît accroître une concurrence très vive sur le terrain de la propriété industrielle pour commercialiser des systèmes propriétaires, à défaut des standards normalisés internationalement. L'universalisation du droit de protection des mesures techniques favorise alors aussi bien la R&D en amont (*watermarking*, cryptographie, édition logicielle, etc.) qu'une compétition industrielle et commerciale qui conduit à une logique de concentration autour d'un assez petit nombre d'acteurs.

- **du point de vue juridique et culturel**, pareille sûreté juridique cherche à garantir les conditions d'une économie durable de la création dans l'environnement numérique, dès lors de plus en plus tributaire de la capacité économique à accéder aux mesures techniques de protection et des investissements à la mise en œuvre de plates-formes de distribution riche.

- **du point de vue des utilisateurs**, les conséquences ne sont pas plus neutres : si les mesures techniques ont pour mission d'« aider les gens honnêtes à le rester », elles pourront apparaître au plus grand nombre comme inutilement contraignantes notamment si la robustesse des techniques est proportionnelle à aux défauts de « jouabilité ». Elles pourraient offrir de manière transparente un potentiel d'usages conformes nouveaux, fondés sur les licitations de droits numériques, eux-mêmes nouveaux du fait du numérique (location, prêt, test, etc.). Mais elles pourront tout autant être appréciées comme des contraintes techniques limitatives, intrusives et stérilisantes de nouveaux usages. La dynamique de création mutuelle de modèles économiques, de modèles d'usages, de modèles techniques et de modèles juridiques, constitue le facteur clef du développement conjoint d'une économie numérique des industries culturelles d'une économie des solutions techniques et d'usages satisfaisants et riches. Elle reste encore largement à créer.

La directive met en jeu de manière plus directe, la confrontation d'intérêts très variés, en particulier en raison du développement des mesures techniques et de leurs catégories. Les mesures techniques de protection de l'accès ont affaire avec l'économie de la distribution de contenus numériques culturels, sa concentration, sa gestion, etc. ; elles ont aussi affaire avec la liberté des différentes catégories d'utilisateurs d'accéder aux œuvres ainsi protégées. Les *DRMS* comprennent des mesures techniques de protection et de contrôle de copie mais visent surtout à donner une traduction technique à l'exercice de l'exception de copie privée des droits exclusifs des auteurs et de titulaires de droits voisins. Ils contribuent ainsi à modifier en profondeur la gestion des droits exclusifs qui ont vocation à une rémunération proportionnelle davantage qu'à emprunter des systèmes de rémunération de copie privée, comme la Commission L. 311.5 du CPI.

Envisager ces questions impliquait bien de procéder à une étude synthétique, d'une part des mesures techniques de protection, et d'autre part, des « Systèmes Numériques de Gestion de Droits » dont la fonction est de créer une chaîne numérique de distribution de contenus numériques protégés, c'est-à-dire employant des mesures techniques de protection.

Pour présenter **« l'état de l'art des protections techniques »**, l'étude a été réalisée à partir d'analyses successives d'un nombre important, sans doute incomplet, de solutions techniques sur le marché. Plusieurs acteurs contactés par la DREE aux États-Unis n'ont pas souhaité répondre, ce qu'on ne peut que regretter. Pour tendre à une position de neutralité et échapper autant que possible aux effets de progrès et d'obsolescence, l'étude s'est aussi appuyée sur l'analyse de chercheurs dans ce domaine. La même méthode a été empruntée pour « **chercher à apprécier et anticiper la robustesse et la pertinence des mesures de protection technique** », c'est-à-dire, en réalité, analyser au moins pour partie leur **« efficacité »** intrinsèque, notamment pour les contenus numériques des œuvres des secteurs de la musique, du cinéma et de l'audiovisuel. Cependant, le critère d'efficacité est juridiquement selon les termes de la directive du 2001/29 du 22 mai 2001 relatif à l'atteinte de l'objectif poursuivi et ne suppose pas une robustesse absolue, d'ailleurs hors de portée. **Il va de soi en effet, qu'aucune mesure technique de protection des œuvres ne prétend à une quelconque inviolabilité, infaillibilité, robustesse absolue, mais que chacune ou leur combinaison tendent à dissuader des usages illicites ou non conformes d'œuvres**. La dynamique initiée par les accords OMPI de 1996 quant à la protection juridique des mesures techniques (interdiction légale de contournement) repose donc désormais sur **une logique bouclier/glaive** sans doute durable.

Pour examiner enfin les conditions dans lesquelles le développement de ces mesures techniques pourrait s'opérer « **en faveur d'un usage informé, efficace et respectueux des droits et libertés** », le parti a été d'abord pris d'y contribuer par **une présentation aussi pédagogique, neutre et synthétique** que possible de l'état de l'art de ces mesures techniques. Ensuite, à mesure de l'analyse des mesures techniques et notamment à chaque étape de description d'un système numérique de gestion des droits, d'en **présenter les principaux effets et enjeux.** Ainsi, dans les étroites limites d'une telle étude, celle-ci peut pointer un certain nombre de questions soulevées tant au regard du droit de la concurrence que du droit de la protection de la vie privée. Mais, il appartient évidemment aux autorités nationales ou communautaires compétentes d'examiner plus avant d'éventuelles conséquences en ces matières que pourrait soulever le déploiement des *DRMS*.

En dépit des limites d'une telle étude et de son inéluctable obsolescence rapide, elle devrait permettre d'éclairer les analyses relatives pour la transposition de la directive 2001/29. Elle devrait aussi servir de base à un travail de suivis réguliers de ce secteur et de ces technologies, à bien des égards stratégiques, autant pour l'industrie que la culture et très importants pour les consommateurs.

* * *
*

1. L'ENVIRONNEMENT DES MESURES TECHNIQUES ET DES *DRMS*.

Depuis le début des années quatre-vingt-dix, l'accélération de l'intégration de la chaîne numérique des contenus, partant de la production jusqu'à la multiplicité des supports de stockage et appareils de lecture, en passant par la numérisation des réseaux, s'est accompagnée d'une mutation de la protection juridique de ces contenus. Les traités OMPI de décembre 1996 ont tracé, pour l'ensemble des Etats, **un modèle de protection juridique des mesures techniques de protection des contenus numériques, notamment en ce qui concerne la phase de distribution de cette économie et la sphère d'usages des consommateurs.**

Contrairement à l'idée faussement répandue d'un rejet d'une absence d'adaptation du droit de la propriété littéraire et artistique à son environnement technique, **le droit de propriété littéraire et artistique a opéré un véritable bouleversement en empruntant ce modèle de protection issu des droits du logiciel et des bases de données pour y fonder les conditions d'une économie durable des œuvres de l'esprit**. Engagée depuis près de dix ans, cette mutation se révèle seulement depuis peu, à travers des manifestations très pratiques et très sensibles pour les consommateurs : pourquoi ne puis-je pas graver l'œuvre que je viens d'acheter chez mon disquaire ou sur Internet, pourquoi mon CD Audio n'est-il pas lisible sur mon PC ou mon autoradio, comment regarder un DVD, pourquoi encore ne puis-je plus déplacer des fichiers musicaux vers mon baladeur *MP3*, etc. ? À chaque fois survient une application de mesures techniques ou la mise en œuvre de fonctions de *Digital Rights Management Systems*.

En arrière-fond, la plupart des réponses à ces questions tiennent aux stratégies économiques, industrielles et techniques menées avec l'émergence de l'économie numérique des contenus. En particulier pour l'économie de la création, elles tiennent à la rencontre :

– de la nécessité de **préserver et développer la valeur économique des industries culturelles** basculant dans l'environnement numérique ;

– de l'intérêt d'**exploiter le nouveau besoin de sécurité** de ces valeurs économiques, profondément attractives pour le **déploiement des industries des technologies de l'information** : informatique, télécommunications, électronique grand public ;

– du **souci de former des offres commerciales les plus adéquates pour satisfaire le consommateur final dans son appétence pour les contenus et dans des conditions d'usages toujours plus flexibles**.

La réunion de ces trois exigences se traduit par le développement des mesures techniques de protection des contenus numériques. Elle en constitue le cadre qui concentre les intérêts respectifs des acteurs économiques.

1.1. LES ACTEURS.

Les contenus numériques sont à l'évidence un facteur majeur d'attraction des technologies de l'information pour les utilisateurs finaux. À côté de la sphère professionnelle, ils constituent pour les industries des technologies de l'information un puissant levier de développement. Dans ce contexte, l'économie des contenus dans l'environnement numérique a conduit chacune des catégories d'acteurs – industries des technologies de l'information d'une part, industries culturelles d'autre part – non seulement à s'organiser mais surtout à opérer des rapprochements importants et réguliers.

Cette convergence d'intérêts n'écarte pas la permanence d'oppositions fortes dont témoignent notamment les débats et les contentieux aux États-Unis notamment. Il reste que la concentration progressive des acteurs des deux types d'industrie conduit à un développement assez rapide des technologies en faveur de mesures techniques.

1.1.1. LES ACTEURS DE L'INDUSTRIE ET LEURS ENCEINTES.

Deux catégories d'industries sont particulièrement concernées par le développement des mesures techniques, mais selon des exigences différentes : l'industrie de l'informatique et l'industrie de l'électronique grand public. Malgré leurs différences de marchés et d'intérêts, leur coopération est très large au sein d'enceintes de normalisation voire de consortiums spécifiques.

1.1.1.1. Les acteurs industriels de la protection des contenus.

Deux secteurs industriels sont principalement actifs : l'électronique grand public et l'informatique, auxquels il faut ajouter quelques entreprises spécialisées.

i. Les entreprises.

– L'industrie de l'électronique grand public est principalement orientée vers des systèmes de lecture et d'enregistrement de supports optiques (CD Audio, DVD) ainsi que par les équipements de réception TV (*set top box*, c'est-à-dire décodeur) et d'affichage (écrans TV). Cette industrie est assez concentrée autour des acteurs suivants :

– Sony. D'origine japonaise, le groupe *Sony* est le leader mondial de l'électronique grand public. Son chiffre d'affaires sur l'exercice 2001-2002 atteint 60 milliards d'euros, dont 24,5 milliards en électronique dans le domaine multimédia et 10 milliards dans le domaine de l'informatique. Il emploie 168 000 salariés à travers le monde.
Sony a mis en place de nombreux partenariats avec *Philips* : déjà le standard du CD Audio (*Compact Disc Audio*) en 1980 puis celui du DVD Vidéo (*Digital Versatile Disk Vidéo*) avec *Toshiba* et *Warner Home Video* en 1995, avaient été des propositions communes. En 1999, *Sony* et *Philips* se sont alliés pour proposer un nouveau format, le *Super Audio CD*. Ce format, comme son concurrent le DVD Audio, permet de stocker jusqu'à 6 bandes sons (le CD Audio, en stéréo, en avait seulement deux) et bénéficie d'un système de protection contre la copie. *Sony* et *Philips* ont également racheté ensemble fin 2002 l'entreprise *Intertrust*, spécialisée dans les systèmes numériques de gestion des droits et de distribution des œuvres par internet. Dans ces domaines, *Intertrust* détient des brevets essentiels qui font l'objet de conflits avec *Microsoft.*

Sony a également inventé en 1991 le *MiniDisc*, un disque magnéto-optique réenregistrable pour baladeur, intégrant les systèmes de contrôle des copies SCMS (*Secure Copy Management System*) et HCMS (*High speed Copy Management System*). Il a également lancé début 2002 le système *Key2audio* de protection de CD Audio qui empêche le stockage sur ordinateur de la musique ainsi protégée. Par ailleurs, *Sony* s'est également impliqué dans des activités de production de contenus, à travers ses divisions *Sony Computer Entertainment* (consoles et jeux vidéo), *Sony Music Entertainment* et *Sony Pictures Entertainment*, issues du rachat en 1988 de *CBS Records* puis en 1989 de *Columbia Pictures Entertainment*. *Sony* a enfin lancé en fin 2001 avec *Vivendi Universal* le service *Pressplay* de distribution en ligne de leur catalogue audio, ainsi que de celui d'*EMI*.

– *Matsushita* Le groupe *Matsushita* (*Matsushita Electric Industrial* — MEI), d'origine japonaise, est plus connu à travers ses marques *Panasonic* ou *Quazar*. En 2001-2002, il a réalisé un chiffre d'affaires de 59 milliards d'euros, dont 16 milliards dans le domaine de l'électronique multimédia. Il emploie 267 000 salariés à travers le monde. Il est notamment à l'origine, avec *Toshiba*, du système de protection des DVD, le CSS (*Content Scramble System*) adopté en 1996 par le CPTWG. Il participe également aux consortiums *4C* et *5C*, à l'origine de plusieurs propositions de systèmes de protection du contenu (cf. *infra*).

– *Philips*. D'origine néerlandaise, le groupe *Philips* est n° 3 mondial et n° 2 en Europe dans le domaine. Il est particulièrement actif dans le domaine des tubes cathodiques couleur (n° 2) et leader dans le domaine des modules pour graveurs de CD Audio et écrans LCD de grande dimension. *Philips* a réalisé en 2001 un chiffre d'affaires de 32 milliards d'euros, dont 11 dans le domaine de l'électronique grand public. Il emploie 184 000 salariés à travers le monde. *Philips* a été à l'origine avec *Sony* du CD Audio, du DVD et propose aujourd'hui le SACD. Il a également annoncé récemment sa participation au consortium *SmartRight* avec *Thomson*. *Philips* a également des activités à destination des producteurs et diffuseurs. Dans ce cadre il propose, en partenariat avec *Digimarc* qui détient les brevets aux États-Unis, des solutions de tatouage avec le système *Watercast*, et il participe également au *Video Watermarking Group*.

– *Thomson* (ex *Thomson Multimédia*). D'origine française, le groupe *Thomson*, avec ses marques *RCA* aux États-Unis et *Thomson* en Europe est le n° 1 dans le domaine des tubes cathodiques couleur et dans le domaine des décodeurs numériques. Il a réalisé en 2001 un chiffre d'affaires de 10,5 milliards d'euros et emploie 73 000 salariés. *Thomson* est notamment détenteur avec le *Fraunhoffer Institute* des brevets du standard de codage audio MP3 (*Mpeg layer 3*). Il est également à l'origine de la proposition *SmartRight* dans le cadre de DVB-CP pour un système de protection du contenu vidéo sur le réseau domestique, à base de cartes à puce. Le groupe a également une stratégie de positionnement global sur la chaîne multimédia, afin de fournir des produits et services aux producteurs et diffuseurs, concrétisée début 2001 par le rachat de *Technicolor*, de la division «*professional broadcast* » de *Philips* et de *Grass Valley*. Cela positionne le groupe sur la filière «amont ». *Thomson* a enfin acquis fin 2002 l'entreprise *Canal+ Technologies* spécialisée dans les systèmes d'accès conditionnel pour contenus télédiffusés (décodeurs à carte à puce).

– *Hitachi*. Le groupe japonais *Hitachi* a réalisé en 2001-2002 un chiffre d'affaires de 68 milliards d'euros, dont 10 dans le domaine de l'électronique grand public. Il emploie 322 000 salariés à travers le monde. Il participe notamment au *Video Watermarking Group* et au consortium *5C*.

– ***L'industrie informatique***. Elle est principalement concernée par le matériel informatique, qui inclut notamment divers composants multimédias pour les PC ainsi que par les systèmes logiciels de lecture (*player*), de compression / décompression, et de transmission par Internet des œuvres.

– *IBM.* Le groupe *IBM* (*International Business Machines*), d'origine américaine, est un des leaders de l'informatique mondiale. Il a réalisé en 2001 un chiffre d'affaires de 95 milliards d'euros, dont 39% dans le matériel (grands systèmes, micro-ordinateurs portables, disques durs) et le reste en logiciels (à travers sa filiale *Lotus*) et services, principalement à destination des entreprises mais également dans le domaine grand public. *IBM* emploie 320 000 salariés dans le monde. *IBM* est à l'origine de plusieurs consortiums, que ce soit le *4C entity* ou « *Galaxy* », désormais intégré au *Video Watermarking Group.*

– *Intel.* Il est le leader mondial des microprocesseurs, notamment dans le domaine des micro-ordinateurs avec la série des *Pentium*, mais aussi dans le domaine des serveurs. Il détient environ 80% des parts du marché des microprocesseurs. Il a réalisé en 2001 un chiffre d'affaires de 30 milliards d'euros et emploie 85 000 salariés à travers le monde. *Intel* participe à l'initiative TCPA visant à définir une plate-forme sécurisée. *Intel* a proposé le standard HDCP (*High bandwidth Digital Copy Protection*) dans le cadre du groupe de normalisation de l'interface vidéo digitale (DVI). Il participe également aux consortiums *4C entity* et *5C entity*.

– *Toshiba.* Conglomérat japonais aux activités diversifiées, mais dont le secteur d'intervention principal concerne les micro-ordinateurs, notamment portables et les systèmes d'information, il a réalisé un chiffre d'affaires de 45 milliards d'euros sur l'exercice 2001-2002, dont 20,5 dans l'informatique, et emploie 176 000 salariés à travers le monde. *Toshiba* était à l'origine du système CSS de protection des DVD avec *Matsushita* et participe au groupe *4C entity*.

– Les éditeurs de logiciels de DRMS.

– *Microsoft*. Le leader mondial du logiciel, notamment les systèmes d'exploitation avec les versions successives de *Windows*. Il a réalisé un chiffre d'affaires de 31 milliards d'euros sur l'exercice 2001-2002 et emploie 50 000 salariés à travers le monde. *Microsoft* s'est également positionné dans le domaine multimédia avec sa solution « *Windows Media*)°, fondée sur un format propriétaire pour l'audio (WMA – *Windows Media Audio* et désormais intégrée au système d'exploitation *Windows*. Il s'agit d'une solution « client / serveur », c'est-à-dire qu'elle comprend une partie installée sur un serveur chez un diffuseur et une partie «client » installée chez l'auditeur, qui correspond à un lecteur. *Microsoft* s'est également impliqué dans l'initiative TCPA (*Trusted Computing Platform Alliance*) avec *Intel*, *IBM*, *Compaq* et *HP*, lancée en octobre 1999. Elle vise à créer une plate-forme PC comprenant des fonctions de sécurité, par exemple en adjoignant un coprocesseur cryptographique, qui devrait permettre de créer des clés cryptographiques ou de crypter la mémoire. *Microsoft* a également lancé sa propre initiative, Palladium, visant à intégrer des briques de sécurité au système d'exportation et utilisant les ressources cryptographiques de TCPA, afin de vérifier l'intégrité des programmes ou de créer un sous-système sécurisé (Nexus), etc.[(1)]

– *Real Networks* a été l'un des pionniers de la diffusion en *streaming* (flux, par opposition au téléchargement) sur Internet avec son système *Real Player* lancé en 1995. Il

[(1)] cf. aussi. 3.1.4.2.

a réalisé en 2001 un chiffre d'affaires de 210 millions d'euros. Il commercialise sa solution multi-plate-forme *Helix Universal Server* / *RealOne Player* qui inclut un *DRMS*. *Real Networks* diffuse également depuis août 2000 un bouquet payant de contenus « *GoldPass* », devenu depuis « *SuperPass* », qui compterait plus de 850 000 abonnés. Il s'est également associé à *AOL Time Warner*, *Bertelsmann* (*BMG*) et *EMI* pour lancer en décembre 2001 le service de distribution de musique en ligne *MusicNet*

– Les spécialistes de la protection technique. Il existe également quelques entreprises spécialisées sur des mesures techniques de protection ou des systèmes de protection fondées sur des technologies innovantes.

– Macrovision. Créée en 1983, entrée au *Nasdaq* en 1997, l'entreprise a réalisé en 2001 un chiffre d'affaires de 113 millions d'euros et emploie 270 personnes. Elle a trois segments d'activité : la protection contre la copie vidéo analogique(63% de son chiffre d'affaires), la protection des logiciels sur Cédérom (10%) et la gestion électronique des licences pour les logiciels (26%). Elle dispose dans ces domaines de nombreux brevets dont elle vend les licences. La protection contre la copie vidéo analogique est implantée sur les cassettes vidéo, sur les lecteurs de DVD et sur les décodeurs pour le *Pay-per-view*. Le *Digital Millenium Copyright Act* a rendu obligatoire sur les magnétoscopes le dispositif automatique de contrôle de gain (*AGC – Automatic Gain Control* qui est sensible à la protection analogique. *Macrovision* fait partie du *Video Watermarking Group* dont il gère les licences. Elle a développé avec la société *TTR Technologies* le système *SafeAudio* de protection des CD Audio. Fin 2002, *Macrovision* a acquis la société israélienne *Midbar* qui avait aussi développé le système de protection pour les CD Audio CDS (*Cactus Data Shield*), et la société *TTR Technologies*. Le système CDS avait été testé fin 2001 en Europe par *Universal Music*, *BMG Entertainment* et *Warner Music*. Il est désormais largement employé, notamment par *EMI*.

– Digimarc. La société *Digimarc*, fondée en 1996, est spécialisée dans les technologies de *watermarking* additif. Précurseur technologique dans ce domaine, elle a déposé de nombreux brevets aux États-Unis. Elle a réalisé en 2001 un chiffre d'affaires de 17 millions d'euros et emploie 338 personnes. Son activité principale concerne plutôt le secteur fiduciaire ainsi que les documents d'identification. Elle a participé à l'initiative SDMI et fait partie du *Video Watermarking Group*.

– Sunncomm Technologies. La société *Sunncomm Technologies* a été créée en 2000 et commercialisa dès 2001 une solution de protection des CD Audio nommée *MediaCloQ*, pour interdire la lecture sur PC. Une nouvelle version est sortie fin 2002, *MediaMax*, qui permet de lire sur les PC des fichiers au format *Windows Media*, sous le contrôle du système de *DRM* de cette plate-forme.

– Nextamp est une jeune entreprise française, née en 2002 d'un essaimage de *Thalès BroadCast et Multimédia* et de *Thalès Communication*. Elle a été créée sur la base d'une technologie innovante de *watermarking* différentiel en temps réel sur flux vidéo numérique compressé en Mpeg-2. Les applications envisagées concernent la traçabilité et le suivi des contenus.

Si les industriels de l'électronique grand public et l'informatique partagent le souci de développer les technologies afin d'offrir, à travers de nouveaux produits et services aux consommateurs, de nouvelles possibilités d'utiliser et donc de valoriser les œuvres, ils sont aussi concurrents dans le cadre de la convergence et leur opposition est parfois vive. Le secteur de l'électronique grand public considère ainsi le monde de l'informatique comme **moins sécurisé pour la protection des œuvres, dans la mesure où l'ordinateur**

est une plate-forme ouverte qu'un pirate peut plus facilement explorer. En réponse, l'industrie informatique souligne l'intérêt des solutions logicielles, distribuables à moindre coût et permettant de renouveler plus facilement les mesures techniques de protection en cas de piratage fatal.

1.1.1.2. Les enceintes : consortiums et normalisation.

Les mesures de protection technique, notamment demandées par les titulaires de droits américains font l'objet de deux catégories d'enceintes : les enceintes de normalisation et standardisation et les consortiums industriels généralement alliés pour répondre à des cahiers des charges spécifiques. Selon les intérêts stratégiques des différents secteurs des technologies de l'information, la participation à cette double catégorie d'enceintes manifeste en tout état de cause **une très forte mobilisation des industriels pour les protections techniques**.

i. Les enceintes de standardisation et de normalisation.

Une des contraintes essentielles de fonctionnement et de déploiement des systèmes est l'**interopérabilité** : il faut en effet que les contenus produits et distribués soient lisibles par les consommateurs, c'est-à-dire que les contenus soient stockés, distribués ou diffusés dans un format que puissent reconnaître les lecteurs vendus par différents industriels aux consommateurs. Ces formats doivent donc être partagés entre les industriels qui produisent les différents systèmes de stockage et lecture ou de diffusion et de réception. Ils sont standardisés dans les enceintes de standardisation, ce qui recouvre en fait deux types d'enceintes :

– Les organismes de normalisation.

Ce sont les organismes institutionnels de normalisation structurés autour des organismes nationaux de normalisation, comme l'**AFNOR** en France (Association Française de Normalisation)(2), ou l'**ANSI** aux États-Unis (*American National Standards Institute*)[3] qui sont regroupés en organismes régionaux (le **CEN** en Europe [4] — Comité Européen de Normalisation) et dans un organisme international, l'**ISO**- *International Standardization Organization*.[5] À côté de ces organismes généralistes existent des organismes plus spécialisés, et notamment dans le domaine de l'électricité et l'électronique, l'**IEC** au niveau international (*International Electrotechnical Commission*) [6], et son pendant européen, le **CENELEC** (Comité Européen de Normalisation Electrotechnique).[7] Dans le domaine des technologies de l'information, l'ISO et l'IEC ont fondé un groupe commun pour en débattre, dénommé **ISO/IEC/JTC1**- *Joint Technical Committee*. Ces organismes internationaux regroupent les organismes nationaux (*National Bodies*) qui sont représentés par leurs industriels qui proposent et discutent des normes.

---

(2) Afnor [http://www.afnor.fr/]
(3) ANSI [http://www.ansi.org/]
(4) CEN [http://www.cenorm.be/] et en particulier le CEN/ISSS *Information Society Standardization System* [http://www.cenorm.be/isss/]
(5) ISO [http://www.iso.ch/]
(6) *International Electrotechnical Commission* [http://www.iec.ch/]
(7) Comité Européen de Normalisation Electrotechnique [http://www.cenelec.be/]

En marge de ces organismes institutionnels existent des organismes de normalisation dont la structure est plus libre, mais qui ont pu acquérir une vraie représentativité, comme l'**ETSI** (*European Telecommunication Standardization Institute*)[8] composé d'industriels et d'administrations, notamment à l'origine de la norme GSM qui standardise également les normes élaborées par le consortium **DVB** (*Digital Video Broadcasting*, cf. *infra*).

Certains de ces groupes n'ont pas à proprement parler une activité de normalisation mais constituent plutôt des groupes de réflexion, en amont de l'activité propre de normalisation, comme le CPTWG (*Copy Protection Technical Working Group*).

– Les consortiums et les gestionnaires de licences.

Les consortiums sont des alliances d'industriels pour proposer une solution commune qu'ils cherchent à faire accepter par d'autres, afin d'en faire une norme. Ils proposent donc leur solution dans le cadre des divers appels à propositions lancés par les organismes de normalisation. Bien souvent cette solution repose sur des brevets qu'ils possèdent et qui leur permettront de tirer profit de la diffusion de leur solution.

Généralement, les consortiums confient à un organisme spécialisé la **gestion des licences des brevets sur lesquels reposent les solutions**, comme la **DVD CCA** (*DVD Copy Control Association*), le **DTLA** (*Digital Transmission Licensing Administrator*) qui gère les licences de la solution DTCP (cf. *infra*), ***4C entity***, etc. Ces organismes peuvent jouer un rôle dans la normalisation lorsque la solution qu'ils proposent est diffusée, car ils sont alors généralement responsables d'en gérer les évolutions et les extensions, comme par exemple la DVD CCA pour la protection du DVD.

De manière générale, les normes ainsi élaborées n'ont aucun caractère obligatoire. Cependant, **lorsqu'un standard est retenu par une majorité d'industriels ou par le marché, la nécessaire interopérabilité le rend de fait quasi obligatoire** : un produit qui n'est pas compatible avec la majorité des autres produits aura du mal à percer le marché, sauf s'il présente des avantages importants.

– CPTWG (*Copy Protection Technical Working Group*).[9]

Le CPTWG n'est pas à proprement parler un comité de standardisation mais un forum de discussion et de promotion, fondé en 1996 par la *MPAA*, la *RIAA* et les industries de l'informatique et de l'électronique grand public, afin de mettre en place les mesures techniques pour empêcher la contrefaçon numérique dans le contexte de l'apparition du DVD vidéo. Ce groupe commença donc par proposer en 1997 le **CSS** (*Content Scramble System*), algorithme de chiffrement du contenu des DVD vidéo, associé au RPC (*Region Playback Control*), système de contrôle du zonage des DVD. Un organisme, la **DVD CCA** (*DVD Copy Control Association*), a été spécifiquement créé pour gérer les licences du CSS auprès des fabricants.[10]

Mais déjà le groupe s'inquiétait du « trou analogique » : le signal analogique obtenu par décodage d'un signal numérique est d'excellente qualité, et rien n'empêche *a priori* de le capter sur la prise reliant le lecteur DVD (ou le décodeur de télévision numérique) à l'écran de télévision pour le re-numériser et obtenir ainsi une copie numérique, donc

---

[8] *European Telecommunication Standardization Institute* [http://www.etsi.fr/]
[9] *Copy Protection Technical Working Group* [http://www.cptwg.org/]
[10] *DVDCopy Control Association* [http://www.dvdcca.org/]

duplicable à volonté sans perte de qualité. Si le système de protection contre la copie, inventé par *Macrovision*, dérivé du système analogique APS (*Analogue Protection System*, utilisant le contrôle automatique de gain), apporte un début de solution, il est déjà contourné par des systèmes électroniques pirates, qui devraient pouvoir être transposés dans le monde numérique par des logiciels dont la distribution sur Internet sera beaucoup plus difficile à contrôler.

Le groupe a donc décidé de s'orienter vers des systèmes de « *watermarking* » pour former en mai 1997 le DHSG (*Data Hiding Sub Group*), qui lança aussitôt un appel à propositions.[(11)] Les onze propositions reçues se groupèrent pour former deux consortiums en février 1999 : la proposition ***Millenium*** portée par *Philips, Digimarc, Macrovision* et la proposition ***Galaxy***, portée par *IBM, NEC, Pioneer, Hitachi* et *Sony*.[(12)] Ensuite les deux consortiums fusionnèrent, pour former le ***Vidéo Watermarking Group*** en avril 2001. Même si la *DVD CCA* est bien consciente de la nécessité de trouver un successeur au CSS, qui a été cassé en décembre 1999 par le logiciel DeCSS puis d'autres systèmes. Elle n'a pas approuvé à ce jour le schéma proposé : la *MPAA* a accusé l'industrie informatique de bloquer le processus, mais celle-ci se défend en considérant les investissements importants à consentir et difficiles à justifier auprès des consommateurs, alors même que le système proposé ne serait pas assez robuste.

Par ailleurs, le CPTWG a également créé en octobre 1996 le DTDG (*Digital Transmission Discussion Group*), chargé d'examiner les solutions de protection du contenu sur le « réseau domestique », notamment à travers l'interface Firewire/IEEE1394, qui permet par exemple de relier un lecteur DVD ou un décodeur à un PC. Il a lancé un appel à propositions en mars 1997 pour un système garantissant l'authentification, le chiffrement et la gestion des droits de copie. Plusieurs propositions ont été reçues et certaines ont fusionné pour former **le consortium *5C***, composé *d'Intel, Toshiba, Hitachi, Sony* et *Panasonic* qui a proposé une solution baptisée DTCP (*Digital Transmission Content Protection*).[(13)]

– DVD Forum. [(14)]

Le DVD Forum est composé des acteurs principaux du DVD, au total 230 entreprises. Il a été fondé par des entreprises notamment japonaises (*Hitachi, Matsushita, Mitsubishi, Pioneer, Philips, Sony, Thomson, Time Warner, Toshiba*) pour définir les formats du DVD et travaille sur les futurs formats (DVD audio, *Blue laser* DVD, etc.). Il comprend en son sein un groupe de travail, le WG9 (*Working Group*), chargé des questions de protection contre la copie, qui a passé un accord pour participer et suivre les travaux du CPTWG, et entériner la solution de protection par *watermarking* lorsqu'elle sera acceptée par la DVD CCA.

– ISO (International Standards Organization).

Au sein de l'ISO/IEC/JTC1/SC29[(15)], deux groupes de travail s'intéressent aux questions des contenus et de leur protection :

---

(11) cf. [http://www.trl.ibm.com/projects/RightsManagement/datahiding/index_e.htm]
(12) cf. [http://www.trl.ibm.com/projects/RightsManagement/datahiding/dhvg2_e.htm]
(13) *Digital Transmission Content Protection* [http://www.dtcp.com]
(14) DVDForum [http://www.dvdforum.org/forum.shtml]
(15) ISO/IEC/JTC1/SC29
[http://www.iso.ch/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=148]

– WG1 (*Working Group 1*) — JPEG 2000 (Images fixes).[16] Ce groupe a élaboré le nouveau format pour les images fixes Jpeg 2000. La 8e partie du standard, « jpsec », concerne la sécurité et notamment l'identification et la protection des droits. En particulier il est prévu la mise en place d'étiquettes permettant d'identifier l'œuvre, l'auteur, le titulaire des droits, les droits octroyés, etc. Pour améliorer la sécurité, il est prévu d'inclure également ces données dans un tatouage. Une autorité internationale a été créée sous le contrôle de l'ISO, JURA (*Jpeg Utilities Registration Authority*), chargée d'enregistrer via les organismes nationaux de normalisation (ex : AFNOR) les autorités nationales (par exemple des sociétés de gestion collective) qui elles-mêmes enregistrent les œuvres.

– WG11 (*Working Group 11*) — MPEG (*Moving Picture Expert Group*) Le groupe MPEG a historiquement défini les standards de compression MPEG-2, utilisé pour la télévision numérique puis MPEG-4 utilisé pour la diffusion de vidéo sur Internet. La partie audio des spécifications est devenue le fameux «MP3 » (*MPEG Layer 3*). Le standard MPEG-4 intègre une partie IPMP (*Intellectual Property Management and Protection*) pour permettre une identification de l'œuvre, une gestion des droits de copie et des éléments de chiffrement du contenu et constituer un standard complet de diffusion vidéo.[17]

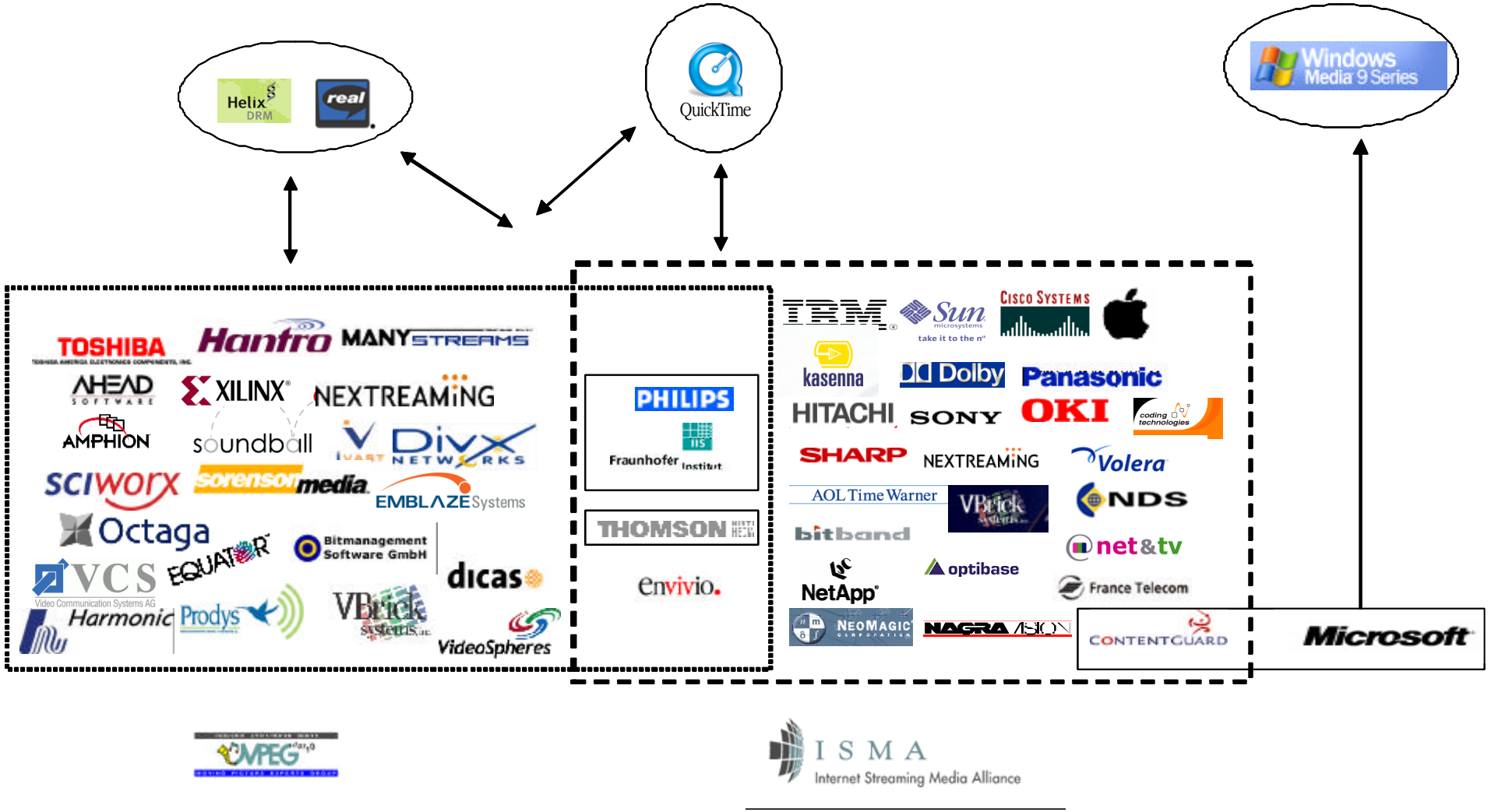
MPEG prévoit de nouveaux formats, notamment **MPEG-7** intégrant des méta-données XML (données complémentaires attachées à la vidéo qui peuvent identifier l'œuvre, décrire les droits, décrire les scènes, etc.) et **MPEG-21**, qui vise à définir une architecture multimédia globale, intégrant divers objets et contenus. **MPEG 21 comprendra notamment également un module IPMP, ainsi que RDD (*Rights Data Dictionary — Dictionnaire de droits*) et REL (*Rights Expression Language — Langage exprimant les droits*).** Le RDD vise à définir une liste organisée de termes correspondant à des droits octroyés, tout en prévoyant la possibilité de gérer des significations différentes selon la législation. Le REL vise à définir les droits octroyés, le bénéficiaire, la ressource concernée et les conditions d'application.[18]

Encadré 1.1. — Les enjeux de MPEG 4 : le marché de la lecture et de la protection vidéo.

MPEG 4 dont les travaux ont commencé en 1995 s'adresse à l'ensemble des marchés de la vidéo, c'est-à-dire non seulement le cinéma, mais aussi la télévision interactive, le multimédia, etc. notamment en vue d'utilisations sur Internet. Il s'agit principalement de normaliser un format de compression vidéo mais cela concerne aussi le transport sur IP, la description de scènes, l'interface transport/application (*Delivery Multimedia Integration Framework)* notamment pour des applications en *Narrowband*, réseau mobile, IP, TV interactive, supports DVD, etc., mais aussi, plus tardivement une interface pour la gestion des droits. [19] MPEG 4, relativement peu avancé quant à la partie IPMP fait l'objet de tensions industrielles vives quant au caractère standardisé ou propriétaire de la lecture des formats vidéo dont les enjeux économiques sont essentiels, notamment entre d'une part Apple (*Quicktime*) et *RealNetworks* qui a développé le *DRMS Helix*, autour de l'ISMA (*Internet Streaming Media Alliance*)([20]), et d'autre part, *Microsoft* (*Windows Media Player 9* avec *DRMS*).

(16) JPEG 2000 [http://www.jpeg.org/JPEG2000.htm]
(17) MPEG 4 [http://www.m4if.org/]
(18) MPEG 21 [http://mpeg.telecomitalialab.com/]
(19) MPEG4 4 Forum [http://www.m4if.org/resources/Overview.pdf]
(20) *Internet Streaming Media Alliance* [http://www.isma.tv/home]

Fig. 1.1. — La compétition des standards de compression et de lecture de la vidéo.



– DVB (*Digital Video Broadcast*).[21]

Le consortium européen DVB a été créé au début des années 1990 afin de définir le standard de la télévision numérique terrestre. Etendu à la diffusion numérique par câble et satellite, le consortium réunit près de 300 entreprises. Il a notamment défini les standards de compression et transmission numérique et d'accès conditionnel (pour les systèmes de télévision payante) aujourd'hui utilisés dans le monde entier. Le groupe DVB est segmenté selon les objectifs de standardisation par supports de diffusion : DVB-S pour la diffusion sur satellite, DVB-C pour la diffusion sur réseaux câblés, DVB-T pour la diffusion sur réseau terrestre, DVB-M/CS pour la de diffusion multipoint par micro ondes. Il comprend aussi des travaux selon les systèmes : DVB-SI pour la navigation, DVB-CA pour le système d'embrouillage, DVB-CI pour l'interface commune des systèmes de contrôle d'accès comme *Viaccess* ou *Médiaguard.* Le groupe DVB a prolongé ces standards avec, la norme MHP (*Multimedia Home Platform*) qui concerne l'interface entre les terminaux et les applications interactives ou contenus multimédias.[22]

Le consortium a ensuite défini une architecture plus globale CPCM (*Content Protection and Copy Management*) pour gérer la circulation du contenu au-delà du système d'accès conditionnel, dans le réseau domestique et les magnétoscopes à disque dur (PVR — *Personnal Video Recorder*). Le groupe de travail DVB-CP (*Copy Protection*) a défini les besoins à couvrir par le système et confié à un groupe technique CPT (*Copy Protection Technical*) le soin de lancer un appel à proposition mi-2001, qui a reçu 24 propositions, dont l'une des plus sérieuses est celle du consortium *SmartRight.*

– SDMI (*Secure Digital Music Initiative*). [23]

La SDMI a été créée en 1998 par la RIAA (*Record Industry Association of America*), RIAJ (*Record Industry Association of Japan*) et IFPI (*International Federation of Phonographic Industry*), pour trouver une réponse technique au développement de la contrefaçon numérique notamment sur Internet. Son objet était de proposer une solution applicable aux nouveaux matériels, qui bloquerait la lecture d'œuvres musicales transmises par Internet sous un format compressé (car la compression MP3 modifie les données). Afin de tester la robustesse de ses propositions qui reposaient principalement sur le *watermarking*, la SDMI a organisé un concours auprès de la communauté scientifique, qui a malheureusement montré la faible robustesse des propositions.

– DVI *(Digital Vidéo Interface).* [24]

Le groupe de normalisation de l'interface vidéo numérique DVI a accepté un standard de protection de copie HDCP (*High-bandwidth Digital Content Protection*) proposé par *Intel.* Ce groupe est cependant très spécialisé et l'interface vidéo est pour l'instant peu répandue. De nombreuses autres enceintes existent, souvent très spécialisées sur un composant (par exemple l'enceinte ATA (*AT Attachment*), spécialisée sur les systèmes de stockage, notamment disques durs) ou sur une liaison entre deux composants, mais bien souvent ces approches souffrent d'une absence de prise en compte globale du système : comme il faut ensuite juxtaposer divers composants avec divers liens entre eux, il peut devenir très difficile de gérer globalement les droits sur un contenu.

---

(21) DVB [http://www.dvb.org/]
(22) MHP (*Multimedia Home Platform*) [http://www.mhp.org/]
(23) SDMI [http://www.sdmi.org/]
(24) HDCP [http://www.digital-cp.com/]

1.1.2. LES TITULAIRES DE DROITS.

Dans une logique économique, seule la titularité de droits exclusifs appelant des remontées de rémunération, autant que possible proportionnelles, et donc fondées historiquement sur la reproduction – numérique, en l'état des techniques et à proportion du déclin des valeurs commerciales et d'usage des techniques analogiques – peut justifier l'intérêt d'acteurs économiques culturels pour la mise en œuvre de mesures techniques de protection de ces droits.[25]

Par conséquent, quant aux droits de propriété littéraire et artistique qui sont aussi des titres de propriétés de valeur présente et future, l'essentiel du positionnement des acteurs de l'économie numérique des contenus s'ordonnance en fonction des conditions qui stabilisent d'abord, garantissent ensuite, puis accroissent ou permettent d'accroître les bénéfices de la détention de droits exclusifs.

Selon la même logique économique, ces bénéfices peuvent prendre deux formes qui sont autant de critères en faveur ou en défaveur d'investissements destinés à la mise en œuvre de mesures techniques de protection ; la sécurité des rémunérations présentes et futures, la quantité présente et future de droits à rémunération.

1.1.2.1. Les critères structurels face aux choix de mesures techniques.

Dans une perspective économique, c'est-à-dire de rationalisation des choix d'investissements en faveur ou non de mesures techniques, le positionnement des acteurs économiques culturels dépend de trois critères principaux :

– La lutte contre la contrefaçon. L'ensemble des titulaires de droit a un intérêt éminent à la limitation de l'ensemble des reproductions numériques qui ne sont pas licitées. À cet égard, il n'y a aucune distinction à opérer entre les catégories de titulaires de droits exclusifs, qu'il s'agisse du droit des auteurs, des droits voisins des producteurs, des artistes et interprètes et des radiodiffuseurs. **La contrefaçon numérique représente pour toutes ces catégories un manque à gagner**, quelle que soit la part, jamais nulle, effectivement substituable à la vente des reproductions numériques contrefaites. Dans l'environnement numérique, **les usages illicites — à des fins de contrefaçon — des réseaux d'échange pair à pair constituent, d'un point de vue économique, sinon une « trappe », du moins une forme de concurrence déloyale particulièrement puissante à l'égard de toute offre licite de contenus numérique**.

Les effets déstabilisateurs de ces usages portent notamment sur la distribution, c'est-à-dire en réalité, dans l'univers numérique sur la remontée de rémunération des droits, qui varie en fonction de la gestion de la cession des droits d'exploitation des œuvres. **Face à la contrefaçon numérique (les usages illicites des réseaux pair à pair**

---

[25] L'objet principal de l'étude étant de percevoir les enjeux industriels – dont le développement – des mesures techniques, les analyses qui succèdent sont nécessairement très synthétiques. Elles sont fondées, au-delà des consultations et des travaux du CSPLA, notamment sur ceux réalisés par la Commission européenne — Direction générale Société de l'Information [http://europa.eu.int/information_society/topics/multi/digital_rights/events/index_en.htm] ; et des *Hearings* réalisées par les Sous Comités du Congrès américain à l'occasion de l'adoption du DMCA ou ultérieurement [http://judiciary.senate.gov/special/feature.cfm ; , etc.] ainsi que dans le cadre de la procédure de *Rulemaking* du *Copyright Office*. [http://www.loc.gov/copyright/] ; mais encore un certain nombre de colloques [http://www.digital-rights-management.de/ ; http://www.w3.org/2000/12/drm-ws/minutes; etc.]

étant postérieurs au droit des mesures techniques), il est de l'intérêt de l'ensemble des titulaires de droits d'investir en faveur de mesures techniques de protection contre la contrefaçon. Un intérêt parallèle à un tel investissement porte sur les mesures techniques de gestion des droits qui favorisent la licitation des droits, une plus large diffusion des œuvres et une meilleure exploitation de ceux-ci.

– Un critère juridique distinctif quant à la gestion de la cession des droits. Il explique les **différences d'intensité d'intérêts** des titulaires de droits exclusifs en faveur des mesures techniques, alors même que chacune d'entre elles représente des titulaires qui disposent de manière exclusive du droit d'autoriser ou d'interdire la reproduction de l'œuvre. **Ce critère dépend de deux facteurs** :

– à titre originaire, des principes généraux du droit de propriété littéraire et artistique qui définissent le régime de dévolution et de cession des droits. Deux modèles dominent ces régimes : le régime de ***copyright*** qui favorise une dévolution et cession des droits en faveur de l'exploitant (producteur, éditeur, voire diffuseur) ; **le modèle de droit européen** qui tend à maintenir sur la tête du titulaire la jouissance des droits et conduit à des logiques à la fois plus contractuelles et concurrentielles entre les catégories de titulaires. Dans ce cadre, **l'intensité d'intérêt pour la protection juridique des mesures techniques de protection des droits suit la dévolution et la cession des droits**. Mais quel que soit le modèle de droit, elle est toujours la plus forte du côté des exploitants (producteurs, éditeurs voire diffuseurs) que du côté des auteurs et des artistes et interprètes. C'est notamment pourquoi, l'essentiel des enjeux relatifs aux mesures techniques est déterminé aux États-Unis.

Encadré 1.2. — La représentation des producteurs.

La MPAA (*Motion Picture Association of America*).[26] Elle regroupe les *majors*, soit : *Walt Disney Company*, *Sony Pictures Entertainment*, *Metro-Goldwyn-Mayer*, *Paramount Pictures*, *Twentieth Century Fox Film*, *Universal Studios*, *Warner Bros.*, mais aussi l'ensemble de la filière cinématographique et de production audiovisuelle américaine.

La RIAA (*Recording Industry of America Association*) [27] Elle regroupe près de 500 entreprises de production de phonogrammes aux États-Unis, dont notamment les *majors*, soit un chiffre d'affaire total de 15 Mds US$. **L'IFPI** (*International Federation of the Phonographic Industry*)[28] regroupe les fédérations nationales de producteurs de phonogrammes dans le monde. **La représentation nationale des producteurs de phonogrammes** est assurée par le SNEP (*Syndicat National de l'Edition Phonographique*) [29].

– à titre institutionnel, du mode de gestion des droits. **L'intensité de l'intérêt pour les mesures techniques apparaît structurellement plus élevée dans le cadre de mode gestion collective des droits**, notamment en raison des relations contractuelles et/ou concurrentielles entre les catégories de titulaires. **Cet effet pourrait cependant contrebalancer en fonction de l'importance de la gestion individuelle des droits**, car en principe, une mesure de protection technique, et surtout un Système numérique de gestion des droits, est neutre par rapport au gestionnaire des droits, par conséquent, dans une logique de commerce électronique, les offres de Systèmes numérique de gestion de droits pourraient être défavorables au mode de gestion collective. En

[26] MPAA [http://www.mpaa.org/]
[27] RIAA [http://www.riaa.org/index.cfm]
[28] IFPI [http://www.ifpi.org/]
[29] SNEP [http://www.disqueenfrance.com/default.asp]

pratique, il apparaît plutôt que tant pour l'élaboration de la description normalisée du régime de l'information sur les droits que pour les investissements nécessaires à la gestion numérique des droits, et plus encore pour l'accès au répertoire, ce mode de gestion peut apparaître comme une « facilité » pour des produits de *DRMS* en concurrence.

Le jeu de ce double facteur est déterminant d'une part quant à la distinction d'intérêt pour les mesures techniques, ou simplement d'appropriation du sujet entre les États-Unis et l'Europe, d'autre part, et plus particulièrement en ce qui concerne l'exercice effectif du droit exclusif des artistes et interprètes d'autoriser ou d'interdire la reproduction.

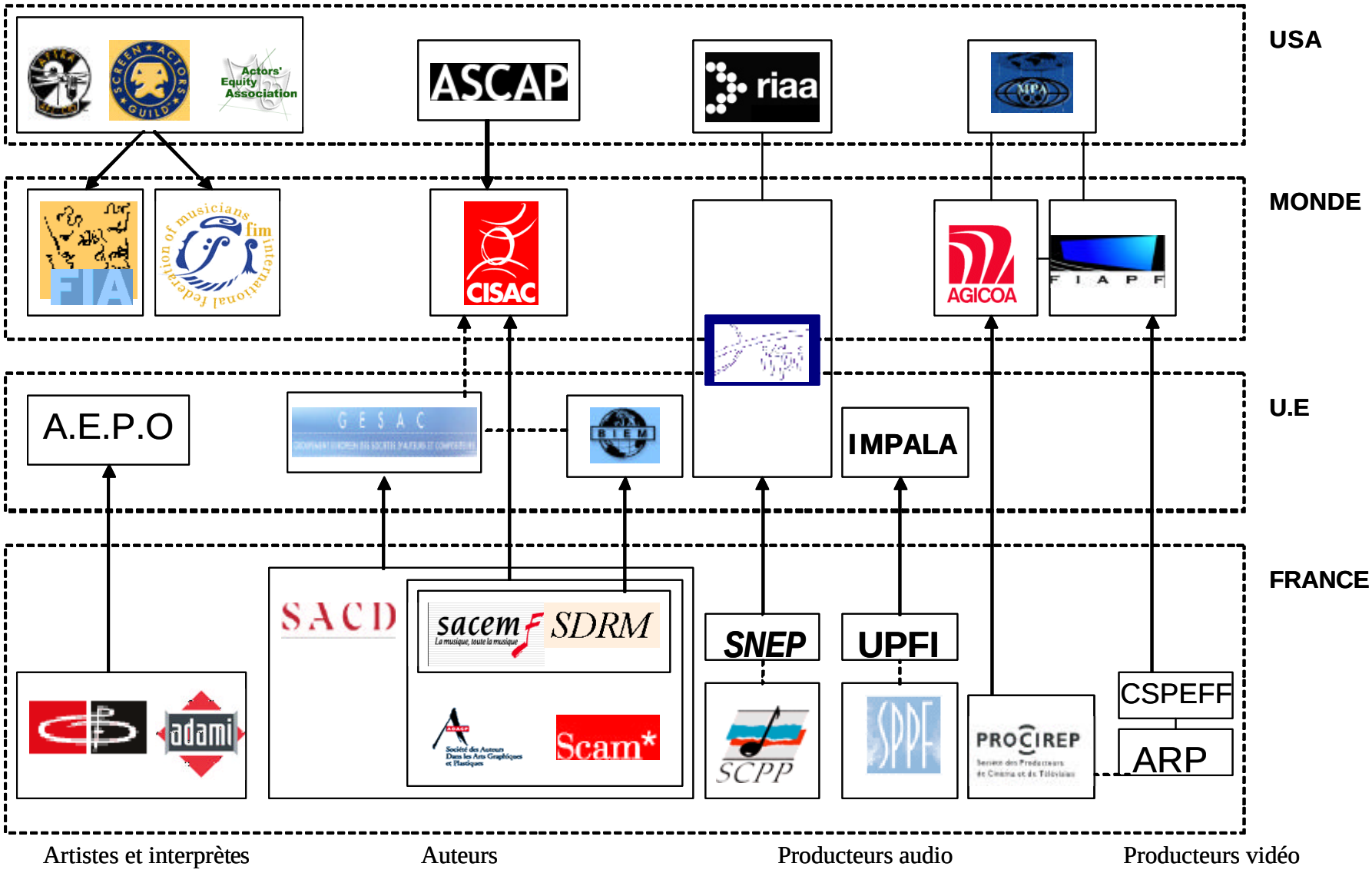
Encadré 1.3. — La représentation des auteurs et des artistes et interprètes [30]

La représentation des auteurs est assurée au plan international par la **CISAC** (Confédération Internationale des Auteurs Compositeurs). Elle regroupe des sociétés d'auteurs de l'ensemble du monde. Elle a notamment travaillé à la réalisation de la normalisation des œuvres : musicales avec l'ISWC (*International Standard Musical Works Code*), audiovisuelles avec l'ISAN (*International Standard Audiovisuel Number*), textuelles avec l'ISTC (*International Standard Text Code*) pour la gestion numérique des droits des auteurs. **Au plan communautaire, le GESAC** (Groupement européen de sociétés d'auteurs compositeurs), créé en 1990 regroupe 25 sociétés d'auteurs de l'Union européenne, de Suisse et Norvège. **Au plan national**, trois sociétés de perception et de répartition des droits des auteurs assurent principalement la représentation de leurs intérêts pour les secteurs de la musique et de l'image. Pour les auteurs de musique, la **SACEM** ; pour les auteurs audiovisuels la **SACD**, pour les auteurs multimédias, la **SCAM**. Une association, l'ARP (Association des Réalisateurs Producteurs) regroupe pour sa part des auteurs réalisateurs et des producteurs cinématographiques. La représentation de ces intérêts et de ceux des producteurs et des éditeurs a été fédérée et étendue à d'autres acteurs (édition, arts plastiques, etc.) pour les questions nationales relatives aux technologies de l'information au sein du Comité de liaisons des industries culturelles (CLIC).

La représentation des artistes et interprètes est assurée au plan international par deux associations représentent les artistes interprètes la **FIM** (*Federation Internationa of Musicians*) qui regroupe 65 organisations nationales et la **FIA** (*Fédération Internationale des Acteurs*) qui regroupe 100 organisations représentatives des acteurs, danseurs, etc. pour 70 pays. **Aux États-Unis**, **l'ASCAP** (*The American Society of Composers, Authors and Publishers*). réalise la représentation la plus vaste de l'ensemble des catégories d'auteurs, d'artistes et d'interprètes, soit les auteurs, chanteurs, musiciens, etc. ; l'AFTRA (*The American Federation of Television and Radio Artists*) représente les artistes de l'audiovisuel ; la SGA (*Screen Actors Guild*) représente pour sa part les comédiens du cinéma. et l'*Actors' Equity Association* assure la représentation en particulier des artistes dramatiques. **Au plan National**, principalement deux sociétés de perception et de répartition des droits des artistes et interprètes assurent une représentation de cette catégorie de titulaires de droits : **l'ADAMI** et la **SPEDIDAM**.

[30] CISAC [http://www.cisac.org] ; GESAC [http://www.gesac.org/fr/gesac/default.htm] ; SACEM [http://www.sacem.fr/] ; SACD [http://www.sacd.fr/] ; SCAM [http://www.scam.fr/] ; FIM [http://www.fim-musicians.com/Datas/FR/GeneralFrame.html] ; FIA [http://www.fia-actors.com/fra/aboupage.htm] ; ASCAP [http://www.ascap.com/] ; AFTRA [http://www.aftra.org/] ; SGA [http://www.sag.org/] ; *Actors' Equity Association* [http://www.actorsequity.org/home.html] ; ADAMI [http://www.adami.org/] ; SPEDIDAM [http://www.spedidam.fr/index.htm].

Fig 1.2. — La représentation des titulaires de droits.



1.1.2.2. Une distinction sectorielle : audio et vidéo.

Cette distinction explique les différences d'intensité d'intérêt en faveur des mesures techniques selon le rapport des coûts de production des œuvres de chaque secteur, mais aussi des recettes potentielles. Elle tient compte du cycle d'exploitation, en particulier pour le cinéma et l'audiovisuel à travers le contrôle des durées intermédiaires d'exploitation (chronologie des médias) et des territoires d'exploitation.

– Le secteur de la production de cinéma a un rôle dominant. La valeur économique des œuvres cinématographiques, en simple raison des **coûts de production** et des recettes attendues pour chaque œuvre, mais surtout du **poids industriel** de cette économie, notamment aux États-Unis, à laquelle s'ajoute la production audiovisuelle, lui confère ce rôle. En second lieu, les œuvres cinématographiques et audiovisuelles constituent le segment de marché, pas seulement pour les appareils de lecture (décodeurs et écrans) qui n'est sans doute pas le plus rentable, qui représente la plus **forte valeur ajoutée pour les industries de l'électronique grand public**. Il joue virtuellement un rôle analogue d'attraction pour les secteurs des télécommunications et de l'informatique personnelle.

Il a assis et entretenu ce rôle sur un contrôle des espaces-temps d'exploitation : chronologie (salles, vidéo, TV payante, TV en clair, Internet), mais aussi sorties différées dans l'espace avec chronologie subséquente, zonage des DVD. Les mesures techniques que ce secteur a toujours établies avant tout autre, résultent de ce rôle (cf. infra ; exemple du DVD). Elles configurent techniquement le contrôle d'exploitation propre à l'économie de ces œuvres.

Le secteur du cinéma notamment américain, pour des raisons tenant à son importance symbolique stratégique, mais surtout de son poids économique, de son régime juridique relatif aux droits et des formes d'exploitation dans le temps et l'espace, de son attrait pour l'ensemble des industries numériques du secteur des technologies de l'information et de la communication, y compris des infrastructures de télécommunications, est donc au centre de la question des mesures techniques.

Il fait porter aujourd'hui l'essentiel des enjeux, moins sur la copie privée numérique (essentiellement réglée par la protection du DVD) que sur la liaison entre ,d'une part, l'univers de l'électronique grand public, notamment les réseaux privés domestiques ou personnels, objet d'une sécurité forte et faiblement ouverts, et d'autre part, l'univers de l'informatique personnelle, en amont sur les réseaux de télécommunications pour le débit et l'abonnement, en aval sur les éditeurs de logiciels de lecture et les systèmes d'exploitation, y compris les consoles de jeux. [(31)]

– Le secteur des phonogrammes joue un rôle pionnier mais sous contraintes. Outre les différences signalées par rapport au cinéma en termes de coûts de production par œuvre et de durée d'exploitation des œuvres, la production de phonogrammes semble

---

[(31)] Le secteur des jeux vidéos, notamment dans une approche de moyen terme, peut jouer un rôle analogue que celui du cinéma. Mais outre des raisons sociologiques (starification sur modèle occidental, dimension culturelle, mode de consommations, etc.), la similarité des économies (rapport création/industrie, coûts de production, structure des acteurs industriels convergence des techniques, etc.) voire esthétiques (interpénétration des imaginaires), économiquement, la durée de vie des produits de ces deux industries, ne fait probablement de cette concurrence qu'une apparence. (cf. : A. Le Diberder, *La création de jeux vidéos*, Département des Études et de la Prospective, Ministère de la culture et de la communication, avril 2002).

soumise à des contraintes économiques, industrielles et techniques, alors que l'analogie domine quant aux conditions juridiques.

Cette situation lui fait jouer un rôle plus limité à l'égard des mesures techniques, en fonction de quatre facteurs principaux :

– Le relatif éclatement industriel du secteur. Internationalement, à la différence du secteur cinématographique très largement concentré aux États-Unis, la situation est un peu moins nette quant au secteur de la production de phonogrammes. Économiquement et industriellement, cette situation s'accroît et limite la convergence d'intérêt avec les principales industries de l'électronique grand public, de l'informatique et des télécommunications. Cette situation peut par exemple s'illustrer à l'égard de la contrefaçon de musique.

– La multiplicité et la concurrence de couples distribution/rémunération. L'industrie musicale, à la différence de l'industrie cinématographique, repose sur une double forme de remontée de recettes d'exploitation des droits – le droit exclusif – et la licence légale, généralement instituée par les législateurs en fonction de l'état des techniques (radiodiffusion) et appelée à une gestion collective des droits. Dans ces conditions, l'analyse des choix relatifs à l'implémentation des mesures de protection technique des œuvres numériques, y compris de la copie privée numérique, se pose dans des conditions très spécifiques.

– Les conditions de choix de sécurisation des contenus numériques musicaux sont plus délicates, puisqu'elles dépendent de :

– la capacité d'instituer une chronologie de la diffusion de musique , selon les supports, sachant que la diffusion radio et audiovisuelle est des modes alternatifs de consommation des œuvres permettant des reproductions numériques (dans certaines conditions) et en tout cas de re-numérisation aisée, ce qui avant la généralisation de nouveaux formats (SACD, DVD Audio) ne produit pas de différence manifeste ;

– la capacité de sécuriser parallèlement l'ensemble des modes de distribution numérique (supports optiques, radiodiffusion, réseaux de télécommunications) ;

– la capacité d'établir un régime de droits exclusifs sur l'ensemble des modes de distribution d'œuvres musicales numériques – et non de licence légale. Or, juridiquement est reconnu au sein de l'Union européenne, un régime de licence légale pour le *simulcasting*, tandis que demeure en débat le régime juridique applicable aux services de *webcasting* et surtout les services « quasi à la demande ». Par comparaison, une solution de licence légale a été établie aux États-Unis pour le *webcasting*, sans doute plus aisément, mais dans la mesure évidemment où aucune rémunération n'était jusqu'alors prévue. Le même type de question pourrait s'étendre à la distribution musicale par les nouvelles générations de téléphonie mobile, sécurisée ou non ;[(32)]

[(32)] La distribution par les réseaux de télécommunications pour la téléphonie mobile des prochaines générations (GPRS, EDGE, UMTS) peut sans doute se réaliser dans un environnement sécurisé par des DRMS. Toutefois, la prise en compte des coûts n'implique pas nécessairement ce type de déploiement.

– de l'accord des autres titulaires de droits exclusifs sur des œuvres musicales ou des résultats de leurs concurrences réciproques. Sont en jeu en Europe le sort des accords *BIEM-IFIPI*, respectivement entre les auteurs et les producteurs de phonogrammes, mais aussi le renouvellement de l'ensemble des accords contractuels entre les artistes interprètes et les producteurs de phonogrammes pour les « *exploitations Internet* ». Est enfin en jeu en Europe, la comparaison des bénéfices présents et futurs de chacune des catégories de titulaires de droits, selon que la rémunération est forfaitaire ou proportionnelle, pour chaque catégorie d'exploitation, y compris la copie privée numérique.

Des réponses apportées à chacune et la totalité de ces questions dépendent évidemment le degré de concentration du secteur de la production de phonogrammes, donc de la place des producteurs indépendants, de l'intégration / ou concurrence entre les services musicaux à la demande – pertinente ou non – de l'industrie de production de phonogrammes (plates formes de distribution en ligne) et de la distribution de supports physiques de contenus numériques musicaux, de la différence d'offre commerciale, y compris de copie, entre ces modes de distribution, etc.

– la pesanteur de choix techniques devanciers mais antérieurs. Elle résulte majoritairement des questions et critères précédents. La complexité des enjeux juridiques, économiques, techniques et commerciaux de la distribution d'œuvres musicales n'a pas eu tendance à favoriser une logique de sécurité d'œuvres à la durée de vie aléatoire. Les formats de supports physiques numériques, devant entrer presque immédiatement en concurrence (et soutien commercial) avec les autres modes de distribution des œuvres, notamment la radio et la télévision.

Dans ces conditions, l'absence de sécurité native du CD Audio est un choix quasi contraint, en dépit du rôle de pionnier de l'industrie des phonogrammes dans l'univers numérique. Cette absence de sécurité, révélée par contraste avec le DVD du fait des risques de contrefaçon accrus par l'émergence – postérieure - des réseaux numériques ouverts constitue sans doute un risque économique permanent sur cette industrie, mais ne détermine pas de manière certaine son intérêt durable pour la sécurisation des contenus numériques. En effet Le rôle de devancier du secteur de l'industrie de phonogrammes n'est pas neutre quant à l'avenir des mesures techniques de protection. Sans doute lui fait-il courir un niveau élevé de risques économiques et le conduit-il à jouer un rôle déterminant en faveur des mesures techniques. Toutefois, compte tenu des facteurs précédents et notamment du facteur relatif aux calculs d'exploitation de la durée de vie des œuvres assez ouvert ou incertain, l'industrie des phonogrammes est face à **l'alternative stratégique suivante** :

– soit, suivre le modèle du secteur cinématographique en faveur de mesures techniques efficaces et inventer des modèles d'exploitation intensive des capitaux de droits dans une économie durable protégée techniquement et juridiquement, et ainsi prolonger des « tests » de services à la demande, y compris de copie privée en mode d'exploitation « normale » ;

– soit, laisser se développer des modes de distribution – partiellement – non sécurisé quitte à faire évoluer les modèles économiques et le régime des droits y afférents, notamment en raison du jeu des facteurs propres à ce secteur et notamment à la concurrence des autres modes de distribution – à terme tous numériques.

Sous ce jour, **l'industrie des phonogrammes est en réalité dans une phase « test » de ses modèles économiques numériques** ; ils portent sur :

– la constitution de plates-formes de distribution comme *Pressplay* ou *MusicNet*, aux États-Unis, *eCompil* en France, donc d'abord à catalogue fermé, en réalité multi-catalogue ;

– la concentration de la distribution par les producteurs eux-mêmes, selon les exemples précédents, ou l'accès aux catalogues à d'autres plates-formes ;

– l'économie du *P2P*, comme a cherché à la développer l'accord — fusion entre *BMG* et *Napster*, ou peuvent le faire des produits d'appel sur ces réseaux ;

– « l'efficacité » de mesures techniques, fragiles en raison de la norme CD et leur réception par le public ;

- **l'intérêt économique et commercial à une «exploitation normale » du droit exclusif en ce qui concerne la copie privée : la grande majorité des services à la demande proposent des offres de « *burning* »** (gravage) **;**

– etc.

L'évolution de l'intérêt en faveur des mesures techniques de protection et de l'établissement de régimes différenciés de copie privée, par secteur, ou par implémentation des techniques résultera des résultats de cette période de test. **L'intérêt des mesures techniques pour le secteur des phonogrammes dépend naturellement aussi de l'avancement de la radio numérique**.

* * *

Dans ces conditions complexes qui mettent en jeu des intérêts très divers et reposent sur un ensemble de conditions qui ne l'est pas moins, il ressort surtout que la relation des titulaires de droits exclusifs aux mesures techniques – au moins en France — tient hiérarchiquement à la résolution des principales données :

– poids des intérêts potentiellement assez convergents des acteurs américains face aux intérêts potentiellement plus divergents en Europe ;

– validité des différents écarts de relations entre mesures techniques et selon les secteurs de la vidéo et de l'audio ;

– capacité d'autonomie d'expression d'intérêts différents à l'égard des mesures techniques de catégories de titulaires de droits exclusifs.

* * *
*

1.2. ENJEUX DES MESURES TECHNIQUES.

Le déploiement des mesures techniques de protection et de la protection juridique de celles-ci, à savoir la prohibition des activités de contournement que prévoit la directive 2001/29 porte des enjeux non seulement quant à l'économie de la société de l'information, et particulièrement des industries culturelles, mais aussi des enjeux d'usages et de libertés pour les utilisateurs. Les enjeux en cause sont surtout de nature industrielle et résultent souvent de choix qui ont lieu aux États-Unis. Ils sont en tout état de cause, juridiques et concernent notamment la question de la copie privée dans l'environnement numérique et ses modalités de dédommagement.

1.2.1. ENJEUX POUR LA SOCIETE DE L'INFORMATION.

La naissance du *Compact Disc Digital Audio*, au début des années quatre-vingt, a marqué le commencement de l'ère « numérique ». Si la problématique de la copie existait déjà dans le monde analogique, avec l'arrivée des cassettes audio compactes dans les années soixante puis du magnétoscope dans les années soixante-dix, elle prenait une tournure nouvelle dans le monde numérique, avec la possibilité de copier sans perte de qualité. Dès l'arrivée des premiers systèmes d'enregistrement numérique, les industriels et les titulaires de droits se sont penchés sur la question des systèmes techniques de protection de la propriété intellectuelle, à travers des systèmes de protection contre la copie.

À la première « révolution numérique » a succédé une seconde révolution au cours des années quatre-vingt-dix : celle de la « société de l'information », qui correspond au développement **conjoint de l'informatique et des communications**, et plus particulièrement en ce qui concerne les contenus, la diffusion de l'ordinateur multimédia et le développement d'Internet et des réseaux *peer to peer*. Ce nouveau contexte engendrait de nouveaux enjeux, tant en terme d'opportunités, avec les nouvelles possibilités d'exploitation offertes, qu'en terme de risques, avec le développement d'une forme nouvelle de contrefaçon, plus diffus et à but non lucratif (ou indirectement), qui diffuse gratuitement les contenus contrefaits.

1.2.1.1. La société de l'information.

Le développement de la société de l'information s'accompagne de très intéressantes perspectives sur le plan économique et sociologique. De manière générale, pour les entreprises, l'amélioration de la gestion de l'information et des échanges engendre les gains de productivité nécessaires à l'amélioration de leur compétitivité et à l'augmentation des revenus qu'elles distribuent tant à leurs actionnaires qu'à leurs salariés. Pour les particuliers, la société de l'information apporte de nouvelles perspectives de consommation, que ce soit dans le domaine des communications enrichies, de l'autoproduction (photos ou caméscope numérique) ou des contenus.

Dans le domaine particulier des contenus, le développement de la société de l'information apporte de **nouveaux outils de lecture** (le *juke-box* personnel sur ordinateur ou sur baladeur MP3), de **nouveaux canaux de promotion ou de distribution licite des contenus** (services d'achat en ligne de contenus), donc de nouvelles activités économiques, au profit des consommateurs et des acteurs économiques, industriels, distributeurs et titulaires de droits.

Mais le développement de la société de l'information, malgré ces aspects positifs, s'est également accompagné du développement de la contrefaçon à un niveau inquiétant et dans une forme nouvelle. Jusqu'alors en effet, la consommation «à la maison» de musique et de vidéo (au sens large, c'est-à-dire télévision, cinéma, cassettes vidéo) relevait exclusivement du domaine de **l'électronique grand public, à travers des appareils dédiés, fermés, que le consommateur ordinaire ne modifiait pas lui-même**. La contrefaçon relevait alors de structures organisées, à travers des échoppes qui, soit vendaient des supports optiques pirates (CD Audio – DVD), soit vendaient des systèmes dédiés ou des appareils modifiés (ou modifiaient sur place les appareils standards), nécessitant des moyens matériels parfois significatifs.

i. L'ordinateur, un système ouvert.

L'ordinateur multimédia, s'il permet d'offrir un nouveau support de consommation et donc de valorisation des contenus, s'il présente l'intérêt d'être multifonctionnel, apporte également le **risque inhérent à un système ouvert**. Alors que dans le domaine de l'électronique, les traitements de données sont effectués par des composants électroniques qui sont difficiles à explorer ou à modifier, dans un ordinateur les systèmes de lecture ou d'enregistrement n'effectuent pas ou peu de traitements de données et s'appuient pour cela sur le processeur, qui concentre l'intelligence du traitement codé dans un logiciel. Cela permet d'obtenir des systèmes à moindre coût, par exemple un lecteur DVD d'ordinateur n'intègre pas de composant électronique pour le déchiffrement et la décompression, cette fonction étant assurée par le processeur. En revanche, **il est possible d'explorer, d'analyser voire de modifier le logiciel** (donc le traitement) sans moyens matériels particuliers, même si cela peut être coûteux en temps.

Les premiers systèmes de protection contre la copie se fondaient sur l'insertion de quelques bits indiquant si la copie était autorisée ou pas et reconnus par les systèmes d'enregistrement (exemple simple : un *bit* valant 1 si la copie est autorisée, 0 sinon). Si ces systèmes étaient efficaces dans le domaine de l'électronique, il devenait très facile de modifier ces informations avec un ordinateur. Même des systèmes plus sophistiqués, comme l'algorithme CSS, pouvaient être explorés, afin de découvrir l'algorithme et les clefs de chiffrement : ainsi, il semblerait que le système de protection CSS ait été « cassé » à partir d'un logiciel agréé de lecture de DVD sur ordinateur.

Si l'ordinateur multimédia et l'Internet sont de nouveaux outils qui permettent de développer la consommation licite de musique et de vidéo, ils permettent également une nouvelle forme de contrefaçon, qui n'est plus le fait de structures organisées mais, à travers les réseaux *peer to peer*, des consommateurs eux-mêmes, sans but lucratif, dans un système totalement dématérialisé et de manière beaucoup plus diffuse, donc beaucoup plus difficile à maîtriser pour ces trois raisons.

ii. L'explosion des capacités de stockage.

Les progrès rapides de la technologie ont également entraîné une croissance rapide des capacités de stockage. Ainsi, dans le domaine de la mémoire vive (stockage sur une puce électronique), la capacité nominale est aujourd'hui de l'ordre de 128 Mo (millions d'octets) avec une croissance exponentielle définie par la **loi de Moore** qui conduit cette capacité à doubler tous les 12 à 18 mois. Dans le domaine des disques durs, la capacité moyenne est de l'ordre de 80 Go (milliards d'octets), avec une croissance exponentielle encore plus rapide, qui voit cette capacité doubler environ tous les ans. Enfin dans le domaine des supports optiques, les CD-R peuvent contenir 800 Mo, les DVD-R à simple

face, simple couche 4,7 Go et les futurs DVD « *blue ray* » devraient pouvoir contenir 50 Go. La progression est moins régulière mais elle est également exponentielle.

Néanmoins la progression exponentielle des capacités de stockage, dans un contexte de relative stabilité des prix de ces supports d'enregistrements, pourrait conduire la **rémunération pour copie privée, si elle reste calculée sur une base forfaitaire en fonction de la durée d'enregistrement, à représenter une part majoritaire du prix global des supports de stockage** sur lesquels elle s'applique. Des révisions très régulières ont sans doute à être établies, d'autant qu'au caractère exponentiel des capacités de stockage s'ajoutent **les progrès de la compression numérique** .

iii. Internet et les réseaux.

Les nouveaux réseaux et Internet en particulier apportent la faculté de diffuser rapidement et à faible coût des contenus dans le monde entier. La diffusion des contenus est déjà et sera très certainement l'un des moteurs du développement des usages à haut débit. Des systèmes de connexion par le réseau téléphonique commuté (RTC), qui permettaient des débits de 32 à 56 kbps (milliers de bits par seconde), les internautes passent progressivement aux connexions câble ou ADSL qui permettent une **connexion permanente, de 128 à 1024 kbps** , voire plus lorsque les opérateurs mettront en place de nouvelles offres. À cette capacité, le téléchargement d'une œuvre musicale de 4 minutes au format MP3 prend moins d'une minute et le téléchargement d'un film prend 7 heures en MPEG-2 (ce temps devrait être réduit de 2/3 par le futur standard de compression MPEG-4 part 10, soit presque du temps réel).

Cette technologie bouleverse de manière fondamentale l'économie des biens immatériels (œuvres, logiciels…) qui peuvent transiter sur les réseaux, à travers plusieurs aspects :

– Les coûts de diffusion par Internet sont très faibles, par exemple par rapport à un système de diffusion par support optique (CD Audio). Force est cependant de constater que les contrefacteurs ont profité de cette évolution plus rapidement que les titulaires de droits et les distributeurs, même si ces derniers commencent à mettre en place des services de distribution par Internet ;

– La couverture internationale crée une forme d'unité de temps mondiale , qui met en difficulté le système du « zonage » des DVD. Ce modèle économique crée une opportunité importante pour la contrefaçon dans les zones de distribution tardive et pourrait menacer l'ensemble de la chronologie des médias depuis la diffusion en salles, dans la mesure il devient possible de diffuser des copies contrefaisantes, dématérialisées d'un DVD avant la sortie en salles dans les zones de distribution tardive ;

– Le développement du commerce électronique peut également permettre la « **désintermédiation** », en permettant la relation directe des producteurs aux consommateurs, comme *PressPlay* et *MusicNet* ou même des artistes aux consommateurs. Ceci est cependant à prendre avec la plus grande prudence et dépend évidemment du poids respectif des acteurs et des diverses filières de distribution, puisque dans ce cadre les fournisseurs se mettent en concurrence avec les intermédiaires qui sont leurs clients, ce qui peut pousser ces derniers à des mesures de rétorsion.

Cette évolution technologique devrait conduire à une évolution du modèle économique de la distribution des œuvres, afin de profiter des nouvelles opportunités ainsi offertes pour améliorer l'équilibre entre la distribution légale et la distribution contrefaisante.

1.1.1.2. Nouveaux usages et nouvelle contrefaçon.

Les développements des industries numériques ont créé auprès des utilisateurs une grande liberté d'accès aux œuvres, y compris de reproduction, mais aussi de distribution. Une telle évolution s'est accompagnée ensuite de l'attrait pour les réseaux *peer to peer*, au cœur des apports techniques du protocole internet, notamment pour leurs capacités de mise à disposition et d'échanges de contenus numériques. Cette mutation a rendu plus prégnantes les questions posées par la protection des contenus numériques.

i. L'émergence de nouveaux usages chez les consommateurs.

Les notions de la propriété intellectuelle restent relativement abstraites et mal comprises par les consommateurs, pour lesquels l'achat d'un support préenregistré se confond bien souvent avec « l'achat d'une œuvre ». Globalement, les attentes des utilisateurs se situent entre la consommation de contenus « poussés », dans le cadre d'une offre éditoriale (radio, télévision) et la consommation de contenus « tirés », à l'endroit et au moment qu'il le souhaite, par exemple dans le cadre de services à la demande, mais ce qui induit aussi les notions de « *time shift* » et « *space shift* » (copie à des fins de décalage dans le temps et dans l'espace).

La diversité des systèmes de lecture, dans le cadre d'une convergence entre les systèmes issus de l'électronique grand public (chaîne de salon, baladeur, lecteur de CD Audio en voiture) et les PC, peut amener à réaliser de nombreuses copies d'une œuvre (sur un disque dur, sur une carte à mémoire, sur un CD Audio) ou à connecter ces divers éléments pour les faire fonctionner en réseau : c'est la perspective du « réseau domestique » (*home network*) sur lequel on trouve un ou des éléments d'accès au contenu (*home gateway* : une antenne satellite, un modem ADSL ou des supports optiques), des éléments de lecture et d'affichage, ainsi qu'un ou des éléments de stockage (que l'on peut appeler serveur domestique — *home server*), qui peut alors desservir les éléments de lecture.

Ce réseau domestique correspond au périmètre de la copie privée. Il nécessite d'approcher la protection du contenu de manière globale sur l'ensemble du réseau domestique.

L'application de mesures techniques de protection peut conduire à réduire le champ d'utilisation des œuvres en deçà de ce périmètre : par exemple, les systèmes de protection des CD Audio excluent la lecture sur un PC. Dans ce sens elles peuvent être mal acceptées par les consommateurs. **De manière générale, il convient que les mesures techniques mises en place n'interdissent pas au consommateur une certaine souplesse dans l'utilisation et trouvent un équilibre entre le découragement des pirates et l'encouragement des consommateurs honnêtes.**

ii. Nouvelle contrefaçon.

La contrefaçon traditionnelle reposait essentiellement sur des structures organisées, fonctionnant sur une base commerciale, qui distribuait des supports ou des systèmes électroniques de contournement des protections (par exemple des fausses cartes pour

décodeurs) et contre lesquelles les outils de lutte étaient principalement juridiques.[33] Le développement de la société de l'information s'est accompagné de l'émergence de nouvelles formes de contrefaçon numérique :

– **pour les contenus non protégés**, les utilisateurs peuvent accéder et redistribuer gratuitement des copies contrefaites par Internet (via les réseaux *peer to peer*, voire courrier électronique, messagerie instantanée, etc.). C'est la forme la plus délicate de contrefaçon numérique, car il est très difficile de lutter avec des outils juridiques contre des utilisateurs en très grand nombre. En revanche, des mesures techniques, mêmes assez rudimentaires, peuvent être « efficaces », au sens où elles atteignent un objectif de sécurité consistant à aider les « gens honnêtes à le rester », pour dissuader de ce type d'usages contrefaisants ;

Encadré 1.4. - Contrôle des échanges illicites sur P2P.

Le développement des réseaux à hauts débits (ADSL, câble, UMTS, etc.) s'appuie à présent sur des logiques d'abonnements forfaitaires qui témoignent (y compris sous forme explicite) de la faculté de téléchargement de musique, en pratique de manière illicite par le biais de réseaux *P2P*. Cette faculté constitue en effet l'un des premiers motifs d'abonnement. Or, l'analyse économique rappelle que dans une période de lancement de produit – et pour des choix politiques de développement de la société de l'information à travers des connexions à hauts débits – la formation du parc d'abonnés est – provisoirement – la variable stratégique. Dans ce contexte, il n'y a aucune rationalité économique à limiter les conditions d'attrait de la formation du parc d'abonnés au réseau, fussent-elles à l'origine d'usages illicites. En revanche, dans une période de maturité du produit et de l'accroissement – sans doute plus lent mais régulier – de la formation du parc d'abonnés, cette logique peut conduire à un arbitrage avec des investissements de capacité d'infrastructures. Une limitation d'accès au réseau *P2P* a pu commencer à se mettre en place par certains Fournisseurs d'Accès à Internet, essentiellement pour des raisons techniques, à travers, par exemple par **le contrôle et la modulation de l'allocation des volumes de bande passante par ports (SMTP pour le courrier électronique, HTTP pour le web) ce qui réduit, par différence, la bande passante utilisable pour le *P2P***. Sans être tout à fait explicite, ce type d'arbitrage est d'autant plus évoqué que les FAI cherchent aussi à développer des services d'accès à des offres musicales licites.

– **pour les contenus protégés**, des « *crackers* » informatiques peuvent les « dé-protéger » et les diffuser à des utilisateurs, ou même diffuser des logiciels de « dé-protection ». Cette diffusion est généralement gratuite et ne génère donc pas de revenus pour ces contrefacteurs, hormis éventuellement quelques revenus de nature publicitaire. Ce type de contrefaçon de l'ordre du « piratage fatal » a des conséquences très importantes. Dans ce cadre, la lutte contre ce type de contrefaçon repose essentiellement sur des instruments juridiques et sur un renforcement des mesures techniques afin de limiter le nombre de sources de contenus « dé-protégés », d'autre part, sur la possibilité de renouveler les protections, afin de faire perdre leur intérêt aux logiciels de « dé-protection ».

iii. Le rôle des distributeurs.

À la charnière de l'offre des industriels en matière de mesures techniques et notamment des *DRMS* pour la distribution en ligne, des catalogues d'œuvres numériques des producteurs et des demandes des utilisateurs, les distributeurs ont un rôle capital à jouer. Ce rôle peut être décliné de la manière suivante :

[33] cf. P. Chantepie, *La lutte contre la contrefaçon dans l'univers numérique*, IGAAC, sept. 2002. [http://www.culture.fr/culture/cspla/rapcontrefacon.pdf]

– Le distributeur constitue une passerelle entre l'univers des titulaires de droits et les plates formes de distribution.

– Le distributeur peut favoriser des formes de marketing fondées sur l'expérience de la distribution en ligne et notamment sur la mise en concurrence des offres des différentes plates-formes (élévation des offres de « *burning* » ou gravage).

– Le distributeur peut favoriser la transparence des *DRMS* et la facilité d'usage pour les utilisateurs. Il doit contribuer à améliorer la qualité des offres musicales en ligne licite face aux facilités offertes par le P2P.

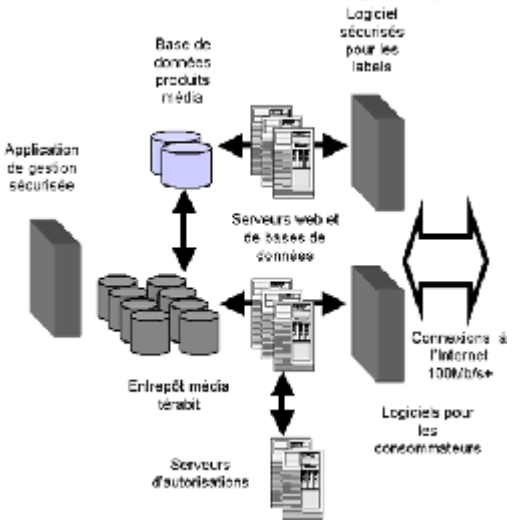
– Le distributeur peut assurer une fonction de tiers de confiance notamment en ce qui concerne la gestion des données personnelles. Il lui appartient non seulement de veiller à l'intégrité physique de l'ensemble des données numériques (œuvres, information sur les droits, données personnelles), mais aussi d'établir la mise en œuvre des garanties nécessaires à la protection des données personnelles contre des usages illicites de celles-ci. En particulier, sa fonction d'intégrateur de *DRMS*, lui permet de contrôler (interdire ou permettre) la remontée et la consolidation de données personnelles aux différents acteurs : sites, producteurs et SPRD.

Encadré 1.5. – La fonction de distribution :'OD2 (*On Demand Distribution*)

***OD2* est une entreprise française, leader européen dans la distribution musicale en ligne.**(34) Il met à disposition une infrastructure technique sécurisée et la solution logicielle de *DRM* proposée par Microsoft. *OD2* assure — pour les titulaires de droits et notamment les producteurs, assure le système de gestion des contenus numériques qui leur permet de conserver le contrôle total sur la diffusion des droits. Le distributeur assure également les téléchargements et transmission en flux (*streaming*).

Dans le cas *d'OD2*, les producteurs concernés sont notamment *EMI*, *Virgin*, *Warner Music*, *BMG*, etc. qui bénéficient d'un *reporting* en continu. Les clients principaux sont les fournisseurs d'accès et les distributeurs physiques de supports : *Wanadoo Music*, *Virgin.net*, *Tiscali*, *Fnac.com*, *MSN.uk*, etc.

Fig. 1.3 Plate forme de distribution



(34) OD2 (*On Demand Distribution*) [http://www.ondemanddistribution.com/fre/home/home.asp]

Le déploiement des *DRMS* et plus largement d'une offre de contenus numériques attractive, en particulier face aux usages illicites du *P2P*, suppose que les distributeurs favorisent des offres complètes par opposition aux premières offres des plates-formes musicales propriétaires *(MusicNet, Pressplay*), notamment susceptibles de réduire l'intérêt des Fournisseurs d'Accès à Internet en faveur de ces usages du *P2P*. Il implique donc une réduction des logiques d'intégration verticale de la production à la distribution, et une prise en compte des différents systèmes juridiques de gestion numérique des droits (gestion individuelle, collective, etc.) à l'égard desquels les *DRMS* devraient demeurer neutres, et donc une participation importante aux travaux de description des droits.

1.2.2. ENJEUX JURIDIQUES.

La transposition de la directive 2001/29 qui assure l'intégration dans le droit interne de la protection juridique des mesures techniques posée par les Traités OMPI du 20 décembre 1996 soulève un grand nombre de questions juridiques mais aussi techniques.[35] Le principal enjeu actuel concerne l'univers de la copie privée numérique à la fois pour les titulaires de droits, car constituant un « **clone** » **d'original**, elle est susceptible de créer **un manque à gagner et un risque de prolifération de la contrefaçon**, mais aussi pour les utilisateurs habitués à procéder à des copies pour profiter de la multiplicité des lecteurs.

1.2.2.1. L'enjeu juridique pour les titulaires et les industriels.

Le manque à gagner représenté par la copie privée numérique faisant l'objet d'un « système de rémunération » aux termes de la directive 2001/29 comme dans la plupart des pays européens, les industriels, notamment fabricants de supports d'enregistrements, portent le poids de la rémunération forfaitaire prévue à l'article L.311 du Code de la propriété intellectuelle. **Or, le déploiement des mesures techniques, notamment contre la copie numérique, et des systèmes numériques de gestion de droits sont – en apparence – contradictoires avec un tel système de dédommagement**. Toutefois, il convient de distinguer les effets de ces mesures sur les modalités de rémunération :

– **L'assiette des systèmes de rémunération pour copie privée est généralement établie sur les supports d'enregistrements numériques. Or, cette assiette ne paraît pas devoir être modifiée dès lors que même contrôlée, limitée, encadrée, la copie numérique s'effectuera toujours sur un support d'enregistrement** (supports optiques vierges, supports dédiés, supports informatiques). Les mesures techniques de contrôle de copie numérique devraient donc produire un effet négatif sur le volume de supports d'enregistrements « *utilisables pour la copie privée* ». En conséquence, du déploiement des mesures techniques de protection des œuvres, il convient surtout de s'attendre, à proportion des usages de copies, à une diminution mécanique de ces volumes. Cette diminution sera toutefois relative dès lors que l'article 5.2 b) de la directive permettant la copie privée est assorti d'une garantie d'exercice par la transposition de l'article 6.4. § 3 qui prévoit que les Etats « *peuvent aussi prendre des mesures appropriées* » pour s'assurer de l'effectivité de la copie privée. Le volume des supports utilisables pour la copie privée pourrait enregistrer une diminution proportionnelle à la montée en puissance de mesures d'interdiction ou de contrôle de copies. Ceci est moins vrai pour les supports hybrides non dédiés, car les mesures

(35) cf. 2e partie de l'étude dont c'est l'objet principal. On retrace ici de manière cursive, les principales conclusions qui peuvent s'extraire de l'analyse des mesures techniques et des Systèmes Numériques de Gestion de Droits.

techniques de contrôle de copie auront également pour effet d'abaisser la part relative des usages liés à la copie privée par rapport aux usages professionnels et au stockage de données personnelles (photo numérique,…).

– **Les *DRMS*, et dans une certaine mesure, les mesures techniques de protection, jouent un rôle quant à la nature de la rémunération pour copie privée**. En effet, un *DRMS* a très exactement pour vocation de contrôler l'utilisation des œuvres numériques protégées, y compris la copie privée numérique. Par conséquent, ces techniques de contrôle et licitation de copie permettent de **substituer à une rémunération forfaitaire établie sur des supports d'enregistrements** (« systèmes de rémunération » au sens de la directive), **des rémunérations proportionnelles à la source des autorisations de copie** (« compensation équitable » au sens de la directive). S'agissant des *DRMS*, c'est précisément la situation qui est rendue possible par des plates formes de distribution comme *Musicnet*, *Pressplay*, *Wanadoo Musique*, *LabelGate*, etc. Or, il s'agit de distribution d'œuvres par des «services interactifs à la demande » pour lesquels l'article 6.4 § 4 de la directive prévoit que l'exercice de la copie privée n'est pas obligatoire, que les Etats membres de l'Union européenne ne peuvent l'exiger, même si l'on constate qu'il est souvent autorisé et en voie de développement, sans doute pour permettre à terme environ trois copies non subséquentes, ce que prévoyait le SDMI. Mais cela entraîne une interrogation sur le cumul des rémunérations, le consommateur pouvant avoir le sentiment de payer deux fois le droit de copie, une fois à travers le système de gestion des droits et une fois à travers la rémunération forfaitaire pesant sur le support d'enregistrement.

L'effet principal des mesures techniques de protection et des *DRMS* consiste à opérer cette substitution d'une rémunération forfaitaire mutualisée sur l'ensemble des supports d'enregistrements, à des rémunérations spécifiques pour chaque copie privée autorisée. Dans ce cas, l'effet des mesures techniques contribue bien pour les titulaires de droits à recouvrer la plénitude de l'exercice de leurs droits exclusifs, mais aussi pour les industriels à voir s'opérer une soustraction des montants en cause. Il reste, que **la compensation pour copie privée proportionnelle ne peut se substituer totalement à un système de rémunération pour copie privée**. **L'enjeu principal porte sur les conditions de cumul et de substitution progressive d'un mode de dédommagement par un autre**.

1.2.2.3. Les utilisateurs : clef d'une dynamique à inventer.

Le déploiement des mesures techniques dans un environnement juridique particulièrement contraint devrait modifier en profondeur dans les toutes prochaines années le périmètre de la copie privée numérique pour les utilisateurs. Cette évolution centrée sur l'emploi de mesures techniques de protection axées sur le contrôle de copie pourrait d'ailleurs s'accentuer s'agissant de l'ensemble des supports optiques, avec l'émergence de nouveaux formats : SACD, DVD Audio. Les mesures techniques appliquées au CD Audio constituent alors une passerelle temporelle de protection des œuvres durant une période transitoire (3 à 5 ans). Ce serait l'effet le plus visible et le plus prochain de la mise en œuvre des Traités OMPI et de leur intégration dans le droit positif avec la transposition de la directive 2001/29.

Un tel contexte peut aisément favoriser un rejet à la fois des mesures techniques de protection et des *DRMS* qui ont tendance à être confondus. En effet, aux apports d'interopérabilité, de flexibilité, de nomadisme, etc. promis par la mutation numérique et les réseaux, **la mise en œuvre de mesures techniques ne peut manquer de mettre à jour la perte de valeur d'usage qu'elles engendrent et les risques d'une offre**

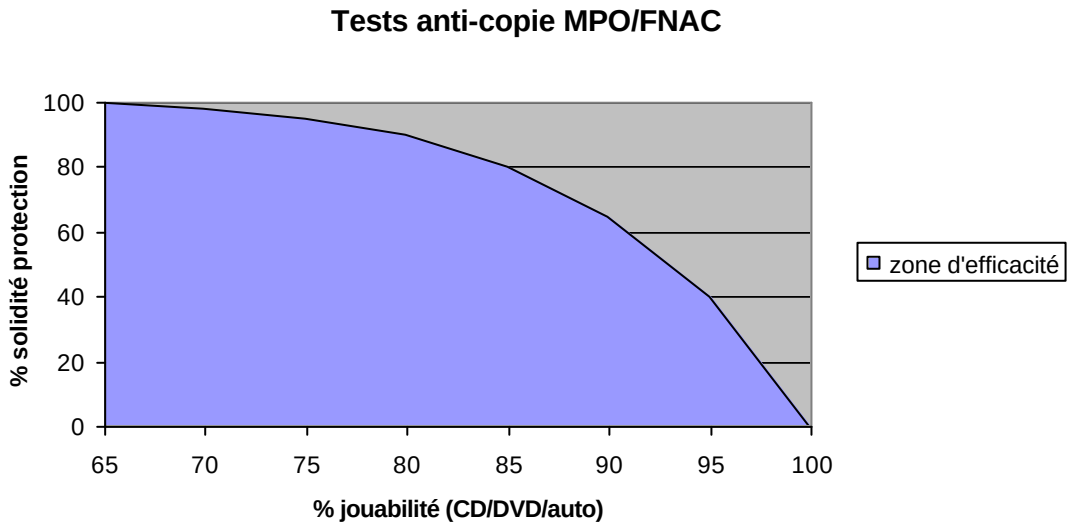
régressive, déceptive et inadaptée aux formes de consommation créées depuis près de dix ans. À l'occasion de cette évolution qui traduira la mutation du droit de propriété intellectuelle et les évolutions techniques, devrait alors s'amorcer une dynamique complexe, dont les principaux facteurs de succès dont les suivants :

i. Les mesures techniques : information, jouabilité.

Les mesures de contrôle de copie, justifiées par les fondements du droit exclusif d'autoriser ou interdire la copie sont, dans ce contexte juridique, ont été placées au centre du dispositif juridique pour favoriser une économie durable de la création. Toutefois ces mesures techniques apparaissent tant par leur objet que par leur principe de fonctionnement, notamment pour le CD Audio, relativement rustiques, fragiles et provisoires, dans l'attente de nouveaux formats. Elles conduisent à une réduction technique du périmètre de la copie privée, sous réserve des « *mesures appropriées* » que les Etats voudront bien prendre. Elles posent aujourd'hui plusieurs catégories principales de difficultés aux utilisateurs :

– **une diminution aléatoire de la « jouabilité » des CD Audio** qui à ce jour est d'autant plus destructrice de valeur apportée aux utilisateurs qu'elle reste aléatoire, mal maîtrisée, et peu susceptible de progrès significatifs sauf à diminuer fortement le degré de protection. C'est ainsi, qu'on ne constate pas de régularité des limitations collatérales de « jouabilité », selon les lecteurs, les gammes de lecteurs, les fabricants, mais aussi selon les systèmes d'exploitation, notamment *d'Apple*, mais aussi une plus faible liberté de reproduction. Cette réduction de valeur pour l'utilisateur doit être réduite au maximum par des efforts en amont de la commercialisation de CD Audio protégés pour repousser la frontière « robustesse/jouabilité ».

Fig. 1.4. – La frontière robustesse/jouabilité

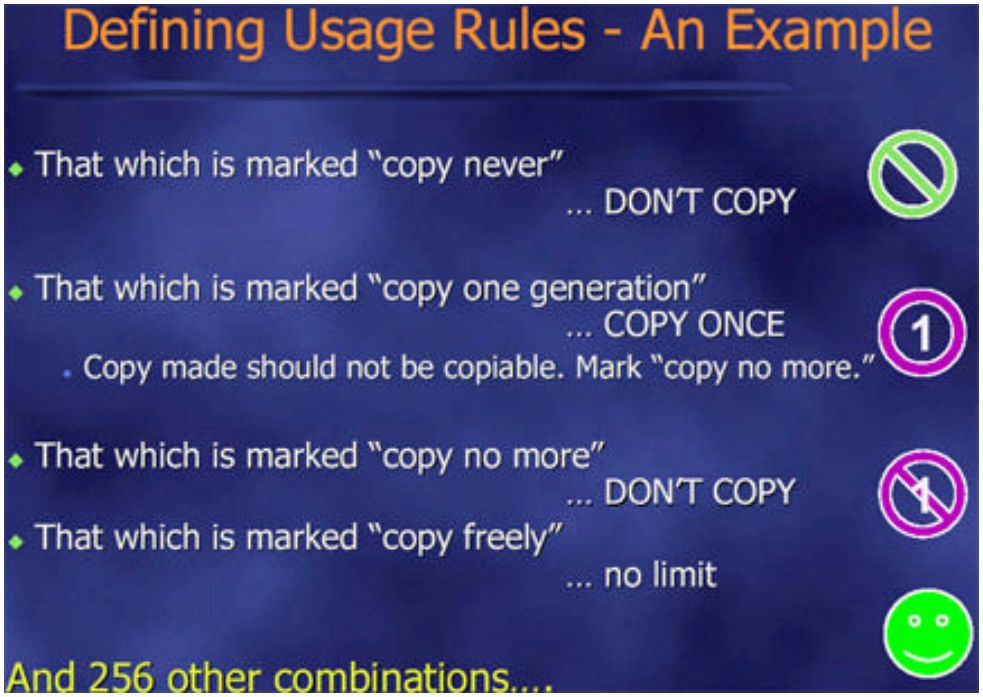


– **une information insuffisante** pour le moment et sans doute difficile à harmoniser et simplifier compte tenu des difficultés évoquées ci-dessus. Il apparaît nécessaire de produire **un effort massif d'information à la fois sur la copie privée numérique (par opposition aux activités de contrefaçon), mais aussi sur les conséquences pratiques d'implémentation des mesures techniques**. Il serait donc

particulièrement opportun de mettre en place une signalétique harmonisée du périmètre de la copie privée. L'information doit notamment viser deux objectifs :

– **une information sur le périmètre de la faculté de copie privée qui devra nécessairement être d'autant plus lisible, visible, explicite et complète**, que cette faculté bénéficierait pour l'environnement numérique d'une garantie législative et/ou institutionnelle. Elle pourrait prendre appui sur des propositions de signalétiques comme la suivante :

Fig. 1.5. – Une signalétique de la copie.



M. Hansen, *The Legal Framework for DRMs*
[http://www.eurubits.de/drm/drm_2002/slides/hansen.pdf]

- **Une information sur la mise en œuvres des mesures techniques de protection des supports optiques** et leurs effets en termes de «jouabilité ». Il ne fait pas de doute en effet, que les techniques mises en œuvres pour limiter la copie d'œuvres fixées sur support CD Audio ne peuvent que s'éloigner voire contrevenir au standard du CD Audio pour atteindre une quelconque efficacité, ce standard ne prévoyant pas de manière native une protection contre la copie (cf. *infra*). Par conséquent, la lecture de CD Audio protégés ne peut manquer d'être limitée selon les appareils de lecture qui peuvent être conformes au standard. Les principales difficultés sont apparues sur des lecteurs autoradio, des lecteurs sur PC munis d'un système d'exploitation Mac OS. 9 ou 10, voire des lecteurs de salon de CD Audio, ou encore des lecteurs de salons de DVD vidéo. Il est à ce stade difficile d'évaluer la nature des difficultés de lecture rencontrées, car elles manifestent un fort caractère aléatoire, selon les types d'appareils, de mesures techniques de protection, de systèmes d'exploitation. Pareille problématique suppose sans doute la mise en œuvre de tests à grande échelle de la part des acteurs mettant en œuvre des mesures techniques : industries de protection, titulaires de droits, en association avec les consommateurs et les distributeurs. **À l'issue de ces tests, une information précise, lisible et complète devrait figurer clairement sur phonogrammes du commerce, la mise en œuvre de mesures**

techniques pouvant constituer en tout état de cause une moindre valeur pour les utilisateurs.

– **Une faible compréhension de l'articulation à venir entre mesures techniques et rémunération forfaitaire pour copie privée** qui sans faire l'objet d'une adhésion forte apparaît bien comme une alternative à la mise en œuvre de mesures techniques anti-copie. Les conditions et méthodes par lesquelles la prise en compte des mesures techniques pourra voir le jour comme le prévoit l'article 5.2 b) de la directive 2001/29 mériteront certainement une clarification.

ii. Les DRMS : transparence, services à valeur ajoutée.

La mise en œuvre de *DRMS*, comprenant des mesures techniques de protection, peut rencontrer d'autres obstacles du point de vue des utilisateurs et implique plusieurs évolutions de la part des acteurs économiques.

– **Des exigences pour les utilisateurs : protection de la vie privée et simplicité.** Les *DRMS* ayant pour fonction d'assurer la licitation d'usages des œuvres peut faire craindre l'apparition de technologies « intrusives », susceptibles de menacer la protection de la vie privée (cf. *infra*). L'acceptation des *DRMS* par les utilisateurs suppose que soient clairement levées ces interrogations, notamment quant au périmètre des données nominatives susceptibles de faire l'objet d'un traitement informatique, c'est-à-dire plus précisément des consolidations d'informations nécessaires à l'exécution des conditions contractuelles d'utilisation des œuvres (cf. *infra*). Au-delà, la mise en place des *DRMS* doit revêtir pour l'utilisateur une grande transparence et ne pas rendre plus complexe l'accès aux contenus, mais plus aisé.

– **L'évolution rapide en faveur d'une offre riche et innovante de contenus.** L'acceptation des *DRMS* est enfin dépendante de la valeur ajoutée nouvelle constituée par la formation d'une offre de contenus numériques élargie et d'une très grande flexibilité d'usages. Si la protection juridique des mesures techniques a pour effet de favoriser le passage des seuls droits d'autoriser ou d'interdire la reproduction à la formation de droits d'accès et d'utilisations, les offres contractuelles nouvelles d'œuvres protégées devront sans doute atteindre un **élargissement des droits d'utilisation des œuvres**, notamment dans le sens de la flexibilité, du nomadisme, de création de communauté, par exemple autour des droits de prêts, de transports, de location, d'accès dans le temps, d'archivage à distance, etc., c'est-à-dire une **innovation dans le domaine des « droits numériques »**.

– **Une capacité à offrir une alternative crédible d'offre licite de contenus**. Si le développement des mesures techniques et des *DRMS* précède l'essor de l'usage du *P2P* à des fins de illicites, il apparaît de plus en plus comme un système ne poursuivant qu'exclusivement la mise au ban de ces systèmes d'échanges qui expriment pourtant le plus exactement la structure du réseau Internet, ou bien restreignant des usages comme la copie privée déjà largement développée. **L'enjeu concurrentiel consiste donc à offrir une alternative d'offre licite et payante de contenus face au *P2P* considérée comme une « trappe à business »**. Un tel objectif implique :

– de favoriser les offres, notamment par l'accès non discriminatoire et le plus étendu possible aux catalogues ;

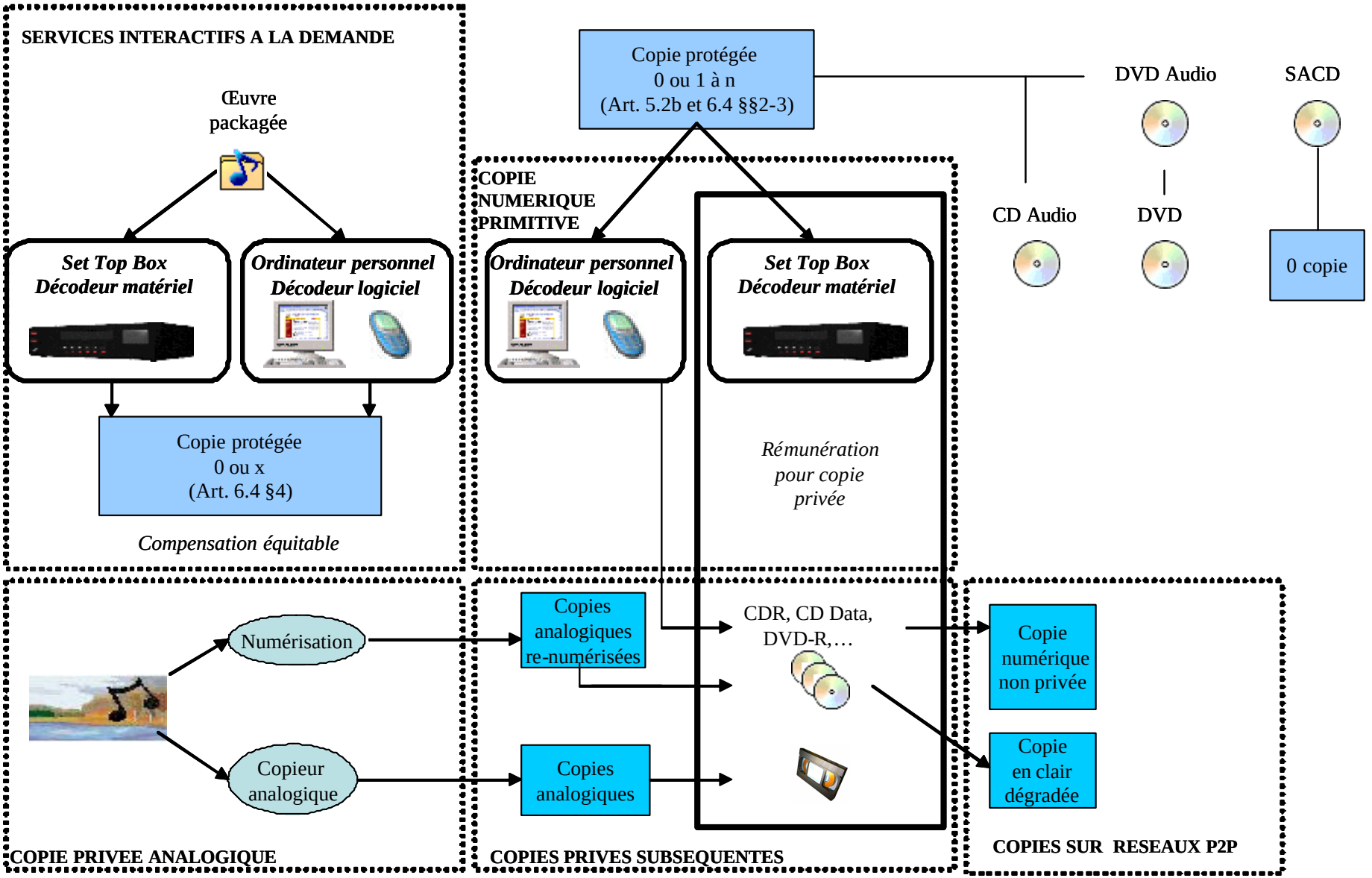
– de veiller à ce que les mesures techniques de protection et les *DRMS* ne favorisent pas des barrières d'entrée à l'accès au catalogue ;

– d'observer les risques d'ententes prohibées ou d'abus de position dominante sur des segments-clés de la chaîne de protection des contenus (formats de compression / décompression, encodeurs / décodeurs, outils de lecture.[36])

La mise en œuvre d'une protection juridique des mesures techniques ouvre une période transitoire dans laquelle devraient voir le jour, non pas seulement une limitation des usages, mais une évolution des droits de propriété littéraire et artistique associés à ces techniques de protection et de distribution. La réunion de l'ensemble des conditions de succès de cette évolution n'est pas à ce jour complètement établie.

[36] Il n'appartient pas à cette étude de procéder à une analyse de tels risques mais simplement d'en signaler l'existence, par exemple dans la perspective de la *Décision de la Commission du 11 octobre 2000 déclarant une opération de concentration compatible avec le marché commun et avec l'accord EEE (Aff. N° COMP/M1845 – AOL/Time Warner)* qui s'était penchée sur les marchés du téléchargement de musique et des outils de lecture, des accords passés avec des fournisseurs techniques, les questions de format, d'outils de compression/décompression, etc. [http://europa.eu.int/eur-lex/pri/fr/oj/dat/2000/c_130/c_13020000511fr00080008.pdf]

Fig. 1.6 — La copie privée au sens juridique.



2. LES MESURES TECHNIQUES DE PROTECTION.

La protection technique des œuvres s'exerce soit à partir du codage numérique des œuvres numérisées (techniques de tatouage) soit à travers des techniques de cryptographie qui concernent non seulement la protection technique d'accès aux œuvres donc les modes de distribution sur supports optiques ou en réseaux, soit des mesures anti-copie.

Si les premières techniques ont d'abord semblé devoir constituer le cœur technologique de la protection des œuvres, ce sont en réalité les secondes qui jouent un rôle déterminant. Les premières ayant trait directement à la numérisation des œuvres qui par nature sont dans l'environnement technique de l'utilisateur, ont montré assez vite leurs limites en termes de protection, mais permettent sans doute des développements d'usages particulièrement féconds, y compris pour la protection – au sens large – de la distribution des œuvres. **Les techniques de cryptographie, déjà utilisées dans le cadre de la distribution des contenus sur les réseaux sont, du fait d'un mouvement de libéralisation des conditions juridiques d'emploi, au cœur technologique de la protection des œuvres.**

Si les composants des mesures techniques se distinguent théoriquement, on assiste de plus en plus souvent à des logiques combinatoires pour le développement des applications, en particulier pour la mise en œuvre de systèmes numériques de gestion de droits (*Digital Rights Management Systems*).

Il faut préciser d'emblée que, par nature, les technologies de protection des œuvres ne prétendent jamais parvenir à un niveau de protection totale, une robustesse absolue ou une inviolabilité générale. Elles tendent principalement à atteindre des niveaux de sécurité, à réduire l'intérêt et la facilité de contournement et s'inscrivent dans une dynamique protection/faillibilité.

2.1. LES TECHNIQUES DE LA CRYPTOGRAPHIE.

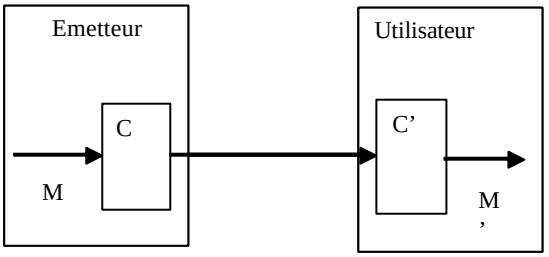
La cryptographie est la technique du secret des messages, développée originairement pour répondre à des besoins militaires mais dont les applications et les usages sont très largement répandus dans la société de l'information, que ce soit pour la sécurité des transactions, la confidentialité des secrets industriels et commerciaux, la protection des contenus, etc.

Après avoir défini le principe de la cryptographie, il convient de détailler les divers éléments susceptibles de constituer le maillon faible du système : l'algorithme et la gestion des clés, puis d'examiner les applications de la cryptographie à la protection des contenus.

2.1.1. LE PRINCIPE DE LA CRYPTOGRAPHIE.

– La cryptographie consiste à chiffrer un message «M » avec un algorithme de chiffrement secret « C », pour aboutir à un message codé « M' » apparemment vide de sens. L'algorithme de chiffrement « C » doit être suffisamment compliqué pour que seul un utilisateur disposant de l'algorithme de déchiffrement également secret «C' » associé à « C » puisse alors déchiffrer le message « M' » pour retrouver le message initial « M ». Le message « M' » est donc sans intérêt pour un utilisateur ne disposant pas de l'algorithme « C' ». Il peut donc être librement diffusé sans risques.

Fig. 2.1. – Principe de chiffrement.



Ce système a pour objet de protéger non seulement contre une rediffusion en clair du contenu par l'utilisateur (ce qui suppose que le déchiffrement chez l'utilisateur s'effectue d'une manière contrôlée) mais également contre une interception par un pirate extérieur (ce qui est en fait la fonction première du chiffrement). Cela explique que ce système soit systématiquement utilisé pour la télédiffusion à péage ou pour les réseaux de télécommunications notamment sur le réseau Internet, mais il peut également être utilisé dans d'autres contextes par exemple la distribution de contenus numériques sur supports optiques (cas du DVD vidéo).

La cryptographie a fait d'immenses progrès en termes de calcul avec l'informatique, qui permet de réaliser très rapidement les diverses opérations nécessaires au chiffrement et au déchiffrement des messages. Pour cette raison, les messages et les clefs sont représentés en binaire : l'élément unitaire d'information est le bit, qui vaut 0 ou 1.

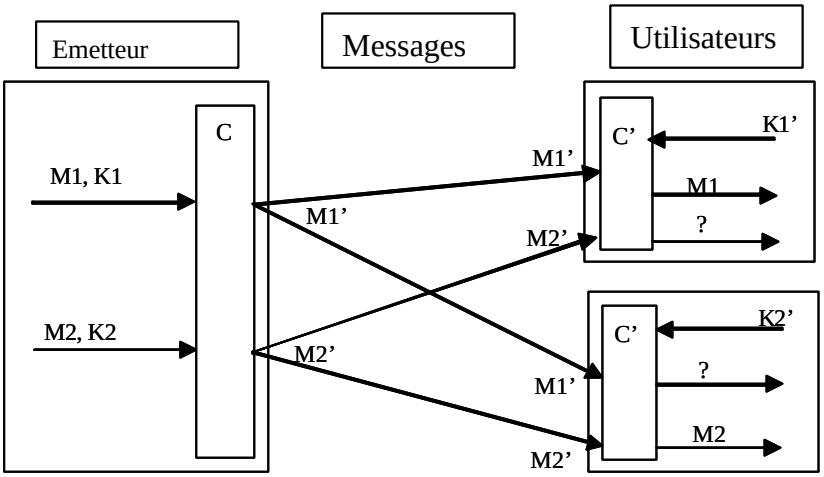
Tableau 2.1. – Le rapport nombre de bits / chiffrement

Nombre de bits	Nombre de valeurs possibles
38	$2^8 = 256$
16	$2^{16} = 65\,536$
32	$2^{32} = 4\,294\,967\,296$
40	$2^{40} = 1\,099\,511\,627\,776$

2.1.1.1. Les clefs : racines de la cryptographie.

Le principe de cryptographie ne permet pas de différencier facilement les utilisateurs : l'émetteur doit pouvoir communiquer avec l'utilisateur « A » sans que l'utilisateur « B » puisse avoir accès au message « M » et vice-versa. On utilise donc des clefs pour faire varier l'algorithme, le chiffrement s'effectuant désormais à l'aide de l'algorithme « C » et d'une clef « K », le déchiffrement s'effectuant à l'aide de l'algorithme «C' » et d'une clef «K' », les clefs «K » et «K' » étant associées de manière unique.

Fig. 2.2. L'algorithme de chiffrement.



L'émetteur utilise alors le même algorithme « C » pour chiffrer tous les messages. Il suffit alors de faire varier les clefs (K, K') d'un utilisateur à l'autre. Tous les utilisateurs utilisent également le même système de déchiffrement « C' ». Cela permet également de cloisonner les risques : si la clef «K1' » de l'utilisateur A est compromise, on peut changer le couple de clefs (K1, K1') sans impacter l'utilisateur B. Le secret ne repose donc plus seulement sur les algorithmes « C » et « C' » mais aussi sur les clefs « K » et « K' ». **À la limite les algorithmes « C » et « C' » peuvent ne pas être secrets.** Pour atteindre un bon niveau de sécurité, ces algorithmes doivent bénéficier de certaines propriétés : par exemple, il faut qu'un pirate ayant réussi à connaître l'algorithme « C' », un exemple d'un message en clair « M1 » et du message codé correspondant « M1' », ne puisse pas retrouver la clef secrète « K1' » de l'utilisateur « A », sinon cela lui permettrait de déchiffrer sans effort tous les messages codés envoyés à l'utilisateur « A ».

Il est recommandé d'utiliser des algorithmes éprouvés, issus de la re cherche en cryptologie. L'inconvénient est que ces algorithmes sont connus, ce qui apporte un élément d'information à un pirate potentiel, l'avantage est que ces algorithmes ont été testés, analysés et que leurs éventuelles faiblesses sont connues à l'avance, ce qui permet de les éviter.

2.1.1.2. Les algorithmes.

Les principaux algorithmes de chiffrement se classent en deux catégories : les algorithmes symétriques et les algorithmes asymétriques.

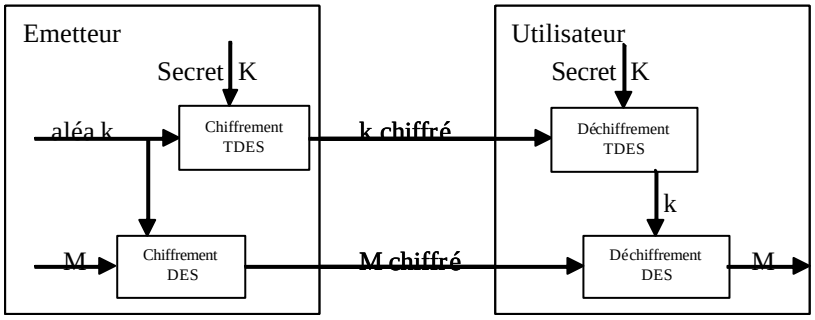
i. Algorithmes symétriques.

Dans le cas des algorithmes symétriques, la clef de chiffrement K et la clef de déchiffrement K' sont identiques : lorsqu'un émetteur veut communiquer avec un utilisateur, ils partagent une unique clef, « K », dite « clef secrète ». L'algorithme symétrique le plus connu est le DES (*Data Encryption Standard*), issu de travaux de recherche menés par IBM dans les années soixante-dix, puis complétés par la NSA (*National Security Agency*) et le NBS (*National Bureau of Standards*). Le DES utilise une clef de 64 bits, dont 8 sont des bits de parité, soit en fait au total 56 bits.(37) Il consiste en 16 passages successifs dans une série d'opérations d'addition bit-à-bit, de substitution et de permutation de bits. Il est donc assez simple à utiliser sur une puce électronique ou un logiciel et assez rapide.

Cependant, l'augmentation de la puissance de calcul des ordinateurs permet désormais de « casser » le DES, en essayant toutes les 2^{56} clefs possibles. Des « compétitions » ont été organisées à cet effet : un système composé du super-calculateur DES Cracker de l'EFF (*Electronic Frontier Fondation*) et de 100 000 PC travaillant en réseau avec *Distributed.net* a ainsi pu «casser » un DES en 22 heures début 1999. Le DES n'est donc plus totalement sécurisé, même si ce type d'attaque n'est cependant pas à la portée de tout le monde. La NSA a interdit l'utilisation du DES pour l'administration américaine et recommande désormais le TDES (triple DES, trois DES successifs avec deux ou trois clefs différentes) et peut être bientôt l'AES (*Advanced Encryption Standard*) issu de l'algorithme belge *Rijndael.*

On peut cependant utiliser l'algorithme DES de manière plus sécurisée, en changeant fréquemment la clef. Cela amène à un **système de clefs hiérarchique**. L'exemple le plus simple étant celui appelé «**l'enveloppe numérique** » : l'émetteur chiffre le message « M » avec une clef aléatoire « k » en utilisant l'algorithme DES. Il chiffre ensuite la clef « k » avec une clef maître « K », avec un algorithme plus puissant comme le TDES, et il envoie le message «M » chiffré et la clef «k » chiffrée à l'utilisateur, qui déchiffre d'abord la clef « k » puis le message « M ». La clef secrète partagée est alors la clef K.

Fig. 2.3. – Chiffrement par « enveloppe numérique »



L'avantage de ce système est d'utiliser un algorithme de chiffrement du message certes plus faible mais surtout plus rapide, tout en cloisonnant les différents

(37) Ces *bits* servent à corriger les éventuelles erreurs lors de la transmission de la clef.

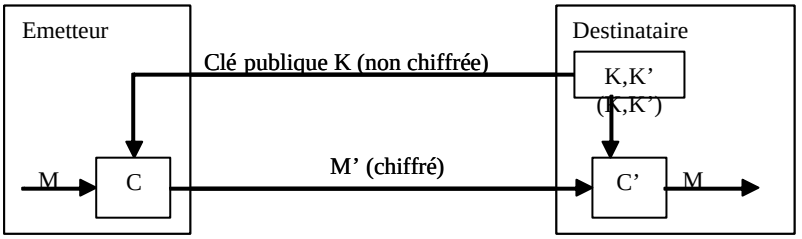
messages : découvrir la clef k est de peu d'utilité puisqu'elle change à chaque message. On retrouvera ainsi ce principe de systèmes de defs hiérarchique dans de nombreuses applications, particulièrement adapté à la protection d'œuvre singulière.[38]

ii. Algorithmes asymétriques ou « algorithmes à clef publique ».

La difficulté majeure des algorithmes symétriques concerne la gestion des clefs : avant d'échanger des messages cryptés, il faut en effet que l'émetteur et l'utilisateur se soient échangés la clef secrète partagée K par une voie sécurisée. C'est l'objectif principal des algorithmes asymétriques. Les clefs de chiffrement « K » et de déchiffrement «K' » sont différentes mais associées de manière unique, **sans que la connaissance d'une des clefs permettre de découvrir l'autre**. Les premiers algorithmes ont été inventés dans les années 1970 afin d'apporter une solution au problème de gestion des clefs. En effet, un destinataire peut générer aléatoirement un couple de clefs (K,K') et communiquer librement la clef de chiffrement « K », appelée « clef publique », tandis que la clef de déchiffrement « K' » reste secrète et prend donc le nom de « clef privée ».

Divers émetteurs peuvent donc utiliser la clef publique «K » pour chiffrer un message, avec la certitude que seul le destinataire pourra déchiffrer le message avec sa clef privée « K' », garantissant ainsi la confidentialité de l'échange, sans reposer sur l'échange initial d'un secret.

Fig. 2.4. – Chiffrement à clef publique.



Les algorithmes de cryptographie asymétrique sont souvent utilisés en lien avec des mécanismes d'authentification et de signature électronique : il faut en effet que l'émetteur puisse être assuré que la clef publique «K » qu'il utilise est bien celle du destinataire auquel il souhaite envoyer un message. L'algorithme asymétrique le plus connu est le RSA (du nom de ses inventeurs : *Rivest, Shamir et Adleman*).[39] D'autres systèmes ont été proposés, reposant sur les courbes elliptiques[40]. Ce type d'algorithmes présente des avantages évidents par rapport aux algorithmes symétriques, mais l'inconvénient d'être environ 1 000 fois plus lents. C'est la raison pour laquelle on utilise fréquemment le système de **« l'enveloppe numérique » : le message est transmis chiffré avec une clef symétrique aléatoire « k », et la clef « k » est transmise chiffrée avec la clef publique du destinataire** .

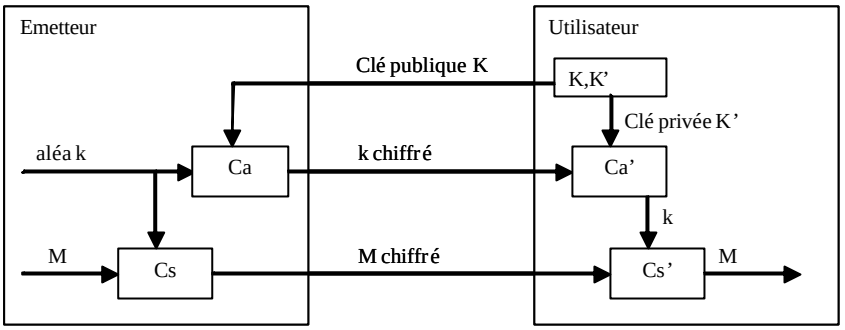
---

[38] De nombreux autres algorithmes symétriques existent, comme le *Blowfish*, utilisé dans DTCP, C2 dans CPRM, RC2, RC4, RC5 (*Rivest's Cipher*) utilisés dans SSL (*Secure Socket Layer*) pour les échanges sécurisés sur Internet. (cf. *infra* selon les mesures techniques fondées sur des solutions de cryptographie.)

[39] L'algorithme *RSA* repose sur le problème de la factorisation de grands entiers en nombres premiers et sur le logarithme discret. (cf. *RSA Laboratories* — Cryptography FAQ — RSA [http://www.rsasecurity.com/rsalabs/faq/3-1.html])

[40] V.S. Miller, *Use of elliptic curves in cryptography*, *Advances in Cryptology* -- Crypto 85, Springer-Verlag, 1986.

Fig. 2.5. – Chiffrement à clef symétrique aléatoire.



iii. La cryptanalyse.

La cryptanalyse est la discipline qui analyse la robustesse des procédés cryptographiques. L'attaque de base d'un algorithme cryptographique est l'attaque par « recherche exhaustive », qui consiste à essayer toutes les clefs possibles. Dans le cas d'un DES avec une clef de 56 bits, cela nécessite donc 2^{56} tentatives. Le nombre de tentatives nécessaires est alors appelé **la complexité de l'attaque**.

L'objet de la cryptanalyse est alors d'identifier des attaques de moindre complexité, puis ensuite de vérifier si ces attaques sont réalisables selon les ressources dont on peut disposer en termes de puissance de calcul et de mémoire.

L'exemple le plus éloquent à cet égard est l'algorithme CSS (*Content Scrambling System*) qui est au centre de la protection du DVD vidéo. Il repose sur des clefs de 40 bits (ce qui est déjà relativement faible par rapport aux clefs DES de 56 bits). Il semblerait que des pirates aient pu casser les clefs en 17 heures par une attaque par recherche exhaustive (soit 2^{40} tentatives). Des cryptanalyses réalisées ensuite ont défini diverses attaques, réduisant la complexité à 2^{25}, puis 2^{16} puis 2^{8}, ce qui permettait de casser la protection en une fraction de seconde !

Les résultats obtenus par les travaux de cryptanalyse sur cette mesure technique de protection de contenus numériques montrent que la cryptanalyse est indispensable pour s'assurer de la robustesse d'un algorithme, d'où l'intérêt d'utiliser des algorithmes éprouvés, sur lesquels de nombreux chercheurs se sont penchés.(41)

Les longueurs de clefs actuellement recommandées sont de 80 bits pour l'algorithme symétrique TDES et de 1 024 bits pour l'algorithme asymétrique RSA. Ces clefs sont considérées comme incassables avec les moyens disponibles d'ici 10 ans. Cela ne veut cependant pas dire que les clefs de longueur inférieure ne sont pas utilisables, mais qu'elles peuvent être cassées, à condition de disposer de moyens importants.

(41) Ce domaine de recherche essentiel, y compris aux mesures techniques protégées juridiquement par les dispositions de la directive 2001/29 suppose donc, sous une forme ou une autre une sécurité juridique des activités de cryptanalyse. (cf. 2e partie de l'étude : *La régulation des mesures techniques.* 2.2.2).

L'efficacité relève principalement de la relation entre le volume de calcul pour casser une clef, fonction de sa longueur, et l'objectif de protection visé par la mise en œuvre d'une solution de cryptographie. À elle seule, elle ne pourrait être considérée comme un critère d'efficacité d'une mesure technique de protection d'une œuvre.

2.1.2. LA GESTION DES CLEFS.

Une gestion efficace des clefs joue un rôle déterminant dans l'efficacité des solutions de cryptographie. Elle comprend divers mécanismes sécurisés du cycle de vie des clefs : la création, la distribution, le stockage et la révocation. La révocation d'une clef consiste à signaler qu'une clef ne peut plus être utilisée, par exemple lorsqu'elle a été compromise. La création des clefs ne présente pas d'enjeux spécifiques à la protection des contenus et ne sera pas évoquée.

Les étapes critiques pour la protection des contenus numériques concernent le stockage des clefs, essentiel à l'objectif de sécurité dans un contexte où l'utilisateur a la maîtrise physique de l'environnement technique, ainsi que **la gestion coordonnée de la diffusion et de la révocation des clés** pour permettre l'évolution de la protection.

2.1.2.1. Les techniques de stockage des clefs.

Un premier point essentiel concerne le stockage des clefs secrètes chez l'utilisateur. Dans le contexte de la protection des contenus numériques, l'utilisateur doit pouvoir disposer de manière limitée des clefs secrètes de déchiffrement, afin de pouvoir lire le contenu dans un **environnement contrôlé c'est-à-dire capable d'interdire ou de limiter l'accès et l'utilisation des clefs de déchiffrement pour obtenir une copie en clair du contenu**. Deux solutions sont envisageables :

– ***La constitution d'une « boîte noire » protégeant les clefs le stockage des clefs secrètes dans un composant électronique avec l'algorithme de déchiffrement***. C'est la solution généralement utilisée dans le domaine de l'électronique grand public. Les systèmes électroniques en général ne sont cependant pas inviolables : un pirate peut analyser le fonctionnement des composants, voire même les radiographier afin d'en comprendre en détail le fonctionnement.[42] Cela nécessite cependant des compétences et surtout de l'équipement spécialisé et parfois coûteux, ce qui limite le risque aux structures organisées fonctionnant sur un modèle de contrefaçon commerciale. **Ce système peut être amélioré en utilisant des «cartes à puce »**, qui permettent de diversifier plus facilement les clefs (chaque utilisateur peut avoir une clef différente) **et surtout de les renouveler en cas de piratage fatal**. Les cartes à puce sont ainsi utilisées depuis longtemps dans les systèmes de télévision à péage. **La difficulté de ces systèmes concerne l'identification et la révocation des systèmes pirates** : un tel système acquis au marché noir peut fonctionner sans que le diffuseur ne s'en rende compte. Une autre difficulté concerne le modèle économique du **renouvellement des cartes à puce**, qui reste coûteux : si ce modèle peut fonctionner pour les systèmes par abonnement comme la télévision à péage, c'est moins simple pour les autres systèmes, où l'utilisateur achète un matériel (lecteur de DVD par exemple).

---

[42] D. Naccache, *Cryptography and copy protection*, Colloque du 17/01/2002 à Rennes [http://tim.irisa.fr/tim-adherents/17-01-2002/Gemplus.pdf].

– ***Une autre solution consiste à stocker les clefs secrètes dans un logiciel (ou un code numérique).*** Un tel logiciel peut alors facilement être transmis pour renouvellement par téléphone ou par Internet, avec un coût limité, ce qui constitue un avantage par rapport à l'électronique. **Mais ce système présente l'inconvénient d'être bien moins robuste** que l'électronique : là encore, un pirate peut analyser le fonctionnement du logiciel pour en déduire la clef et cela ne nécessite que peu d'équipement (un ordinateur). C'est d'ailleurs grâce à l'analyse d'un logiciel que l'algorithme CSS a été cassé.

Il existe cependant des techniques visant à durcir les systèmes, tant logiciels qu'électroniques, pour en faire des systèmes « résistants au tripatouillage ».[(43)] De nombreux travaux de recherche proposent des solutions en ce sens.[(44)] Dans le cas particulier de la vente de contenu par Internet, la sécurité du logiciel de lecture peut être accrue en ne stockant la clef de déchiffrement que le temps de l'utilisation du contenu, avant de la détruire.

Dans tous les cas il convient certainement de cloisonner les clefs concernant la protection des mesures techniques assurées par des systèmes électroniques ou par des systèmes logiciels.

2.1.2.2. Techniques de transmission et de révocation des clefs.

Parmi les nombreux systèmes de gestion des échanges de clefs, deux d'entre eux correspondent le mieux aux situations rencontrées par la distribution de contenus numériques :

– **Les systèmes de transmission «en ligne** » qui supposent l'existence d'une communication possible de l'utilisateur vers l'émetteur, utilisés notamment pour la diffusion sécurisée par Internet, comme pour le protocole SSL (*Secure Socket Layer*) protocole « *handshake* ».[(45)] Dans le cas des systèmes «en ligne », le protocole est le suivant : l'émetteur commence par envoyer à l'utilisateur sa clef publique « K », authentifiée. L'utilisateur génère alors une clef symétrique aléatoire « k », qu'il renvoie chiffrée avec la clef publique « K » de l'émetteur à celui-ci. L'émetteur est donc le seul à pouvoir déchiffrer la clef chiffrée «k », avec sa clef privée « K' » associée à sa clef publique « K ». L'émetteur et l'utilisateur sont alors les seuls à connaître la clef secrète symétrique partagée « k », qui leur permet d'échanger des messages chiffrés. L'utilisateur peut alors transmettre son numéro de carte bancaire et recevoir en échange un contenu et une clef de déchiffrement (qui restera cachée dans le logiciel).

Comme cette clef de déchiffrement change pour chaque contenu distribué, l'attaquer présente un intérêt limité par rapport aux efforts nécessaires pour le pirate. Elle est d'un grand intérêt pour la distribution œuvre par œuvre, utilisateur par utilisateur.

---

(43) Traduction de « *tamper-resistant* » proposée par G. Brassard, *Cryptographie Contemporaine*, Masson, 1992.

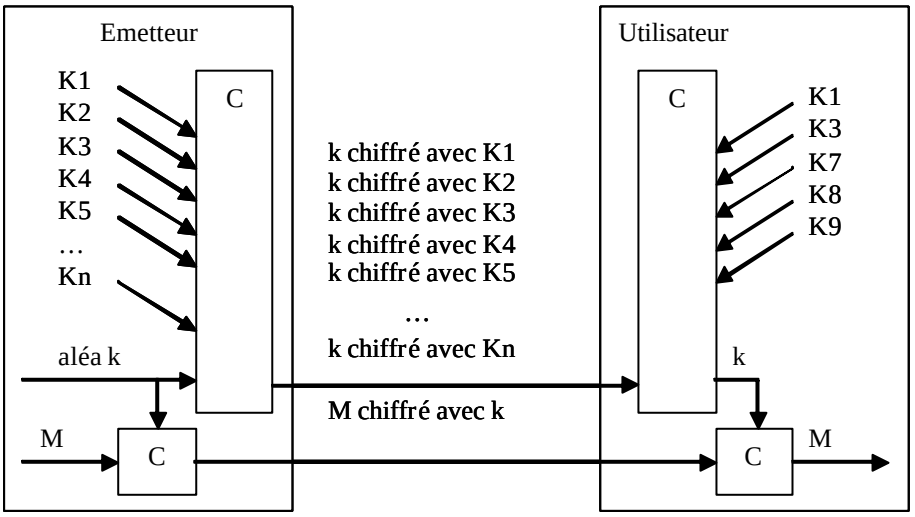
(44) S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot, *A white-box DES implementation for DRM applications, Pre-proceedings for ACM DRM-2002 workshop* ; T. Ogiso, Y. Sakabe, M. Soshi, A. Miyaji, *Software Tamper Resistance Based on the difficulty on Interprocedural Analysis*, 3rd international *Workshop on Information Security Applications*, 2002.

(45) Voir *RSA Laboratories, Cryptography* FAQ [http://www.rsasecurity.com/rsalabs/faq/2-2-4.html]

– **Les systèmes «à sens unique ».**[46] Ils sont utilisés pour la télédiffusion (*broadcast*) ou dans la protection des supports optiques chiffrés ; ils ne prévoient pas de retour de l'utilisateur vers l'émetteur.

Dans le cas des systèmes «à sens unique », la sécurité repose nécessairement sur une ou plusieurs clefs secrètes initiales. Mais **afin de bien cloisonner le système et pouvoir révoquer un pirate sans gêner les autres utilisateurs, il faut différencier les clefs d'un utilisateur à l'autre, sans pour autant devoir utiliser des milliers voire des millions de clefs**. Des techniques ont été proposées, consistant à définir un ensemble de n clefs (K1, K2,… Kn). À chaque utilisateur est attribué un sous-ensemble des clefs, ce qui multiplie les possibilités. Par exemple, pour un ensemble de 400 clefs, si chaque utilisateur dispose d'un sous-ensemble de 5 clefs, ce système permet de définir 83 218 600 080 sous-ensembles différents (soit le nombre de combinaisons possibles de 5 clefs parmi 400) correspondant à un nombre théorique équivalent d'utilisateurs potentiels. L'émetteur définit alors une clef symétrique aléatoire « k », qui servira à coder le contenu. Il transmet aux utilisateurs le contenu chiffré avec la clef « k » et la clef « k » chiffrée avec les n clefs (K1, K2, … Kn). Tout utilisateur peut déchiffrer « k » avec son sous-ensemble de clefs puis déchiffrer le contenu avec « k ». Cependant, l'émetteur peut révoquer un utilisateur pirate en supprimant le sous-ensemble unique de clefs qui lui a été attribué, sans impacter les autres utilisateurs.

Fig. 2.6. – Transmission de clefs « à sens unique ».



Exemple avec 5 clés : Si l'émetteur supprime les clés K1, K3, K7, K8 et K9, l'utilisateur ci-dessus ne pourra plus déchiffrer k et donc M. Par contre, un autre utilisateur qui disposerait par exemple des cinq clés K1, K3, K7, K8, K10, pourra toujours utiliser la clé K10.

(46) A. Fiat, M. Naor, *Broadcast Encryption*, 1993, [http://www.wisdom.weizmann.ac.il/~naor/PAPERS/broad.ps] ; D. Naor, M. Naor, J. Lotspiech, *Revocation and Tracing Schemes for Stateless receivers*, 2001, [http://www.wisdom.weizmann.ac.il/~naor/PAPERS/2nl_no_fig.pdf]

2.1.3. CRYPTOGRAPHIE ET PROTECTION DES CONTENUS.

Les mesures techniques de chiffrement/déchiffrement peuvent être appliqués aussi bien comme mesures techniques d'accès que comme mesures techniques de contrôle de copie. Dans ce cas, sont associés des opérations — distinctes — de chiffrement/déchiffrement des contenus numériques, et d'autre part du régime d'information sur les droits. Cette double fonctionnalité repose sur une évolution du contexte de protection des contenus numériques.

2.1.3.1. L'évolution du contexte de sécurité des contenus numériques.

Le développement de la société de l'information a fait basculer les contenus numériques dans un monde ouvert, où il est désormais possible, avec des moyens limités, d'accéder aux informations d'un support optique, d'analyser un flux numérique, de stocker des informations, de les diffuser à travers le monde, etc. Dans ce cadre, les approches classiques de la protection des contenus numériques, soutenues par l'industrie de l'électronique grand public, consistaient à conserver le contenu dans un « **périmètre sécurisé** », **ne comportant que des appareils conformes**, au sens où ils doivent respecter les paramètres de protection des contenus numériques.(47) Avec l'arrivée des ordinateurs, par essence multifonctionnels et ouverts, cette notion a eu tendance à disparaître.

Le champ des applications de la cryptographie s'en trouve élargi, puisqu'elle contribue à (re)créer les conditions d'un «périmètre sécurisé » dans l'environnement technique ouvert de l'informatique et des réseaux : **les opérations de chiffrement/déchiffrement des contenus numériques et de l'information sur les droits qui y sont attachés consistent essentiellement à contrôler (ouvrir/interdire) l'accès à des systèmes conformes, et en leurs seins, à contrôler des contenus numériques**.

i. L'expérience de la sécurisation du DVD Vidéo pour le DVD Audio.

Le DVD vidéo fut créé en 1996, à l'initiative de l'industrie qui y voyait un nouveau produit susceptible de conquérir le public et de générer de l'activité en terme d'équipement des foyers et des unités de fabrication. L'industrie du cinéma, en revanche, n'était pas favorable à la diffusion de ses films en format numérique sans protection contre la copie. La création d'un nouveau format était l'occasion idéale pour créer un nouveau système de protection. Comme le DVD était destiné à être lu aussi bien dans des appareils électroniques grand public que dans des ordinateurs, l'objectif de sécurité tenait à la création d'un système adapté à ces deux environnements. La protection dans les ordinateurs nécessitait le recours à la cryptographie. L'industrie électronique grand public était réticente à cette approche, considérant qu'un système cryptographique ajouterait de la complexité et des coûts dans ses systèmes.

Le CPTWG (*Copy Protection Technical Working Group*), fondé à cet effet a défini ainsi les objectifs de sécurité :

(47) Traduction de « *compliant* ». cf. *Proceedings of the IEEE*, 87, 7, 1267-1276, 1999, par J. A Bloom, Ingemar J. Cox, T. Kalker, J-P. Linnartz, M. L. Miller, B. Traw.

– Le système devait apporter une protection technique et juridique suffisante pour **aider les gens honnêtes à le rester** (« *keep honest people honest* »), c'est-à-dire difficile à contourner pour un utilisateur moyen ;

– Le système devait apporter une **protection technique et juridique suffisante contre le piratage fatal**, c'est-à-dire contre les moyens permettant de contourner la protection ;

– Le système devait pouvoir être **implanté dans les appareils électroniques grand public et dans les ordinateurs, sans être coûteux ni pesant** dans le fonctionnement courant ;

– Les **licences devaient apporter une protection juridique au système** sans être coûteuses ;

– Le système devait être **transparent** lors de la lecture par les consommateurs.

Le **CSS (*Content Scramble System*)** a constitué la réponse globale au cahier des charges de sécurité du CPTWG. Il est issu d'abord de *Matsushita* et *Toshiba* qui proposèrent un système spécifique et breveté répondant aux objectifs de sécurité et fut ensuite allégé pour répondre aux demandes du secteur de l'industrie de l'informatique qui souhaitait pouvoir décompresser les signaux MPEG-2 avec le microprocesseur. Le CSS comprend les principaux dispositifs suivants :

– **Un système hiérarchique de clefs** : les données sont chiffrées avec des clefs de secteurs variables, elles-mêmes chiffrées avec une clef de disque, elle-même chiffrée par un ensemble d'environ 400 clefs « de fabricants » (dans un schéma similaire au système de gestion de clefs à sens unique évoqué précédemment) ;

– **Une longueur de clefs de 40 bits**, en raison de la réglementation américaine restreignant l'exportation de systèmes cryptographiques, tous les chiffrements étant exécutés avec le même algorithme ;

– **Une transmission chiffrée de clefs** : le lecteur de DVD transmet ses clefs à l'application de lecture dans un tunnel chiffré avec une clef de session.

Encadré 2.1. — La réglementation du contrôle des exportations des armes conventionnelles et des biens à double usage (civil et militaire).

Suite à la fin de la guerre froide, cette réglementation a été assouplie dans le cadre de l'accord de *Wassenaar*, qui a réuni 33 pays dont les États-Unis, la France mais aussi la Fédération de Russie en 1996. Les exportations ont été notamment autorisées pour les systèmes grand public qui n'utilisent pas d'algorithme symétrique avec des clés de longueur supérieure à 64 bits. L'Union Européenne a adopté ces dispositions par le règlement n° 1334/2000 du Conseil du 22 juin 2000. En décembre 2001, une nouvelle réunion des pays participant à l'accord a levé la restriction sur la longueur des clés. Ceci devrait être prochainement transposé en droit européen.

Le CSS fait l'objet d'un brevet dont la gestion des licences a été confiée à la DVD CCA (*DVD Copy Control Association*). Les licences sont accordées gratuitement, à condition que les appareils de lecture soient conformes aux dispositifs suivants de protection des droits :

– **Une mesure technique de contrôle de copie numérique** : CGMS (*Copy Generation Management System*) comprenant deux bits pouvant prendre 4 valeurs : *copy_never* (pas de copie), *copy_once* (une copie), *copy_no_more* (plus de copie), *copy_free* (copie libre), en numérique ou en analogique. C'est l'équivalent vidéo du SCMS (*Serial Copy Management System*).

– **Une mesure technique de contrôle de copie analogique et de copie dégradée**, précisément d'activation par un système de pbit — alternative ou cumulative – des protections développées par *Macrovision* : la protection de la copie analogique APS (*Analog Protection System*), la dégradation de la copie par l'application du dispositif *Colorstripe.*

– **Une mesure technique d'identification :** chaque DVD est pourvu d'un identifiant unique pour contrôler les éventuelles copies.

– **La gestion du zonage géographique**.

Encadré 2.2. — Problématiques techniques du piratage du CSS.

Le CSS a été cassé une première fois en 1999 par un étudiant norvégien, dans le cadre d'un projet qui visait à concevoir un lecteur de DVD pour Linux (système d'exploitation pour les PC proche d'Unix). L'algorithme du CSS a été découvert en décompilant un logiciel de lecture de DVD, conforme mais insuffisamment sécurisé. Un logiciel, nommé DeCSS, a été écrit et permet de lire un DVD vidéo et de stocker le contenu déprotégé sur disque dur. Depuis, des cryptanalyses ont montré que l'algorithme avait plusieurs failles, faisant tomber la complexité de l'attaque de 2^{40} à 2^{25}, puis 2^{16} et 2^{8}, soit une fraction de seconde de calcul pour un PC. Un autre programme, consistant en sept lignes de code Perl, a également été proposé par des chercheurs de MIT (*Massachusset's Institute of Technology*).(48)

Cet exemple amène à tirer les conclusions suivantes :

– Le système de licence peut paraître curieux puisqu'elles sont gratuites. En fait c'est un moyen juridique intéressant permettant d'obliger les fabricants de systèmes de lecture à commercialiser des systèmes conformes. **Sans licence, les systèmes de lecture sont une contrefaçon** ;

– Dans les systèmes hiérarchiques de clefs, il est nécessaire que les algorithmes de chiffrement, au moins en haut de la hiérarchie, soient éprouvés ;

– **L'évolution de la réglementation de la cryptologie dans le sens de la libéralisation doit continuer d'évoluer vers plus de souplesse pour permettre l'utilisation de clefs de longueur satisfaisante** ;

– U**n piratage fatal comme le *DeCSS* n'implique pas par lui-même la fin de l'efficacité de la mesure technique** à l'égard de la très grande majorité des utilisateurs ; il enjoint en revanche un renouvellement de la mesure technique.

– La sécurisation du DVD Audio.

Si le CSS souffrait de faiblesses, l'architecture globale du système est cependant exemplaire. Elle a ainsi été reprise dans le cadre de la **proposition CPPM** (*Copy*

(48) Sur les aspects juridiques. (cf. 2e partie. 2.2.2.)

Protection of Pre-recorded Media) **proposée par le groupe 4C pour la protection des DVD audio**, avec les améliorations nécessaires tirées de l'expérience malheureuse du CSS. Ainsi, le système devrait reposer sur l'algorithme C2 (*Cryptomeria Cipher*), avec des clés de 56 bits. L'équivalent de l'ensemble des clés de fabricants deviendra un ensemble appelé KMB (*Key Management Block*) comprenant 16 colonnes de 3000 clés (soit 48 000 clés, au lieu de 400 pour le CSS), ce qui devrait permettre une gestion effective des révocations.

Enfin, par rapport à d'autres systèmes de cryptographie, utilisés notamment pour la diffusion de contenus par Internet ou par télédiffusion, la faiblesse majeure du CSS correspond à l'impossibilité de renouveler la protection, aggravée par les faiblesses initiales de l'algorithme qui n'a pas permis de mettre en place le schéma prévu de révocation.

ii. L'exemple de DVB.

Le DVB (norme de la télévision numérique) fait partie, avec le GSM, des quelques grandes normes européennes qui finissent par s'imposer au plan mondial. Le système de protection défini dans le cadre de DVB s'appuie sur une architecture à trois niveaux :

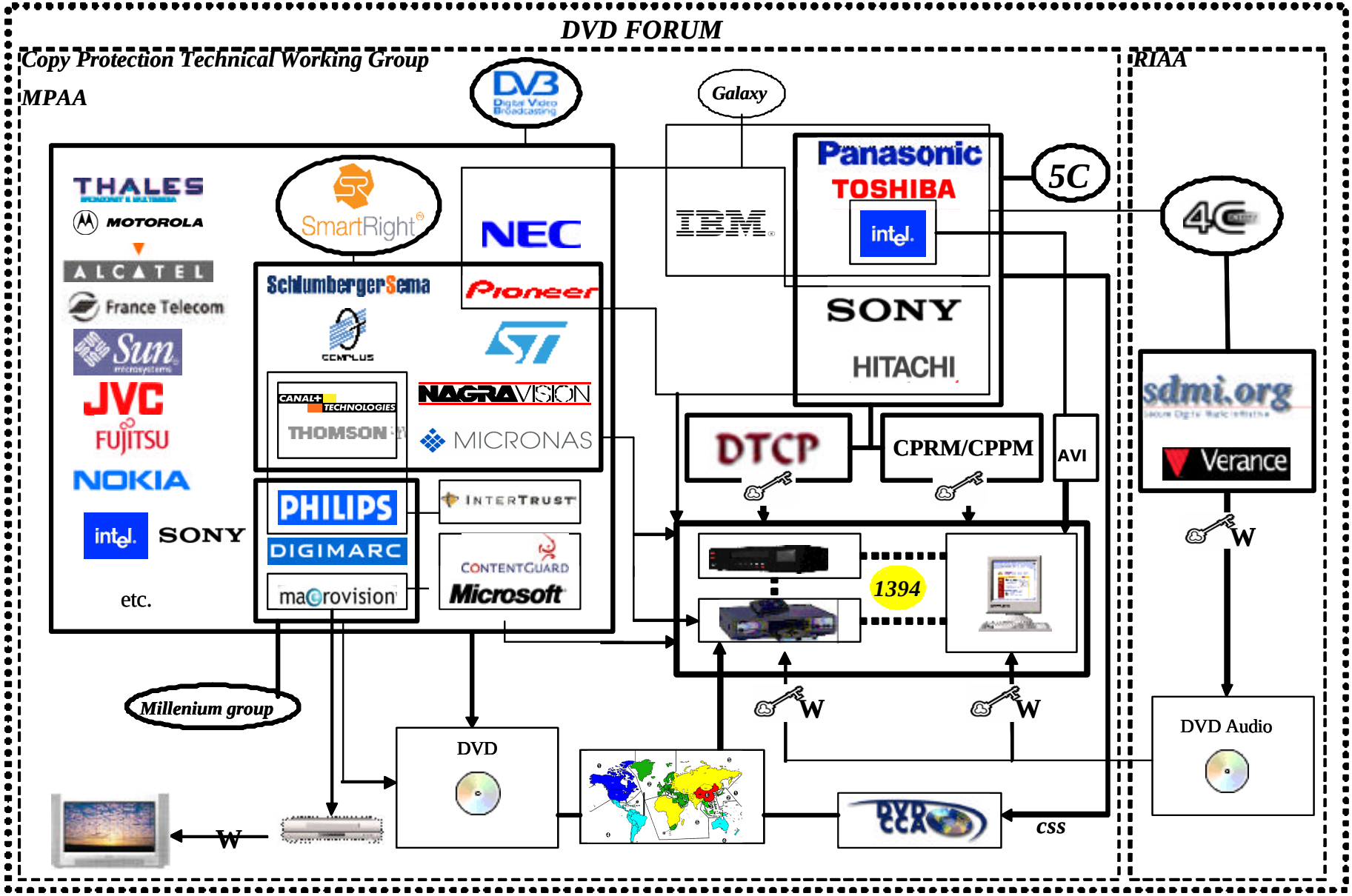
– Le contenu est chiffré, avec une clé appelée « mot de contrôle » (*Control Word*) et un algorithme qui est généralement le Triple DES, la clé pouvant aller jusqu'à 168 bits ;

– Le « mot de contrôle » est transporté chiffré dans un message de contrôle appelé ECM (*Entitlement Control Message*) ;

– La clé de chiffrement de l'ECM ainsi que les informations nécessaires à la gestion des droits de l'utilisateur sont transportées chiffrés dans un message appelé EMM (*Entitlement Management Message*).

DVB a également défini une interface commune (*Common Interface*) qui permet de traiter les données relatives aux messages ECM et EMM sur un système amovible (comme une carte PCMCIA), qui peut lui-même contenir une carte à puce. Cela donne la liberté aux opérateurs de mettre en place le système avec le niveau de sécurité qu'ils souhaitent et si nécessaire de le faire évoluer, soit en changeant la carte à puce pour changer les clés, soit même en changeant le système amovible s'il s'avère que les algorithmes utilisés ont une faille.

Fig. 2.7. – L'univers industriel de la protection du DVD



2.1.3.2. Authentification et signature électronique.

La signature électronique est définie par l'article 1316-4 du Code Civil, comme « *un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* ».[49] Les *DRMS* et les mesures techniques de protection sont susceptibles de faire appel à la signature électronique ou à ses briques technologiques à des fins d'identification des œuvres ou à des fins d'authentification d'un utilisateur.

i. La signature électronique.

La signature électronique s'appuie sur des « *données de création de signature électronique* », qui sont les données propres au signataire, et un « *dispositif de création de signature électronique* ». Elle peut être vérifiée par des «*données de vérification de signature électronique* » et un dispositif de vérification de signature électronique ».[50].

Cette définition est large, mais dans la pratique, les dispositifs de création de signature électronique font appel aux algorithmes de cryptographie asymétrique, qui sont dans ce cas utilisés en sens inverse par rapport à l'usage qui en fait pour leurs fonctions de confidentialité :

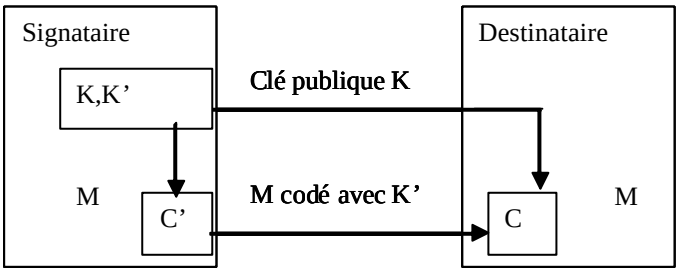
– le signataire code le message avec sa clef privée K' (données de création de signature), qu'il doit conserver secrète ;

– le signataire transmet sa clé publique authentifiée (données de vérification de signature) au destinataire afin qu'il puisse vérifier la signature.[51]

A

Ainsi, dans la mesure où les clés K et K' sont associées de manière unique, le signataire est le seul à pouvoir coder des messages qui pourront être décodés avec sa clef publique K.

Fig. 2.8. – Signature électronique.



Ce schéma suppose de pouvoir authentifier la clé publique K, afin de pouvoir établir le lien entre K et l'identité du signataire. Ceci est réalisé par **l'utilisation de certificats, dont c'est la fonction et qui sont délivrés par des prestataires de services de certification, également appelés «*autorité de certification* » ou dans un sens plus large « *tiers de confiance* »**. Cette dernière appellation résume le rôle des prestataires de

[49] Ajouté par la loi n° 2000-23 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, qui transpose la Directive 1999-1993/CE du Parlement Européen et du Conseil.

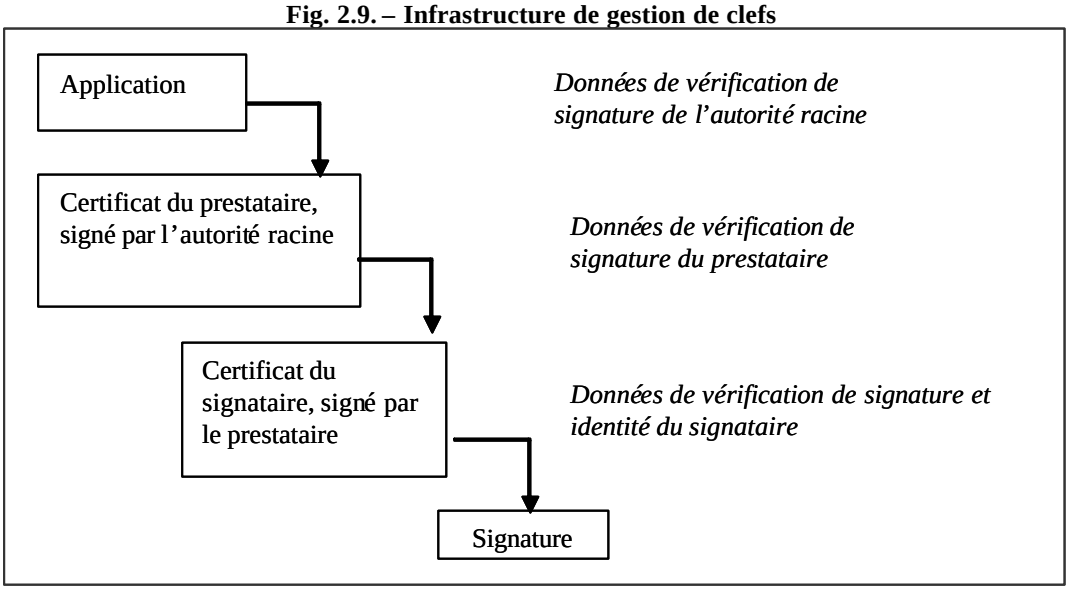
[50] Décret n° 2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique

[51] On n'utilise pas les mêmes clefs pour les fonctions de signature et de confidentialité.

services de certification, destinés à permettre la confiance dans un échange : le prestataire enregistre l'identité du signataire et lui délivre un certificat comprenant son identité, signé par le prestataire.[52] Le problème est donc concentré dans la vérification de la signature du prestataire. En général, le prestataire fait lui-même référence à une autorité « racine », qui lui délivre un certificat. Les certificats de ces autorités racines peuvent alors être enregistrés dans les applications (par exemple les navigateurs Internet).

Les divers certificats nécessaires à la vérification de la signature peuvent être fournis par le signataire lui-même ou bien par le prestataire. Dans ce dernier cas, le prestataire doit gérer une **infrastructure de gestion de clefs** (IGC ou PKI – *Public Key Infrastructure*), qui correspond à une base de données sécurisée des certificats qu'il a délivrés.

Fig. 2.9. – Infrastructure de gestion de clefs



Dans le cadre de la protection des œuvres, l'émetteur peut être lui-même sa propre autorité de certification et gérer une infrastructure de gestion de clés en interne, se contentant par exemple de relier des données de vérification de signature à une identité réduite à un numéro de compte d'abonné ou un numéro de carte bancaire.

ii. Fonctions de hachage.

Dans la mesure où la signature électronique utilise des algorithmes asymétriques qui sont assez lents, le signataire ne code pas l'ensemble du message avec sa clé privée mais plutôt un « condensé » du message (*message digest*), obtenu par une fonction de hachage. Afin de garantir l'intégrité du message attaché à la signature du condensé, la fonction de hachage doit avoir certaines propriétés de sécurité, notamment de ne pas pouvoir être inversée : connaissant le condensé, il doit être très difficile de modifier le message d'origine sans que cela ne conduise à calculer un condensé différent.

---

[52] Usuellement ces fonctions sont réalisées dans un format interopérable correspondant à la norme X.509v3 développé conjointement par l'ISO/IEC/ITU (*International Organization for Standardization /International Electrotechnical Commission/International Telecommunication Union*) et l'ANSI (*American National Standards Institute*).

Les fonctions de hachage peuvent également être utilisées à des fins d'identification, d'indexation et de contrôle d'intégrité des contenus (dans ce cas elles prennent le nom de « signature » du contenu, à ne pas confondre avec la signature électronique qui y ajoute l'authentification de l'émetteur ou du titulaire des droits).

Il existe des fonctions de hachage éprouvées, comme MD2, MD5 (*message digest*) ou SHA (*secure hash algorithm*). Des recherches sont en cours pour définir également des fonctions de hachage plus adaptées à certains types de contenus comme l'audio, les images ou la vidéo, qui puissent avoir la souplesse nécessaire pour résister à des manipulations comme la compression, le ré-échantillonnage pour l'audio, l'agrandissement pour les images, etc.

* * *

Les techniques de cryptographie occupent désormais un rôle majeur dans la protection de l'ensemble des contenus numériques, d'une part pour la protection de l'accès, notamment dans le cadre de la distribution, mais aussi pour les supports optiques. Cette présence croissante dans un contexte favorable à la libéralisation de la cryptographie est d'autant plus nette qu'elle s'étend par combinaison à l'autre catégorie principale de technique de protection des œuvres : les techniques de tatouage.

2.2. LES TECHNIQUES DE TATOUAGE.

Les techniques de tatouages, principalement le *watermarking*, mais encore le *fingerprinting*, ont pour objet d'insérer de manière imperceptible des informations (texte, code, etc.) parmi des données numérisées, sous la forme d'un tatouage, d'un filigrane ou d'une empreinte.[53] Initialement, la recherche relative à ces techniques a poursuivi des objectifs de protection des œuvres numérisées. D'une manière générale, les conditions d'application de ces techniques ou leur nature propre les font désormais plutôt poursuivre des objectifs d'identification, d'authentification, d'intégrité ou de traçabilité des œuvres, en particulier à travers le tatouage de l'information sur les droits.

2.2.1. PRINCIPES DES TECHNIQUES DE *WATERMARKING*.

Appliquées aux œuvres numérisées, ces techniques constituent un ensemble de mesures techniques caractérisées par le fait que **les filigranes, empreintes ou tatouages sont rendus indissociables des données ou du signal numériques dans lequel l'œuvre est codée**, qu'il s'agisse d'une image, d'un flux audio ou vidéo, de texte, etc. Elles peuvent être rendues « imperceptibles » par exemple par la « steganographie ».

2.2.1.1. Objet des techniques de *watermarking*.

Ces procédés peuvent avoir pour fonction la protection des œuvres par création d'un filigrane ou le transport avec l'œuvre d'information sur les droits relatifs à celle-ci, par empreinte. Elles offrent en amont de ces applications une fonction principale d'une autre nature : **l'authentification de l'objet numérique et de son intégrité**. Le *fingerprinting* consiste à superposer plusieurs tatouages sur une même œuvre, apposés à chaque traitement ou copie de l'œuvre. Cette technologie permet ainsi la traçabilité de l'œuvre, le contrôle par identification de la diffusion des œuvres. **Le *watermarking* comme signature numérique** permet l'administration de preuves quant à l'intégrité, l'origine, voire la titularité s'il porte sur le régime des droits des œuvres, le contrôle de la reproduction, la vérification des modifications d'informations ou d'altérations des œuvres, etc.

La neutralité du *watermarking* aux différentes applications qui peuvent en être faites explique que, pour répondre à l'objectif de protection des œuvres, cette technique a dû, d'une part évoluer dans le sens d'une complexité croissante, d'autre part, tirer parti, sinon des techniques mêmes de cryptographie, du moins de la cryptologie.

Par nature, le *watermarking* n'est donc pas prioritairement une technologie de protection des œuvres, mais les principales applications initialement développées ont consisté à répondre à cet objectif. En dépit des progrès réalisés en terme de protection, la persistance des insuffisances de ce type d'application conduit d'une part à ne pouvoir que l'associer à d'autres mesures techniques de protection, notamment cryptographiques, voire à s'engager dans des applications n'ayant plus un objectif direct de protection.

---

[53] La stéganographie qui emprunte aux techniques de *watermarking* désigne plutôt un usage de ces techniques pour l'échange d'informations dissimulées.[http://www.watermarkingworld.org/] et les liens présentés.

2.2.1.2. Méthode.

Techniquement, le *watermarking* consiste à ajouter une quantité d'informations numériques au signal (audio, vidéo, image, texte, etc.) par un algorithme de codage ou « tatoueur ». **Cet ajout doit, pour avoir une signification technique et économique dans les industries culturelles, offrir des qualités de robustesse au sens où les signaux peuvent avoir à subir des transformations nombreuses et variées** par leurs natures : compression, étirement, rotation, ajout de bruit, ré-échantillonnage, etc. qui ne doivent pas altérer le tatouage même.

Le volume d'informations est en pratique fonction de la nature du signal, par exemple en général de l'ordre de 64 bits pour un flux vidéo de quelques secondes ou une image de taille importante qui permettent une quantité d'informations utiles. Or, ce volume d'informations, objet du filigrane, doit répondre à des objectifs contradictoires :

– **un objectif d'imperceptibilité pour ne pas déformer l'œuvre ou sa perception ;**

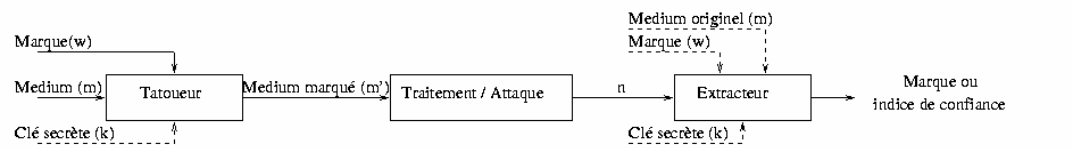
– **un objectif de résistance aux attaques qui implique une quantité substantielle d'informations tatouées.**

Les algorithmes de tatouage ont connu des évolutions importantes pour répondre à l'objectif de sécurité. L'idée générale consiste à introduire un biais dans la répartition statistique des données numériques des œuvres. Ce biais statistique sert à coder l'information que l'on veut dissimuler, tout en étant très peu visible. Les méthodes d'introduction du biais statistique sont variées et dépendent notamment de la nature des œuvres : images, flux audio ou vidéo.[(54)]

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

– une clef secrète de tatouage, qui permet à l'éditeur d'insérer le tatouage dans l'œuvre ;
– une clef de lecture qui permet de décrypter le tatouage.

Fig. 2.10. – Watermarking et cryptologie



Source : M. Brunet et F. Raynal, le Watermarking à l'INRIA [http://www-rocq.inria.fr/codes/Watermarking/]

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

2.2.2. APPLICATIONS DU *WATERMARKING* A DES FINS DE PROTECTION.

Les usages des techniques de tatouage comme mesures de contrôle d'actes autorisés par les titulaires de droits sont principalement de trois ordres : le contrôle d'enregistrement et le contrôle de lecture, mais leur fragilité et leur difficulté de mise en œuvre conduit surtout à développer des usages relatifs au régime des droits. Il s'agit aussi d'un double usage d'une mesure technique qui peut cumuler une double protection juridique comme mesure technique de contrôle de l'utilisation des droits et comme technique d'identification relative au régime des droits.

2.2.2.1. Points d'application et points faibles.

Différentes approches ont été considérées afin d'utiliser le *watermarking* pour la protection des contenus. Elles s'appuient généralement sur un contrôle d'enregistrement ou de lecture. **Au moment de l'enregistrement**, un détecteur de *watermarking* peut bloquer l'enregistrement des œuvres contenant un *watermarking* indiquant qu'elles sont protégées. **Au moment de la lecture**, on peut combiner deux *watermarking* : un *watermarking* robuste indiquant que l'œuvre est protégée et un *watermarking* fragile. La lecture est autorisée pour les contenus contenant les deux *watermarking*, qui correspond à une utilisation licite de l'œuvre, ou pour les contenus ne contenant pas de *watermarking* (contenus non protégés ou autoproduits). En revanche, le *watermarking* fragile est conçu pour disparaître lors de la manipulation du contenu, notamment lors d'une compression pour transmettre le contenu par Internet (cas SDMI) ou lors de la copie (cas SACD). Après la compression, le *watermarking* robuste indiquant que l'œuvre est protégée sera toujours là, mais pas le *watermarking* fragile : la lecture de l'œuvre est alors bloquée. **L'intérêt de cette dernière approche est qu'elle ne vise pas directement les pirates mais plutôt à bloquer l'utilisation des contenus piratés chez l'utilisateur moyen, ce qui réduit le niveau d'exigence en terme de robustesse.**

Dans ce contexte, le *watermarking* souffre cependant de plusieurs faiblesses, notamment par rapport aux techniques cryptographiques :

– Alors qu'il est facile de renforcer la robustesse des systèmes cryptographiques, en allongeant la longueur des clés, en améliorant la résistance au «tripatouillage » des logiciels ou des composants électroniques (carte à puce), si toutefois on accepte d'en payer le coût, **les techniques visant à améliorer la robustesse du *watermarking* sont limitées**. **La quantité d'informations tatouables dans un contenu est limitée et pourrait même diminuer avec les progrès des techniques de compression** qui poursuivent un but contraire, car elles visent à réduire l'information non directement utile à la qualité du contenu, catégorie dans laquelle rentre le *watermarking.*

– La mise à disposition d'un détecteur de *watermarking* le fragilise beaucoup. En effet, l'utilisation du *watermarking* à des fins de protection technique suppose que les dispositifs de lecture ou d'enregistrement contiennent un détecteur de *watermarking*, que les pirates pourront donc utiliser à des fins d'analyse. Dans l'hypothèse où il existe des contenus non protégés (cas des contenus autoproduits), des travaux de recherche semblent démontrer qu'un tel dispositif présente une faible robustesse et n'est pas adapté. [55]

[55] T. Kalker, *Watermark Estimation Through Detector Observations, Benelux Signal Processing Symposium*, mars 1998.
[http://www.intec.rug.ac.be/Research/Groups/hfhsdesign/viva/publications/bsps98.pdf]

Les premières générations de tatouages ont donc été systématiquement attaquées avec succès, y compris des produits de tatouage d'entreprises disposant de brevets très spécifiques et d'un niveau élevé de recherche. Les analyses d'évaluations des systèmes de *watermarking* semblent conclure aux mêmes résultats décevants en termes de protection, qu'il s'agisse d'attaques concernant le marquage d'images, du signal vidéo ou du signal audio, y compris par des méthodes d'attaques relativement simples.[56]

Encadré 2.3. — Le SDMI *challenge*

Le 6 septembre 2000, L. Chiariglione, alors Directeur du consortium SDMI (*Secure Digital Music Initiative* qui réunit plus de 200 sociétés et organisations représentant les technologies de l'information, les constructeurs de matériel électronique, les entreprises de sécurité informatique, l'industrie du disque, et des fournisseurs d'accès à Internet)[57] a invité les « hackers » à tenter de casser les mesures de techniques de protection développées. L'essentiel des couches de protection fondée sur des technologies de *watermarking* a été attaqué valablement le 28 novembre. [58]

Les évaluations des techniques de *watermarking* sont sans doute insuffisantes, mais laissent paraître une certaine fragilité en terme de robustesse aux attaques.[59] Cette vulnérabilité est apparue notamment à l'occasion du défi lancé aux chercheurs et plus largement aux hackers par le *SDMI.*

Encadré 2.4. — Deux projets européens de recherche : *Certimark*, *Talisman*

Le projet *Certimark* [60] qui a réuni notamment des acteurs nationaux comme l'INA, *Netimage*, Thomson CSF, Eurecom, la SACD s'est déroulé de mai 2000 à juillet 2002. Il a conçu et mis au point un système d'évaluation des procédures de mises en œuvres de protections techniques fondées sur le *watermarking*. Les objectifs de certification permettent principalement des applications validées de *watermarking* pour le contrôle de diffusion, l'identification et l'authentification des œuvres. *Certimark* constitue donc un outil d'évaluation à côté de produits comme *Stirmark*.

Le projet *Talisman* (*Tracing Authors'rights by Labelling Image Services and Monitoring Access Network*)(61) qui s'inscrivait dans le Programme IST, travaille à la création d'outil de protection contre les copies illicites de supports numériques. Le projet s'appuie sur une analyse des aspects juridiques et institutionnels des droits, (organisations, titulaires, etc.) comme des modes de circulations des œuvres, pour définir un cadre de contrôle et de protection des œuvres. Le projet, par des technologies de *watermarking*, doit atteindre les objectifs suivants : protection vidéo, authentification des titulaires et contrôle de la circulation des œuvres selon les terminaux.

---

(56) F. A. P. Petitcolas, *Le copyright numérique : encore beaucoup de progrès à faire*, Liaison n° 6, août 1998. [http://www.cl.cam.ac.uk/~fapp2/publications/liaison6-filigrane.doc] ; F.A. P. Petitcolas, R. Anderson. *Weaknesses of copyright marking systems*, M*ultimedia and security workshop*, 1998. [http://www.cl.cam.ac.uk/~fapp2/publications/acm98-weaknesses.doc]

(57) *Secure Digital Music Initiative* (SDMI) [http://www.sdmi.org/index.htm]

(58) Le système de protection a notamment été déjoué par le département informatique de l'Université de Princeton : S. A. Craver, M. Wu, B. Liu, A. Stubblefield, B. Swartzlander, D. W. Wallach, D. Dean, E. W. Felten, *Reading between the lines, the lessons from the SDMI Challenge, Proc. of 10 th USENIX Security Symposium, August 200.* [http://www.usenix.org/events/sec01/craver.pdf]

(59) F. Petitcolas, *Watermarking schemes evaluation*, E.E.E. Signal Processing, 2000 [http://www.cl.cam.ac.uk/~fapp2/publications/ieeespm00-evaluation.doc]

(60) Certimark [http://vision.unige.ch/certimark/public/public.html]

(61) Talisman, *Tracing Authors'rights by Labelling Image Services and Monitoring Access Network* [http://www.tele.ucl.ac.be/TALISMAN/index.html]

2.2.2.2. Les usages de gestion.

Les techniques de tatouage permettent de réaliser une gestion numérique des droits, en inscrivant la représentation des droits sur le tatouage de l'œuvre elle-même.

L'une des fonctions les plus intéressantes pour la gestion numérique des droits des techniques de *watermarking*, par exemple pour **la gestion du nombre de copies autorisées à partir d'un support, est très vulnérable aux attaques des systèmes électroniques de lecture de l'œuvre**. Par exemple, pour le respect par *watermarking* du régime de gestion des droits relatifs au nombre de copies autorisées de DVD, il faudrait s'assurer voire certifier que les lecteurs de DVD commercialisés « brûlent » bien les *bits* réservés à cet effet par le *watermaking*, selon le nombre de copie réalisé. Cela paraît difficilement compatible avec l'approche « no mandate » défendue par l'industrie. Dans le cas supports comme le CD Audio ou le DVD, pour lesquels la question du *watermarking* n'a pas été envisagée dès le début, l'existence d'une base importante de systèmes de lecture ou d'enregistrement non conformes est rédhibitoire pour la mise en place a posteriori d'une protection de ces contenus par des techniques faisant appel au *watermarking*.[(62)].

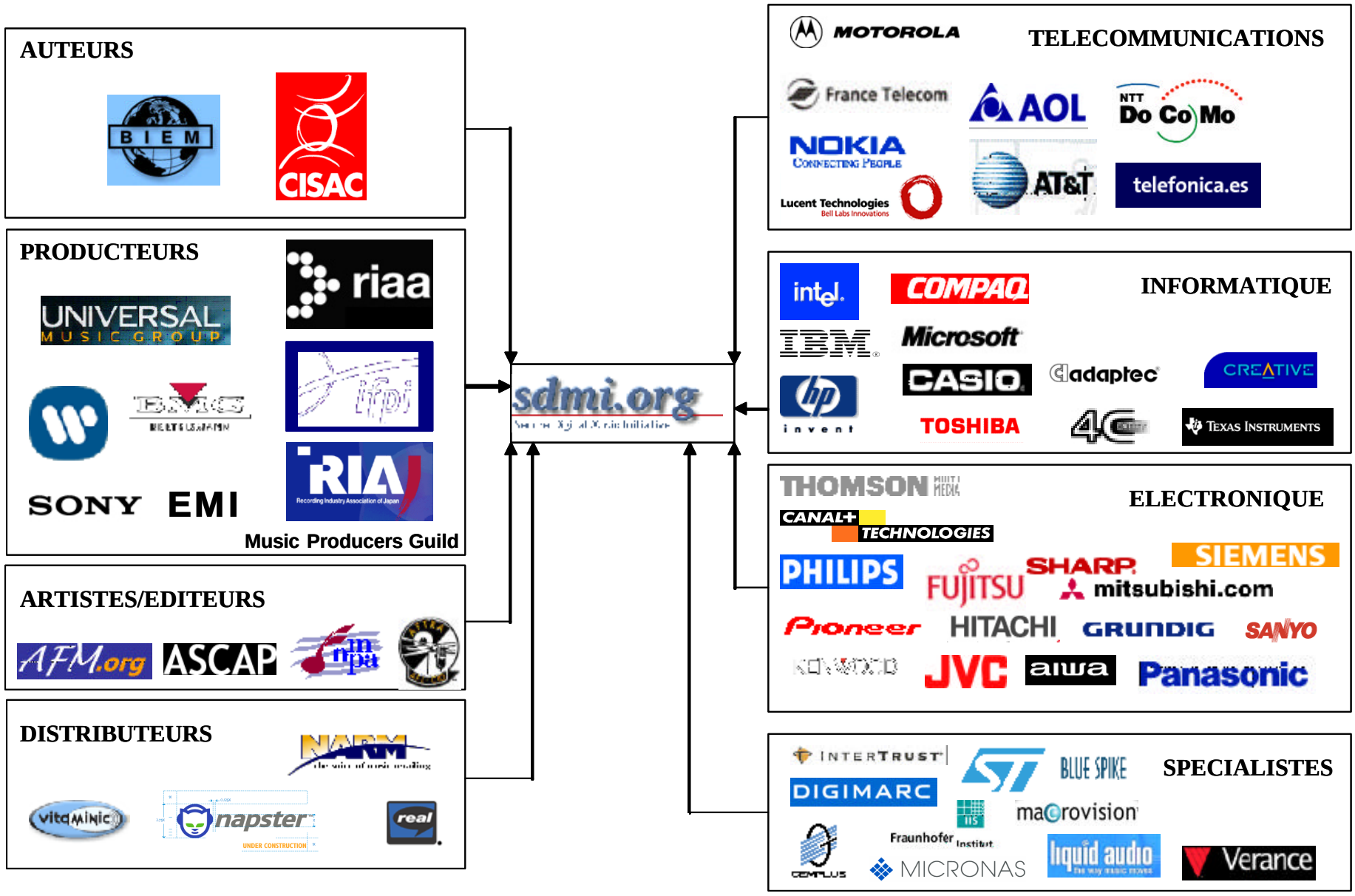
Toutes ces fragilités ne mettent pas seulement en cause la fonction de protection des techniques de protection qui peut être assurée par un système de différentes mesures de protection techniques, mais des fonctions moins sensibles, comme l'authentification et la probation. Par exemple, les filigranes qui ont été produits sans répondre au critère de non-réversibilité peuvent être employés pour que plusieurs personnes attestent de l'originalité d'un enregistrement d'une œuvre.

Dans ces conditions, les techniques de *watermarking* doivent bien pouvoir être employées comme une couche parmi d'autres de mesures de protection technique notamment cryptographiques. Elles doivent surtout s'intégrer dans des mécanismes institutionnels mais aussi techniques d'évaluation voire de certification. Ce sont ainsi développés des outils ou des entreprises qui poursuivent cet objectif.[(63)] En effet, cette évolution apparaît nécessaire parce que **l'apport principal de ces techniques est de l'ordre de la preuve numérique en ce qui concerne l'intégrité, l'authentification, la datation, etc. Ces évolutions sont d'autant plus probables que les techniques de *watermarking* sont loin de ne devoir être utilisées que pour la protection de la propriété intellectuelle**. Elles intéressent par exemple le domaine de la santé (imagerie médicale), l'administration de documents, etc. donc davantage des applications de services.

[(62)] cf. *Final Report of the Co-Chairs of the Broadcast Protection Discussion Subgroup to the Copy Protection Technical Working Group*, juin 2002, notamment points 5.6 et 5.7. [http://www.mpaa.org/Press/Broadcast_Flag_BPDG.htm]

[(63)] Optimark [http://poseidon.csd.auth.gr/optimark/] *Stirmark benchmark* [http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/index.html], *Checkmark* [http://watermarking.unige.ch/Checkmark/].

Fig. 2.11. – La protection de l'audio : le SDMI.



2.2.2.3. Applications des techniques de *fingerprinting*.

L'absence de fonctionnalités élevées en termes de protection des œuvres ne conduit pas à l'absence d'utilité de ces techniques pour la propriété intellectuelle au sens large. Un certain nombre d'entreprises ou d'organismes, au plan national et mondial développement de nouveaux usages.[64]

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

L'identification d'un pirate peut conduire à des poursuites judiciaires. Cette réaction ne paraît cependant pas très adaptée, tant par la difficulté à conférer au *fingerprinting* le statut juridique de preuve qu'à cause du délai d'aboutissement d'une telle action, sauf peut-être à des fins de dissuasion. Au regard des difficultés rencontrées par exemple par les opérateurs de télévision à péage dans l'identification des systèmes pirates et au coût des opérations générales de renouvellement des cartes à puce, **cette identification peut-être beaucoup plus intéressante à des fins techniques, comme contribution au maintien de la protection par la révocation des systèmes pirates et le renouvellement des clés ou des systèmes compromis.** Le cadre le plus adapté à une telle application est celui des services interactifs, pour lesquels il est possible d'appliquer le *fingerprinting* à la source, avant diffusion. **Cela fait du *fingerprinting* un outil très complémentaire de la cryptographie.**

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

Encadré 2.4. — *Thalès/Nextamp* : l'identification à des fins de traçabilité

La société *Nextamp*[65], issue d'un essaimage de *Thalès* [66], propose des solutions de *watermarking* en temps réel de flux vidéo numérique (MPEG2). Ces solutions devraient principalement être utilisées à des fins de traçabilité, notamment pour le suivi d'audience et le contrôle des rediffusions dans le cas de la télévision. Un partenariat pourrait être monté avec la société *Médiamétrie* à cet effet. Ce système pourrait également à la traçabilité de la chaîne du cinéma numérique.

(64) Pour la France : *Thomson*, *Thalès*, *Netimage*, *INRIA*, *ENST*, etc. ; dans le monde : *Intertrust* [http://www.intertrust.com/] ; Macrovision [http://www.macrovision.com/] ; Datamark [http://www.datamark.co.uk/] ;Digital Watermark [http://www.digital-watermark.com] ; DCT Group [http://www.dct-group.de/] ; DIGIMARC [http://www.digimarc.com/] ; Philips [http://www.research.philips.com/password/pw5/pw5_10.html] ; Verance [http://www.verance.com/], etc.

(65) *Nextamp* [http://www.nextamp.com/].

(66) *Thalès* [http://www.thalesgroup.com/ga/business_zone/solutions.htm].

Fig. 2.12. – L'univers du *watermarking*

2.3 AUTRES SYSTÈMES DE PROTECTION.

D'autres systèmes de protection contre la copie ont été ou sont en cours de mise en place par les producteurs. Il s'agit notamment des systèmes de protection contre la copie analogique de la vidéo et les divers systèmes de protection des CD Audio qui sont apparus depuis l'année 2001.

Ces systèmes se situent dans une approche radicalement différente des systèmes précédemment évoqués. En effet, les systèmes de protection utilisant la cryptographie ou le tatouage se fondent sur la création d'un périmètre sécurisé, qui nécessite que la protection soit conçue en même temps que le système de lecture des œuvres, puisque celui-ci devait intégrer les éléments de contrôle correspondant à la protection. La protection repose ensuite sur la conformité des appareils au système de protection défini.

Par rapport à cette approche, les autres systèmes de protection partagent la caractéristique d'avoir été conçu après les systèmes de lecture ou d'enregistrement, sur la base d'une exploitation de leurs défauts.

2.3.1. PROTECTION CONTRE LA COPIE ANALOGIQUE DE LA VIDÉO.

Il s'agit ici principalement des systèmes conçus et commercialisés par l'entreprise *Macrovision*. [67]

– Le système APS (*Analog Protection System*) est fondé sur la présence d'un circuit électronique de contrôle automatique de gain dans les magnétoscopes (AGC – *Automatic Gain Control*). Le circuit AGC a pour fonction d'ajuster la luminosité de l'enregistrement sur un magnétoscope, mais il n'existe pas sur les téléviseurs. Dans le signal analogique vidéo, il existe un délai de quelques millisecondes entre deux balayages de l'écran, pendant lequel le signal ne produit aucune image visible. Le système APS consiste alors à ajouter périodiquement une forte impulsion dans ce délai invisible, comme si l'image devenait d'un coup très lumineuse. Le contrôle automatique de gain réagit alors en abaissant la luminosité, sur une durée qui empiète sur les images suivantes. Ces images apparaissent donc très foncées sur la copie réalisée, rendant l'enregistrement inutilisable.

– Un second système a ensuite été conçu, baptisé « *Colorstripe* », qui perturbe le signal couleur enregistré par le magnétoscope , mais pas celui affiché par le téléviseur.

Initialement, le système APS a été utilisé sur les **cassettes VHS** (location et vente), sur lesquelles on enregistrait le signal analogique avec les impulsions. Pour les DVD, il n'était plus possible d'enregistrer ces impulsions en codage numérique. Il a donc été prévu que les lecteurs de DVD devraient inclure un circuit créant la protection APS sur leur sortie analogique. **Les DVD enregistrés comprenaient alors un signal destiné à activer le système.** Cela permettait à *Macrovision* de se rémunérer non seulement sur les ventes de lecteurs DVD mais également sur les ventes de DVD. Un système similaire est également implanté sur les décodeurs numériques de télévision *pay-per-view*, mais il

[67] Présentation de M. Belinsky, *Macrovision*, devant le '*Committee on the Judiciary*', 17 septembre 1997 [http://www.house.gov/judiciary/4021.htm].

semblerait que les opérateurs aient un différend avec les titulaires de droits à ce sujet, refusant d'activer ce système tant que la fenêtre calendaire de diffusion en *pay-per-view* ne se rapprochait pas significativement de celle du DVD.

Macrovision avait mis en œuvre une stratégie de protection juridique originale, consistant à breveter les systèmes de contournement possibles. Malgré cela, de nombreux systèmes de contournement sont apparus, sous la forme de petits boîtiers électroniques généralement appelés « stabilisateurs vidéo ». Le *DMCA* a ensuite renforcé cette protection juridique (cf. 2e partie de l'étude).

2.3.2. LES SYSTÈMES DE PROTECTION DES CD AUDIO.

L'année 2001 a vu apparaître un certain nombre de CD Audio protégés contre la copie, avec des mécanismes proposés par quelques sociétés spécialisées, *Macrovision* qui a acquis récemment *Midbar* dans ce but, *SunnComm*, *Key2audio*.

En fait ces mécanismes vont beaucoup plus loin que la protection contre la copie, puisqu'ils ont généralement pour effet d'empêcher la lecture normale du CD Audio sur un PC avec les outils habituels. Comme les graveurs de CD Audio de salon (hors PC) sont relativement moins répandus que les graveurs PC et qu'ils contrôlent les copies avec le système *SCMS*, ceci devait avoir pour effet de fortement limiter les copies sur support optique et de supprimer les copies *MP3*.

Les premières générations de ces mécanismes ont rencontré un certain nombre de difficultés :

– **des problèmes de compatibilité ou « jouabilité »** : les CD Audio ainsi protégés fonctionnaient mal dans certains lecteurs, que ce soient des lecteurs de CD Audio dans des lecteurs de CD Audio dans les voitures, des lecteurs de DVD, des lecteurs de consoles de jeux, ou bien sûr, des lecteurs PC ;

– **des problèmes d'information des consommateurs**, qui ont eu le sentiment d'avoir été mal informés sur les caractéristiques du produit : les limites posées à l'utilisation normale des CD Audio par ces mécanismes n'ont pas toujours été précisées clairement, tant en terme de lecture que de copie privée :

– **des problèmes de robustesse**, dans la mesure où un simple masquage avec un feutre ou du ruban adhésif de certaines zones repérables suffisait à ôter la protection d'un de ces mécanismes.

Certains de ces mécanismes exploitent le fait que les lecteurs de CD Audio dans les PC ont été conçus pour lire plusieurs types de CD Audio, aussi bien des CD Audio (avec un codage audio) que des Cédérom (avec un codage de données) ou des CD-R (enregistrable une seule fois, mais multisessions, c'est-à-dire en plusieurs sessions successives d'enregistrement).[68] Le format multisessions implique notamment la possibilité d'inscrire sur un CD-R plusieurs «tables des matières » (TOC — *Table Of Content*), dans lesquelles sont précisés la position des pistes, ainsi que le format du codage — audio ou données.

---

[68] J. Halderman, *Evaluating New Copy-Prevention Techniques for Audio CDs*, ACM — DRM2002 [http://www.cs.princeton.edu/~jhalderm/papers/drm2002.pdf].

Dans les divers CD Audio protégés, il existe plusieurs tables, dont certaines contiennent des erreurs qui ne concernent pas les données habituellement lues par les lecteurs CD Audio de salon, mais qui correspondent seulement à la position des diverses pistes dans la première table, d'où la possibilité de lire les CD Audio dans les lecteurs de salon. **Les procédés utilisés – technologiquement assez rudimentaires – consistent donc à inclure des erreurs** : incohérence entre diverses tables, emplacement de départ erroné (*Midbar*, *Key2audio*), format de données erroné (*SunnComm*). D'autres mécanismes consistent à **inclure des erreurs dans le codage audio**, que les lecteurs de salon savent corriger par interpolation mais qui génèrent des erreurs ou des bugs dans les PC.

Globalement, ces mécanismes reposent sur l'incapacité des lecteurs PC à corriger certaines erreurs, de part leur fragilité intrinsèque qui correspond à leur multifonctionnalité. Ces erreurs sont relativement simples à corriger. Certains systèmes existant ne sont d'ailleurs pas sensibles à cette protection, par exemple le pilote d'un lecteur qui avait été conçu pour savoir bien traiter certaines erreurs ou un logiciel de copie bit-à-bit, qui permet de réaliser certaines copies sur CD-R.[69] Certains constructeurs de lecteurs PC ont également annoncé qu'ils mettraient à jour leurs pilotes, afin de leur permettre de traiter correctement les erreurs.

Dans la pratique, il est certain que les pirates seront capables de contourner ces protections, sans doute dans des délais assez brefs au regard des techniques utilisées : la plupart des titres ainsi protégés se sont ainsi retrouvés sur Internet. **Mais la grande diversité du parc de lecteurs existant ne permettra qu'à peu d'utilisateurs d'avoir accès aux mises à jour des pilotes permettant de corriger les erreurs. Dans ce sens, si ces mesures n'assurent pas une protection très robuste, elles devraient rester relativement efficaces auprès des utilisateurs moyens et limiter les pratiques de copie, au moins durant une période transitoire avant l'émergence de supports optiques audio sécurisés nativement : SACD, DVD Audio.**

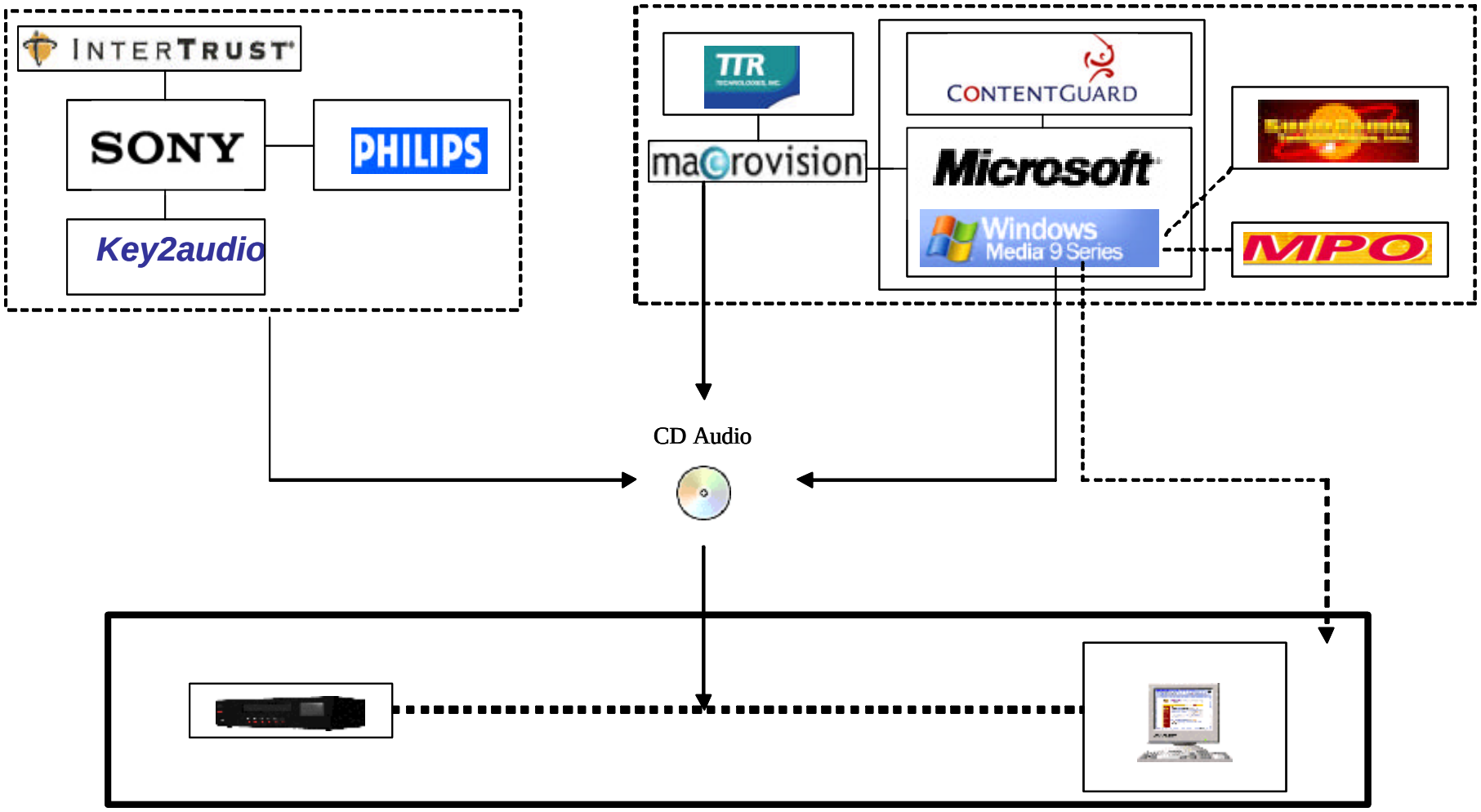
Encadré 2.6. — *SunnComm* : couplage mesure technique – *DRM* pour les CD Audio

Les problèmes rencontrés au démarrage par ces mécanismes ont également fait l'objet de certaines corrections. Afin de renforcer leur acceptabilité par les consommateurs, certains mécanismes prévoient désormais de coupler un système de protection de CD Audio avec un système de *DRM*.

- la solution *MediaMax*, conçue par la société S*unnComm* en partenariat avec *Microsoft*, permet, dans le cadre protégé de *Windows Média 9*, de lire les CD Audio sur un PC, d'effectuer des copies voire d'échanger des titres (dans le cadre du *fair use*).

[69] Le pilote ou *driver* d'une interface est le programme ajouté au système d'exploitation et destiné à gérer les accès à cette interface.

Fig. 2.13. – La protection du CD Audio.



2.3.3. ÉVALUATION PAR MODE DE DISTRIBUTION.

Une comparaison simplifiée des trois principaux supports de diffusion, peut être réalisée quant à l'analyse de leur protection et des risques économiques liés au piratage ou à la contrefaçon. Ces évaluations représentent ce que l'état de la technique permet de faire, sans signifier que tous les systèmes existants sont à ce niveau.

Trois variables peuvent être retenues : **robustesse**, c'est-à-dire résistance aux attaques : **possibilité de renouvellement** de la protection ; **risque économique** lié au piratage.

2.3.3.1. Télévision numérique à péage.

Ce support utilise un décodeur avec carte à puce. L'évaluation suivante est indépendante du mode de diffusion retenu (satellite, câble ou ADSL).

L'attaque de la protection par carte à puce nécessite des moyens matériels coûteux qui restreignent le piratage à des structures organisées avec une motivation commerciale. **La robustesse est donc forte et il est facile de renouveler la protection** en changeant la carte à puce, même si cela a un coût.

Le risque économique du piratage est moyen, puisqu'il correspond à l'arrivée de décodeurs pirates et que la redistribution du contenu est peu probable. Ce risque peut être encore réduit par la mise en place d'une voie de retour (par exemple téléphonique) pour gérer automatiquement le *pay-per-view*, car cela permettra de contrôler les systèmes pirates. Le risque est augmenté si le contenu est transféré sur un ordinateur (mais ce n'est pas le cas avec un disque dur interne au décodeur ou également protégé par une carte à puce).

2.3.3.2. Diffusion payante par Internet.

L'attaque de la protection logicielle est probablement difficile mais cependant accessible à une équipe de pirates motivés, ne travaillant pas dans une logique commerciale.

Il est par contre **très facile de renouveler la protection** en diffusant une nouvelle version. La protection tombe par contre à un niveau comparable à celui des supports optiques si le système permet de fixer le contenu sur support optique (comme le demanderont probablement les consommateurs pour l'audio, afin de pouvoir écouter le contenu dans leur salon ou leur voiture), mais elle peut être renforcée par l'utilisation d'un système de *fingerprinting* qui pourrait permettre d'identifier les systèmes pirates, afin de stopper la distribution de contenu vers eux.

Le risque économique du piratage est élevé, puisqu'il concerne la rediffusion de contenu ou la diffusion de logiciels de contournement par les pirates, de manière gratuite, mais cela peut être réduit par l'utilisation de *fingerprinting.*

2.3.3.3. Supports optiques (CD Audio/DVD).

Les nouvelles protections anti-copie des CD Audio ou le CSS, même s'il a été cassé, restent **relativement efficaces** vis-à-vis des utilisateurs ordinaires, mais assez facilement contournables par des pirates.

Il n'est pas possible de renouveler réellement la protection, étant donné le parc de lecteurs installés. **Le risque économique du piratage est élevé**, puisqu'il concerne la rediffusion de contenu ou la diffusion de logiciels de contournement par les pirates, de manière gratuite. La protection pourra être améliorée avec les nouveaux standards de supports optiques audio (DVD Audio ou SACD) mais leur pénétration du marché sera lente.

Tableau 2.2. – Evaluation des objectifs de protection.

Support	Robustesse	Possibilité de renouvellement	Maîtrise du risque économique
Télévision à péage	+ +	+	+
Diffusion par Internet	+	+ +	-
Support optique	-	- -	- -

Des outils de cryptographie sont ainsi les outils les mieux adaptés aux enjeux de la protection des contenus, mais ils peuvent être utilement complétés par l'utilisation du *fingerprinting*, lorsque c'est possible.

La différence de niveau relatif de sécurité et le contexte de baisse les coûts de distribution par Internet (y compris pour la contrefaçon) vont dans le sens d'une évolution du modèle économique, notamment dans le domaine du cinéma. Cela tendrait par exemple à revoir le calendrier des modes de diffusion, pour privilégier les modes de diffusion les plus sécurisés, comme la diffusion en télévision à péage ou par Internet par rapport à la sortie sur support optique, afin de limiter le piratage et ses réels effets d'éviction.

* * *

La technologie la plus prometteuse à des fins de protection est très certainement le chiffrement. En effet, elle présente l'avantage de résoudre, en même temps que la protection des droits, la protection de la transmission (ce qui est particulièrement utile pour la télédiffusion ou sur Internet) et la protection du stockage (un contenu stocké chiffré n'a pas d'intérêt sans sa clé de déchiffrement). Par l'utilisation de diverses clés, elle peut être évolutive, diversifiée et renouvelable. Enfin elle bénéficie du contexte favorable lié à sa libéralisation récente.

Cependant, le chiffrement peut utilement être complété par l'utilisation du *watermarking* à des fins de traçabilité du contenu, lorsque c'est possible. Enfin, l'utilisation d'autres technologies peut s'avérer nécessaire à défaut de protection, même si leur efficacité est généralement moindre.

* * *
*

3. LES SYSTÈMES NUMÉRIQUES DE GESTION DE DROITS.

Dans l'environnement numérique, notamment sur des réseaux de télécommunications, les systèmes numériques de gestion de droits (*Digital Rights Management Systems*) offrent aux titulaires de droits la faculté de recouvrer l'exercice effectif de leurs droits exclusifs d'autoriser ou d'interdire la représentation et la reproduction des œuvres, mais aussi un ensemble de licences d'utilisations dont ils peuvent contrôler le respect et obtenir rémunération. Même s'ils partagent certains objectifs et technologies des mesures techniques de protection, principalement appliquées aux supports physiques à des fins de contrôle de la reproduction, les systèmes numériques de gestion de droits s'en distinguent.

Les *DRMS* constituent l'architecture du commerce électronique des contenus numériques dont les conditions juridiques de protection et d'exploitation sont spécifiques. Les systèmes numériques de gestion de droits reposent sur la définition d'un « **espace de confiance** » nécessaire à la distribution de contenus numériques d'œuvres de toute nature, qu'ils réalisent dans un ensemble systématique de techniques de description des droits, d'identification et de protection des contenus numériques, d'identification et d'authentification des utilisateurs, de protection de la distribution, de procuration des licences d'utilisation, de gestion des données et des rémunérations, etc.[70]

La création d'un « espace de confiance » au sein duquel la communication est sécurisée est singulière à la distribution numérique d'œuvres. Par principe dans ce domaine, le titulaire des droits ne peut avoir confiance dans l'utilisateur. Ainsi, les systèmes numériques de gestion de droits doivent non seulement créer l'espace de confiance mais aussi, par des moyens techniques souvent similaires, l'élargir à l'ensemble de la chaîne de distribution. L'objectif est de repousser au maximum la limite au-delà de laquelle le contenu numérique sort du domaine de confiance. Ainsi, tout au long de la chaîne de distribution, des outils techniques permettent de garantir que les transactions sont sécurisées : ces outils assurent la mise en œuvre technique de la gestion numérique des droits, de la procuration des droits et de leur exploitation.[71]

---

[70] Dans l'exemple d'un système de sécurité, on considère classiquement que « Alice » et « Bob », se font confiance et souhaitent échanger des informations qu'un tiers ne pourra pas intercepter et que pour se faire ils doivent créer par des outils techniques un « espace de confiance ».

[71] L'ensemble de cette partie effectue une description aussi synthétique que possible de l'ensemble des *DRMS*, notamment développés par *Microsoft*, *Sony*, *Thomson*, *Philips*, *IBM*, *HP*, etc.

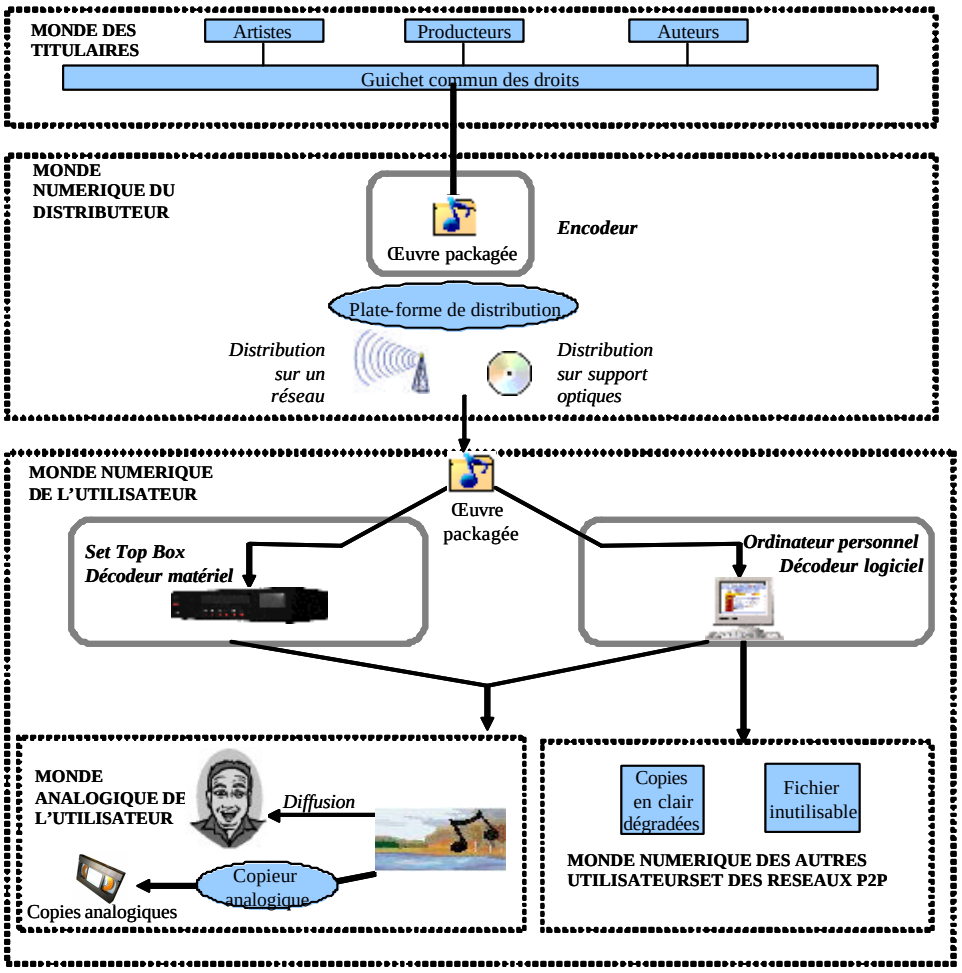
Les trois fonctions principales d'un *DRMS* – gestion numérique des droits, procuration et exploitation des œuvres et droits – assurent la mise en relation numérique de trois mondes :

– **le « monde des titulaires »** qui comprend les auteurs, les artistes et interprètes et les producteurs qui sont titulaires des droits exclusifs des œuvres, et pour les derniers propriétaires des supports de fixation des œuvres ;

– **le « monde numérique du distributeur »** dont la fonction principale consiste à assurer l'encodage des œuvres et de l'information sur les droits, mais aussi à gérer les plates formes de distribution électronique, particulièrement pour les flux économiques ;

– **le « monde de l'utilisateur »** acquéreur des supports physiques des œuvres ou des licences d'utilisation que ce soit dans le « monde numérique de l'utilisateur », le «monde analogique ou le « monde numérique des autres utilisateurs » qui échappe au système de protection et distribution licite visé par les *DRMS*.

Fig. 3.1 — Les « trois mondes » d'un *DRMS*



3.1. LA GESTION NUMÉRIQUE DES DROITS.

L'expression « **gestion numérique de droits** » est souvent l'objet d'une confusion par métonymie avec les « **systèmes numériques de gestion des droits** » que sont les *Digital Rights Management Systems* qui supposent juridiquement, techniquement et économiquement une « gestion numérique des droits ». Ainsi, un *Digital Right Management System* procède de la gestion numérique des droits, placée en amont de la chaîne numérique de distribution. Il ne saurait s'y résoudre, pas plus qu'il ne peut être confondu avec l'expression de « système de gestion des droits numériques » qui pourrait désigner en aval certaines utilisations des œuvres permises par l'environnement numériques et licitées par la gestion numérique des droits. En définitive, **la gestion numérique des droits correspond à la gestion des données relatives à l'information sur le régime des droits** qui est distinguée juridiquement des mesures techniques.[72] Toutefois les techniques employées pour la mise en œuvre du régime des droits empruntent à certaines des techniques requises pour garantir la protection des contenus mêmes.

3.1.1. LA DEFINITION DU REGIME DES DROITS.

Les données relatives à l'information sur les droits constituent le régime des droits associés aux œuvres protégées. Ce régime juridique des droits est préalable. Il est traduit techniquement pour former des modules « packagés » d'œuvres ou de « contenus numériques » entrant dans la chaîne de distribution.

Lors de la définition des droits d'exploitation d'une œuvre protégée, les titulaires de droits associent, pour chaque catégorie d'utilisateur et/ou d'utilisation, un ensemble de droits d'exploitation, relevant des droits de reproduction, de représentation, mais aussi d'utilisations comprenant la location, le prêt, mais aussi formés selon des logiques plus commerciales, fondées notamment sur l'accès, et déclinant des fonctionnalités selon la durée, la qualité, la jouabilité, etc. des œuvres.

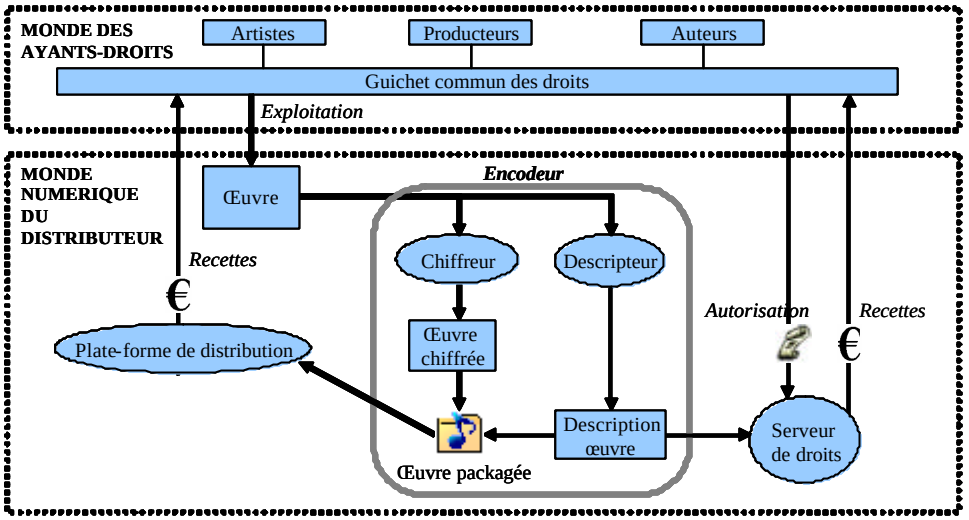
La définition du régime des droits établit donc la relation primitive d'un *DRMS* entre le « monde des titulaires de droits » et « le monde numérique du distributeur ». Évidemment, **cette relation suppose la numérisation du « monde des titulaires de droits »** afin d'intégrer le système numérique de gestion de droits. C'est l'un des enjeux d'un « guichet commun ouvert » de gestion de droits. [73] Par nature, un *DRMS* est neutre sur le caractère individuel ou collectif de la gestion des droits exclusifs, même s'il lui est possible d'assurer de manière précise une gestion individualisée de rémunérations proportionnelles à l'exploitation de chaque type d'exploitation et d'utilisation.

---

[72] cf. article 7 de la directive n° 2001/29.

[73] Pour la France, l'ensemble de ces outils pourrait s'établir au sein du « guichet commun » des droits. cf. P. Chantepie, *Soutenir un « guichet commun » des droits de propriété littéraire et artistique*, Rapport n° 2001-41, Ministère de la culture / IGAAC ; Travaux du Conseil supérieur de la propriété littéraire et artistique [http://www.culture.fr/culture/cspla/comguiccom.htm]

Fig. 3.2. — La gestion numérique des droits.



Dans la pratique, l'association d'un ensemble de droits d'utilisation à une œuvre implique l'emploi de quatre principaux types d'outils numériques :

– des outils d'identification du contenu numérique ;
– des outils de description des droits du contenu numérique ;
– des outils de protection du contenu numérique ;
– des outils de mise en relation des droits avec les données commerciales sur les utilisateurs.

3.1.1.1. L'identification des contenus.

La formation d'un vocabulaire commun minimal est la condition nécessaire à la réalisation de la fonction d'identification des contenus numériques.

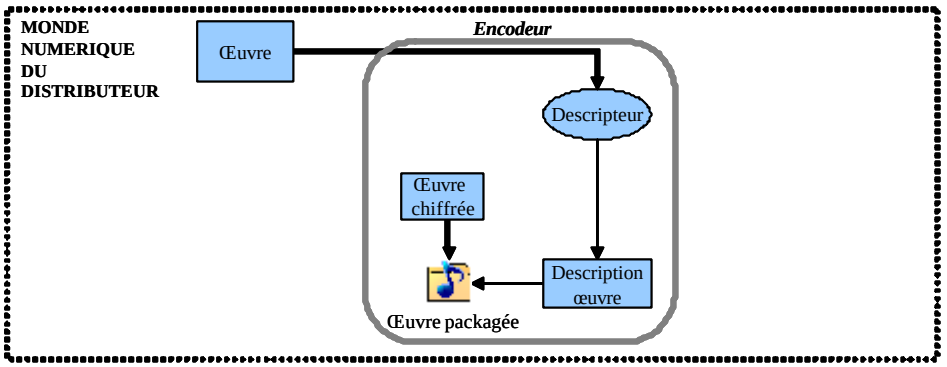
i. Rôle d'un système d'identification des contenus.

Afin de traiter numériquement un contenu, en particulier pour pouvoir réaliser la description du régime des droits qui lui est associé, mais aussi, la protection du contenu numérique, sa distribution et finalement sa restitution auprès de l'utilisateur, il est nécessaire que les outils numériques employés à ces opérations soient en mesure d'**identifier le contenu de manière non ambigu** pour les acteurs concernés :

– **Le titulaire de droit doit choisir un système d'identification qui permet, pour un contenu donné, d'assigner un identifiant unique**. Cet identifiant a vocation à être distribué conjointement avec le contenu protégé. Il ne contient pas les informations permettant de restituer le contenu numérique, mais les informations permettant de savoir de quel contenu numérique il s'agit (identification du contenu), et ainsi de quelle « clef » il faut nécessairement disposer pour le restituer ;

– **Pour le distributeur, cet identifiant sert à classer les clefs associées à chacun des contenus numériques de son catalogue commercial** ;

Fig. 3.3. – La fonction d'identification des contenus.



– **Pour l'utilisateur, cet identifiant sert à savoir qui a protégé le contenu numérique et à demander les droits pour la restitution de ce contenu ; il peut également lui permettre de gérer son répertoire**.

Parce qu'ils ne contiennent aucun secret, ces identifiants n'ont pas besoin d'être protégés. Un utilisateur malveillant ne peut pas espérer déverrouiller un contenu en falsifiant l'identifiant associé à ce contenu protégé : dans le meilleur des cas, il obtiendra une clef qui lui permet de restituer un autre contenu, mais pas le contenu qu'il souhaite attaquer. En effet, pour chaque clef, il existe au plus un contenu que cette clef peut ouvrir. Le système d'identification des contenus pouvant être public et non protégé, les acteurs ont la possibilité se mettre d'accord sur un système unique d'identification.

ii. Les systèmes d'identification des œuvres.

On observe que diverses approches existent, selon des catégories spécifiques aux œuvres ou plus génériques :

– **Les numéros ISO**, comme l'ISBN (*International Standard Book Number*) qui est un numéro international normalisé permettant d'identifier le titre d'un livre, ou les numéros ISWC, ISAN, etc. [(74)] ;

– **Le DOI (*Digital Object Identifier*)** est un système international d'identification des documents publiés sous forme électronique. Initialement développé par l'AAP (*Association of American Publishers*) dans le but de protéger le *copyright* des documents électroniques, il s'oriente maintenant vers un système de référencement unique et permanent permettant, entre autres, la mise en place d'hyperliens réciproques entre documents. Le DOI fait apparaître distinctivement l'éditeur. [(75)]

– **Le système d'immatriculation des images fixes numériques** (photographies, dessins, peintures, illustrations, etc.). Le système prévoit que la fonction d'immatriculation puisse être déléguée à des autorités nationales. Le numéro fait apparaître distinctivement le type d'œuvre, le pays d'enregistrement selon les normes ISO, le numéro de l'autorité d'immatriculation et le numéro séquentiel du fichier que délivre l'autorité

(74) cf. note préc.
(75) *Digital Object Identifier* [http://www.doi.org/]

d'immatriculation. Le numéro est inséré dans le fichier d'origine du contenu numérique.[76]

– **Les systèmes propriétaires**. Les éditeurs et les distributeurs sont libres d'utiliser leur propre système de référencement, éventuellement de façon conjointe avec l'utilisation d'un système normalisé facilitant les échanges.

Le comité de normalisation MPEG travaille sur la description et l'identification des œuvres numériques, notamment à travers les groupes MPEG-7, traitant des méta-données, et MPEG-21 part 2, traitant de la déclaration des ressources numériques.

3.1.1.2. L'intrication contenu – identifiant.

La protection d'un contenu numérique, et l'intrication du même contenu numérique avec son identifiant sont deux concepts indépendants. [77]

i. Une nécessaire intrication.

Si l'identifiant d'un contenu numérique n'a pas besoin de mesures techniques de protection lors de sa distribution, il est souhaitable en revanche que l'identifiant ne puisse pas aisément être séparé de l'œuvre.

– La protection d'un contenu numérique tend à limiter son « accès » à certaines personnes pour certaines utilisations, en fonction des droits licités et acquis. La protection est mise en place par le distributeur, elle est physiquement détachée du contenu lorsque celui-ci devient analogique, par exemple pour être restitué à l'utilisateur, ou bien lors de la réalisation d'une copie analogique.

– L'intrication d'un contenu et de son identifiant tend à ce qu'un lecteur d'identifiant détenu par le titulaire de droit lui permette d'identifier ce contenu, quelles que soient les opérations effectuées sur le contenu numérique. En particulier, l'intrication est particulièrement utile lorsque, même si le contenu est mis sous forme analogique, puis re-numérisé, le lecteur d'identifiant est toujours capable de reconnaître ce contenu. Par exemple, si l'intrication d'un identifiant sur un contenu est efficace, il est possible d'effectuer les opérations suivantes sur un contenu sans altérer l'identifiant :

– imprimer une image puis la scanner ;
– filmer avec une caméra numérique un film projeté à écran ;
– enregistrer avec un microphone relié à un PC un morceau de musique joué sur une chaîne hi-fi ;
– découper des extraits d'image, de vidéo ou de son.

ii. Les techniques d'intrication identifiant / contenu numérique.

---

[76] cf. *SACD, Image Fixe* [http://www.image-photo.sacd.fr/regaut] ; Projet *2Kan, Jpeg 2000*, développé notamment par *Netimage, Thalès, SACD.* [http://www2kan.org]

[77] L'intrication d'une donnée numérique au sein d'une œuvre consiste rendre ces deux éléments indissociables. Ainsi, l'information sur les droits est partie prenante de l'expression numérique de l'œuvre et inversement l'œuvre ne peut être accessible sans disposer de l'information sur les droits.

Deux principaux types de méthodes existent pour intriquer un identifiant avec un contenu : les approches par tatouage et par signature. Malgré leurs différences, l'une et l'autre occupent la visée centrale de la finalité de la protection juridique des mesures techniques de protection des œuvres, car elles répondent – de manière différente – aux objectifs de protection assignés à l'intrication identifiant / contenu numérique :

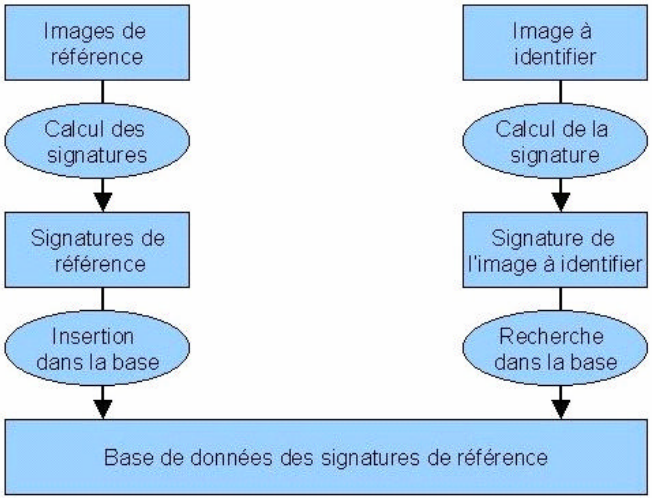
– l'objectif de **contrôle *a priori* de licéité de l'accès** ;
– l'objectif de **contrôle *a posteriori* de contrôle d'utilisation, d'identité et d'intégrité**.

– ***Intrication d'un contenu et de son identifiant par tatouage.***[78] Les techniques de tatouage peuvent être utilisées pour intriquer un contenu numérique avec son identifiant, ou bien avec une référence vers son identifiant. Dans ce cas, le tatouage contient une référence vers un identifiant, tandis que le lecteur d'identifiants possède la clef pour accéder au tatouage présent sur le contenu, le lire et procéder à l'identification de l'œuvre, éventuellement en se reliant à une base de données des références.

– Intrication d'un contenu et de son identifiant par signature. Plutôt que de créer pour chaque contenu un identifiant, et d'insérer cet identifiant à l'intérieur du contenu, une approche alternative consiste à extraire l'identifiant des données de l'œuvre elle-même. Plus exactement, le titulaire de droit calcule pour chacune des œuvres une signature, de petite taille, qui ne dépend que des informations contenues dans l'œuvre.

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

Fig. 3.4. – Fonction d'identification d'une base de données de signatures d'œuvres.



(78) cf. *supra* 2.2.

Il existe deux catégories de signatures :

– **Les signatures statistiques**. Pour toute œuvre sous format numérique, il est possible de réaliser une analyse du signal numérique associé, **ne tenant pas compte du sens pour un être humain de ce signal**. Cette analyse permet d'obtenir des données représentatives de l'œuvre, au sens mathématique. À partir de ces données, il est possible de constituer une signature statistique de l'œuvre.

– **Les signatures sémantiques**. Une signature sémantique est calculée à partir des éléments de l'œuvre qui créent du **sens pour un être humain**. Dans le cas de la musique, ces éléments peuvent être par exemple le nombre d'instruments et leur timbre, les mélodies, le *tempo*, le nombre de couplets, etc. Dans le cas d'une image ou d'une vidéo, il peut s'agir de la position relative des coins des objets représentés.

Encadré 3.1. — L'INA et l'IRCAM : identification des contenus par signature

L'INA a développé un système de signature sémantique pour les images et les vidéos. Ce système permet une reconnaissance automatique des œuvres, ce qui facilite leur identification. Il peut être utilisé à des fins de traçabilité des œuvres, c'est-à-dire du suivi de leur diffusion. De même, l'IRCAM a développé un système de signature statistique pour les œuvres sonores.[79]

iii. La robustesse des mesures techniques d'intrication.

Les techniques d'intrication identifiant/contenu numérique, qu'il s'agisse des signatures statistiques comme sémantique ou des tatouages,, présente des avantages et des inconvénients dont l'évaluation est fonction des usages mais aussi de la nature des œuvres.

– **En termes de robustesse suite à des modifications légitimes du contenu**. Un tatouage est conçu pour résister à des modifications ordinaires de l'œuvre, telles qu'un changement d'échelle, une suppression de certaines parties, ou un passage en analogique puis « re-numérisation ». En revanche, la modification d'une œuvre conduit à la modification de sa signature. **Un système de signature peut toutefois être aussi robuste aux modifications qu'un système par tatouage s'il s'agit d'un système de signature sémantique** , et si le moteur de comparaison des signatures est paramétré pour ne pas tenir compte des petits écarts.

– **En termes de robustesse suite à une attaque par un pirate**. Un pirate, souhaitant par exemple contrefaire une œuvre, pourrait avoir intérêt à supprimer l'identifiant attaché à une œuvre. **Un système mettant en œuvre des signatures est alors plus robuste qu'un système de tatouage**. En effet, un tatouage ayant été ajouté à l'œuvre originale, on peut imaginer qu'un pirate bien informé peut le retirer, même si l'algorithme de tatouage est non-réversible. De plus, les tatouages sont particulièrement sensibles aux attaques

[79] Le fonctionnement de ces systèmes est détaillé dans la partie 3.3.3.2.ii sur les principes et les applications de la traçabilité des copies numériques.

par coalition.[80] En revanche, une signature est particulièrement difficile à falsifier sans altérer l'œuvre de façon significative. Dans le cas d'une signature sémantique, et même si l'algorithme est connu par les pirates, modifier la signature d'une œuvre implique une modification du sens de celle-ci, aboutissant en général à une annihilation de sa valeur commerciale.

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

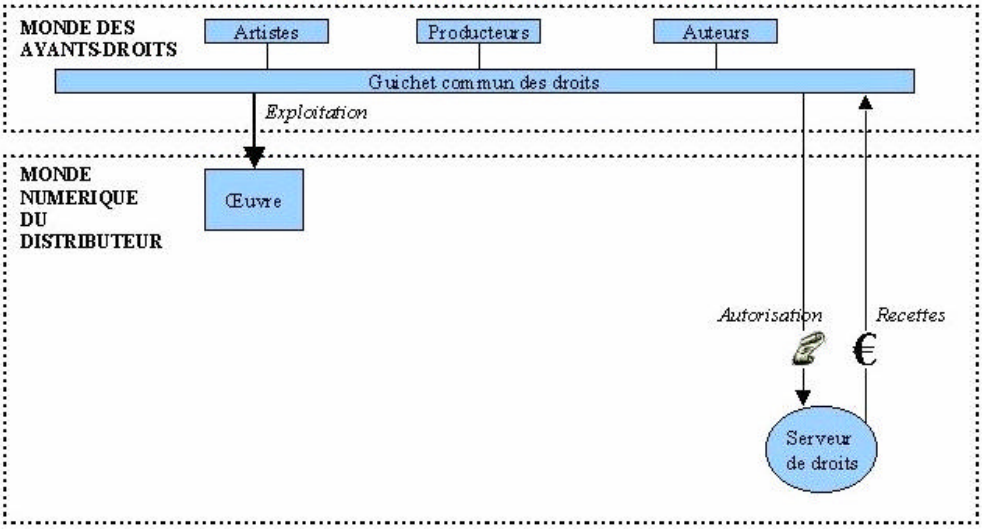
– **En termes d'antériorité.** Un système par tatouage ne permet d'identifier que les œuvres qui ont préalablement été tatouées avant leur diffusion. En revanche, un système par signatures permet d'identifier toutes les œuvres dont on possède une copie, même celles qui ont déjà été diffusées.

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

3.1.2. LANGAGES DE DESCRIPTION DE DROITS.

Pour les systèmes numériques d'identification des œuvres, le « monde numérique des ayant droits » et le « monde numérique du distributeur » doivent posséder un « vocabulaire » commun pour réaliser la description des droits de contenus numériques que ces deux catégories d'acteurs ont intérêt à protéger.

Fig. 3.5. – Fonction de description des droits.



[80] Attaque par coalition = lors d'une attaque par coalition, plusieurs destinataires d'une même œuvre mélangent leurs versions afin d'obtenir une nouvelle version de l'œuvre non identifiable

Sans nécessité, plusieurs vocabulaires communs coexistent, notamment en raison de développements d'idiomes propriétaires qui doivent ensuite évoluer pour devenir interopérables. C'est pourquoi, ils doivent reposer eux-mêmes sur un méta-langage de description de droits, comme celui qui résulte du projet Indecs (*interoperability of data in e commerce systems*), retenu notamment dans le cadre de MPEG 21.[81]

Pour autant, le «vocabulaire» commun d'identification des œuvres demeure inerte si les «langages de description de droits» ne sont pas établis et mis en mouvement. Ils sont la « **grammaire** » nécessaire pour parvenir à décrire les droits associés à chaque œuvre, pour chaque utilisateur, et ainsi, former la « langue » des *DRMS*. Un langage de description des droits permet de décrire numériquement les droits sur une œuvre sous format numérique (texte, œuvre musicale, image fixe ou animée, vidéo, jeu vidéo, etc.). [82] Un langage de description des droits doit, pour être pertinent et partagé, doit être :

– **précis** quant à l'identification des titulaires de droits et des utilisateurs des droits, à la description des catégories de droits licités, et à l'objet des dispositions contractuelles ;

– ouvert afin que le langage soit pérenne, il doit être possible d'ajouter de nouveaux types de droits ou d'identification ;

– générique (indépendant des systèmes d'exploitation), **clair et expressif c'est-à-dire non ambigu et aussi intelligible que le langage naturel**

Pour disposer synthétiquement de ces qualités, un langage de description de droits doit, autant que possible, faire l'objet d'une normalisation.

3.1.2.2. La normalisation des langages de description de droits.

Le caractère stratégique du langage de description des droits dans la chaîne numérique d'un *DRMS*, notamment parce qu'il est à la croisée des univers industriels et des producteurs de contenus, peut rendre compte de la très forte concurrence entre les standards appelés à normaliser le langage et donc les groupes d'acteurs industriels sur ce segment. Deux standards de langages normalisés de description, l'un et l'autre fondés sur le métalangage XML (*eXtensible Markup Language*) pour la création de langages descriptifs, notamment des langages à balises tels que HTML (*HyperText Markup Language*), sont donc en voie d'émergence et de compétition.

– ODRL (*Open Digital Rights Language*).[83] Il est né de la fusion entre le langage XMCL (*eXtensible Media Commerce Language*)[84] de *Real Networks* et du langage MRV développé par *Nokia*.
– XrML (*eXtensible rights Markup Language*).[85] C'est le nouveau nom du langage DPRL (*Digital Property Rights Language*) issus des travaux du *Xerox*

---

(81) *Interoperability of Data in e Commerce Systems* [http://www.indecs.org/]
(82) F. Alves, S. Guilley, L. Rojey, F. Tournois, *Langages de représentation des droits*, ENST, 2002 [http://www.comelec.enst.fr/~guilley/ressources/drm/]
(83) *Open Digital Rights Language* (ODRL) [http://odrl.net/] ; présentation : R. Ianella, IPR. [http://www.bakercyberlawcentre.org/2002/DRMS_Papers/DRMS-Sym-RI-Mar2002.pd}
(84) eXtensible Media Commerce Language (XMCL) [http://www.xcml.org]

Palo Alto Research Center (Xerox-PARC) et dont les brevets sont détenus désormais par *Contentguard* dont *Microsoft* est actionnaire.[86]

La position de marché d'XrML semble plus solide que celle d'ODRL : la phase d'exploitation a commencé. De plus, XrML a été adopté en tant qu'élément de la norme naissante MPEG 21. La 5e partie de cette norme donne en effet des recommandations portant sur les langages de description des droits.

Même si ces normes connaissent un développement rapide, elles ne sont encore que très récentes : XrML 1.0 a été publié en 1999 tandis qu'ODRL 1.0 a été publié en novembre 2001. Les systèmes de gestion numérique des droits sur internet commencent à les exploiter, mais les systèmes plus anciens (télévision par câble ou satellite) mettent en œuvre des langages propriétaires.

La question de la description des droits est stratégique. Elle détermine – par la fixation et la maîtrise de la grammaire – et le plus en amont possible, l'ensemble de la distribution de contenus numériques, c'est-à-dire aussi bien la nature originaire des droits de propriété littéraire et artistique que la place et la fonction des acteurs respectifs, et l'ensemble des modes d'utilisations des œuvres, autrement dit les stratégies commerciales présentes et futures. Elle fait donc l'objet d'une compétition importante.

3.1.2.3. Exemple d'un langage de description des droits : XrML.

XrML assure une méthode universelle associée à tout type de ressources de spécification et de gestion sûre de droits et de conditions.

i. Principes de XrML.

XrML assure une intégrité totale des droits tout au long des chaînes de communication grâce à l'intégration d'un système de confiance. XrML implémente la possibilité de définir des organismes de certification, dont le rôle est d'assurer que les échanges sont conformes, par exemple qu'il n'y a pas d'abus d'identité ou de promesse non tenue. Cette fonction de superviseur peut se déléguer.

Comme ODRL, XrML est un «schéma » au sens du W3C, c'est-à-dire un modèle générique permettant d'instancier des objets spécifiques conformes à un standard. Une licence est construite sur une phrase, XrML repose sur la phrase suivante : « *une licence est un ensemble de concessions qui procurent à certaines personnes certains droits sur certaines ressources sous certaines conditions* ». En sachant qu'une concession et un droit sont des ressources, on peut produire des documents très complexes et une très large et flexible capacité de description.

ii. Mécanismes mis en jeu par XrML.

Un langage de description des droits décrit quelles opérations numériques peuvent ou doivent être effectuées, mais il ne décrit pas en tant que tel quels moyens doivent être mis en œuvre. La norme XrML donne des recommandations sur les mécanismes fondamentaux du système de gestion numérique des droits :

---

(85) eXtensible rights Markup Language (XrML) [http://www.xrml.org/]
(86) *Digital Property Rights Language* (DPRL) [http://xml.coverpages.org/dprl.html].

– **L'identification des personnes et des ressources**. L'identification vise à reconnaître l'identité d'un objet. XrML prévoit que celle-ci soit fondée principalement sur les mécanismes de clefs publiques. La personne correspondant à une clef publique est l'entité qui possède le secret correspondant. Ce système est conceptuellement simple, et permet l'authentification, mais il impose que les utilisateurs du langage mettent en place des infrastructures de gestion de clefs.

– **L'authentification des personnes et des ressources**. L'authentification vise à vérifier que l'identité avancée par une personne ou une ressource est bien conforme à la réalité. Dans la lignée de l'identification, les mêmes types de procédés sont utilisés pour assurer l'authentification. Une clef publique est requise pour les personnes, un condensé ou une signature pour les ressources numériques. [87]

– **La signature et le chiffrement** s'appuient sur les normes W3C en cours de développement : XML-ENC pour le chiffrement, et XML-SIG pour la signature.

iii. Exemples de licences.

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

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

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

– **Prêt d'un livre électronique** : après avoir acheté un livre électronique, un utilisateur peut prêter ce livre à une tierce personne pour une durée déterminée. À l'expiration de la durée, l'utilisateur retrouve automatiquement l'usage du livre tandis que la tierce personne n'y a plus accès. Cette fonction de prêt de livre électronique (*Adobe* ou *e-book*) est notamment implantée par un logiciel de la société *Info2Clear*.[88] Le prêt d'une œuvre est également prévu pour les films par la société *Medialive*.[89]

– **Copie privée : 1 fois**. Après avoir acheté le droit de consulter une œuvre, l'utilisateur peut réaliser une et seulement une copie numérique parfaite de cette œuvre. De plus, cette copie parfaite est stérile, c'est-à-dire qu'elle ne peut pas engendrer d'autres copies.

---

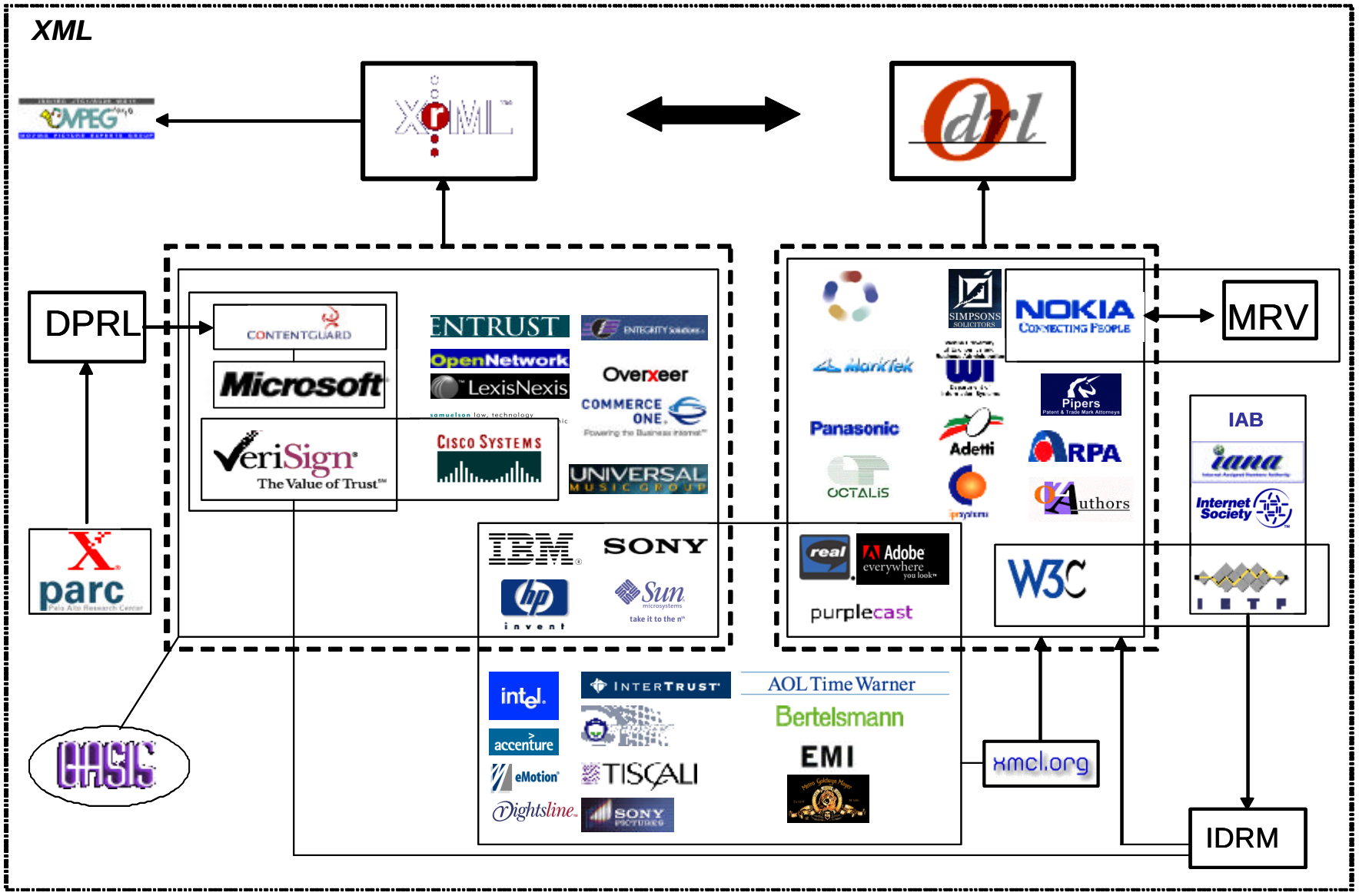
[87] Le *condensé* d'une ressource numérique, appelé aussi *haché*, est un objet numérique de plus petite taille extrait de cette ressource. Les fonctions de hachage sont décrites dans la partie I.1.3.2.
[88] *Info2clear* [http://www.info2clear.com/FR/index.asp]
[89] *Medialive* [http://www.medialive.fr/] cf. *infra*.

– **Copie privée : *n* fois.** Après avoir acheté le droit de consulter une œuvre, l'utilisateur peut réaliser un nombre *n*, et exactement *n*, de copies numériques de cette œuvre. Par ailleurs, ces copies sont stériles, c'est-à-dire qu'elles ne peuvent pas engendrer des copies subséquentes. Ce type de droits est notamment prévu par le système *Windows Media Right Manager* de *Microsoft.* [(90)]

– **Copie privée sur réseau privé personnel**: après avoir acheté le droit de consulter une œuvre, l'utilisateur peut réaliser un nombre illimité de copies parfaites, mais ces copies ne sont lisibles que par ce même utilisateur au sein de son réseau privé personnel.

[(90)] *Windows Media Rights Manager* [http://www.microsoft.com/windows/windowsmedia/drm.asp] cf. *infra*.

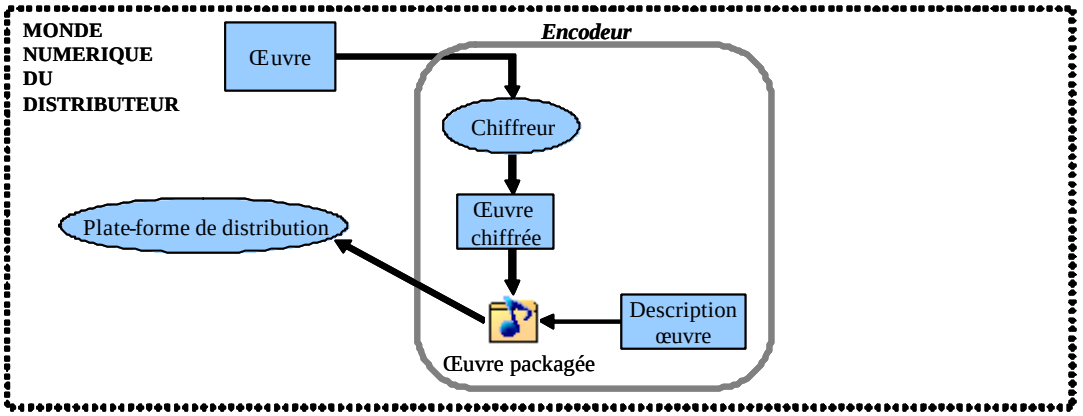
Fig. 3.6. — La description de droits.



3.1.3. LE CHIFFREMENT DES CONTENUS.

Le langage de description des droits permet de rédiger un contrat entre les titulaires de droits et les utilisateurs. Ce contrat prévoit les conditions juridiques d'exploitation et d'utilisation de certaines œuvres par certaines personnes sous certaines conditions. Toutefois, le langage à lui seul ne peut ni empêcher, ni même détecter, si un utilisateur ne respecte pas les termes du contrat. **Un système de gestion numérique des droits associe donc un langage de description de l'information sur les droits avec des mesures de protections techniques visant à contrôler le respect du contrat.**

Fig. 3.7. – Fonction du chiffrement des contenus et de l'information sur les droits.



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

C'est exclusivement la combinaison de ces deux éléments qui permet à l'utilisateur d'exercer les divers droits d'accès et d'utilisation à l'œuvre qu'il a acquis. Au lieu d'être sous une forme inexploitable, l'œuvre peut-être sous une forme partiellement exploitable, afin d'assurer une promotion commerciale de l'œuvre et inciter les utilisateurs à acheter les droits pour l'œuvre complète. Considérant que la taille de la représentation numérique des droits sur une œuvre est insignifiante comparée à la taille de la représentation numérique de cette œuvre, ce système de séparation des œuvres et de la représentation des droits permet de :

– **la séparation spatiale et temporelle de l'action de distribution de l'œuvre de l'action de procuration des droits sur cette œuvre** ;

– **la mise à jour des droits d'un utilisateur sur une œuvre** sans avoir à lui envoyer une nouvelle version de l'œuvre.

Cette séparation de la distribution de l'œuvre et de la procuration des droits n'est possible que s'il est possible de distribuer une œuvre sous une forme inexploitable en tant que telle, et de distribuer la clef permettant de l'exploiter, en même temps que la représentation des droits. Un chiffrement efficace des œuvres doit pouvoir répond à cette exigence.

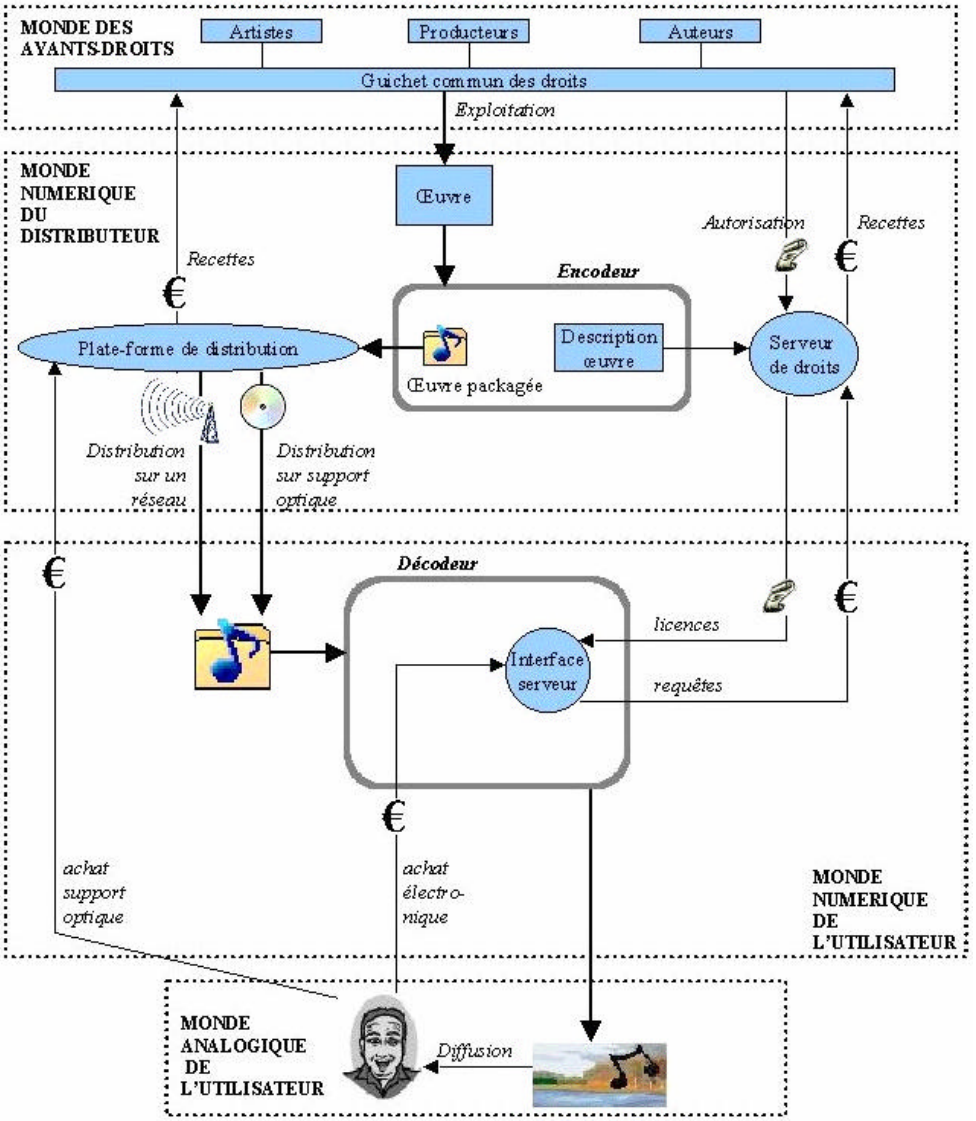
3.1.4. ARCHITECTURES TECHNIQUES DES *DRMS* ET DES *PRMS*.

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

3.1.4.1. Lien avec la base de données clients.

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

Fig. 3.8 – La fonction d'échanges de droits et données.



La délivrance des concessions est généralement centralisée au niveau d'un serveur informatique, appelé « serveur de droits ». Ce serveur est la propriété du titulaire de droit, le cas échéant, par délégation ou redondance du distributeur. **Le serveur de droit doit être situé dans un environnement de confiance** à la fois **physiquement** (bâtiment sécurisé, accès restreint au local) et **virtuellement** (la connexion entre le serveur et les utilisateurs est sécurisée, de telle sorte que les utilisateurs ne puissent pas pénétrer sur le serveur pour y faire des opérations illégales). Les technologies de sécurisation d'un serveur disponibles aujourd'hui sont très robustes.

Le serveur reçoit en entrée de la part des titulaires de droits, l'ensemble des licences définies, avec un langage de description des droits, de façon générique pour chaque œuvre ; il reçoit de la part des utilisateurs, des requêtes de concessions, éventuellement accompagnée d'un paiement. Il émet en sortie, vers les titulaires de droits, le nombre de requêtes pour chaque œuvre et le total des sommes perçues correspondantes, et, vers les utilisateurs, des concessions. Deux scénarios d'exploitation sont possibles :

– **Les licences définies par les titulaires de droits ne sont pas nominatives**. Elles sont du type : « *telle œuvre peut être achetée au prix de 20 €, sa location pour un jour coûte 5 €, etc.* ». De même, **les bilans envoyés aux titulaires de droits sont consolidés pour chaque œuvre, ne précisant pas le nom des personnes ayant acheté telle ou telle œuvre**. Un tel scénario garantit une protection maximale des données personnelles.

– **Les titulaires de droits souhaitent personnaliser les licences**, par exemple définir des catégories de consommateurs qui bénéficient d'un régime spécial. Dans ce cas les licences sont nominatives, **mais cela n'implique pas que les bilans envoyés par le serveur aux titulaires de droits le soient aussi**. On peut imaginer que le serveur de droits ne retourne que les recettes générées par chaque œuvre, ou bien les dépenses effectuées par chaque utilisateur, sans que les titulaires de droits aient la possibilité de savoir exactement les utilisations de telle œuvre par tel utilisateur. Il serait possible qu'une autorité indépendante certifie techniquement le niveau de protection des données personnelles associé à un serveur de droits, et à son interface avec la base de données clients d'un titulaire de droit.

Dans les deux cas, **le serveur de droits pose des questions du point de vue du respect du droit de la protection de la vie privée**. Cette question est techniquement posée par l'articulation entre les *DRMS* et les *PRMS* (*Privacy Rights Management Systems*) qui constitue un sujet assez neuf, mais majeur pour le développement des *DRMS*. L'essentiel de la problématique de la relation entre les *DRMS* et *PRMS*, chargés l'un comme l'autre de garantir des valeurs (données personnelles / distribution de contenus numériques) consiste à rendre leurs architectures compatibles sans avoir à partager leurs «secrets » respectifs. Si cette articulation est mieux maîtrisée pour les usages du commerce électronique et le respect des droits des consommateurs comme des données personnelles, elle pourrait apparaître plus problématique s'agissant de « contenus numériques », essentiellement parce que leur distribution numérique notamment sur les réseaux relève de la « communication audiovisuelle » au sens de la loi et engage donc le respect du **« secret des choix des personnes »**.[(91)]

[(91)] cf. 2ème partie de l'étude.

Encadré 3.2 — Les données personnelles indispensables à l'usage d'un *DRMS*

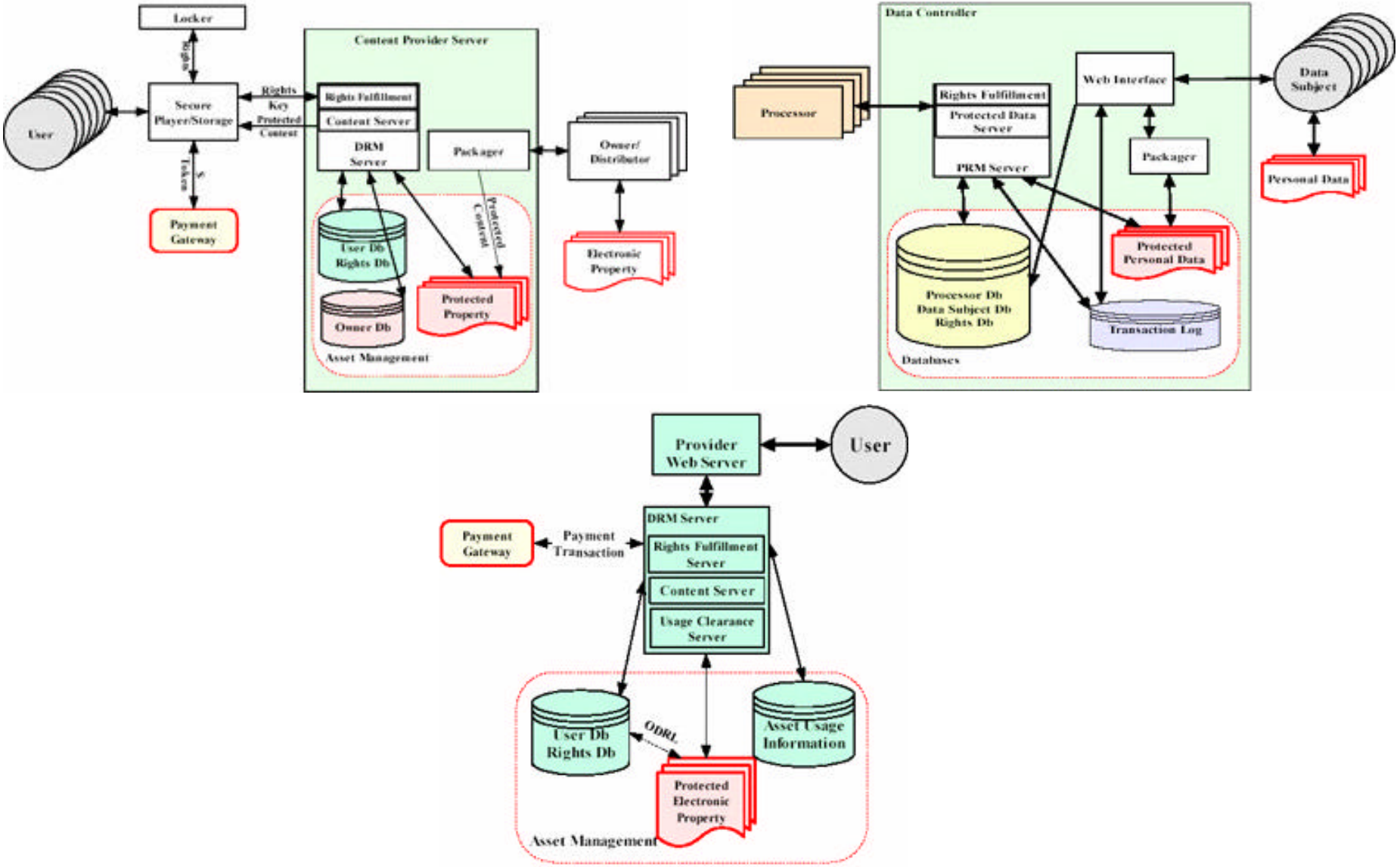
La mise en œuvre d'un *DRMS* peut n'appeler en pratique qu'un nombre très réduit de données personnelles et n'impliquer que des consolidations de données très limitées, comme pour la plupart des services de commerce électronique. Dans ce cadre, la consolidation des données dépend principalement du régime juridique et technique applicable (*opt-in* ou *opt-out*) et de l'architecture des remontées différenciées des données selon les acteurs. Dans le cas notamment d'un usage de DRMS par un distributeur opérant comme intermédiaire entre titulaires de droits et services de diffusion de contenus :

- pour l'opérateur de *DRMS*, l'identifiant plus ou moins authentique (nom ou pseudonyme) mais surtout adresse e-mail pour la formation du contrat et numéro de carte bancaire pour les opérations financières, externalisées ou non ;
- pour les titulaires de droits, une répartition des volumes de consommation d'œuvres selon leurs modes de distribution (en fonction des tarifications de ceux-ci), autrement dit en volume à des fins de facturation, le cas échéant des indications en volume des périodes (heure et date) d'accès ;
- pour les éditeurs de services, des mêmes données, le cas échéant, des identifiants associés aux consommations selon l'option de gestion de la protection des données personnelles.

Dans ce cas, le distributeur opère une fonction centrale de tiers de confiance, comme :

- gardien d'étanchéité sinon des remontées de données personnelles entre l'inscription au service de distribution de contenus (site de distribution dont c'est la « clientèle ») et les données relatives aux consommations (titulaires de droits) ;
- gardien exclusif de l'attribution des clés de décryptage, sans remontée des données personnelles et de consommation en direction du fabriquant de DRMS, notamment en vue de reconstituer des bibliothèques virtuelles perdues du fait de défaillance du PC, etc.
- gardien de l'intégrité physique de conservation des données personnelles d'inscription aux services et de la gestion des choix des utilisateurs (*opt-in* ou *opt-out*).

Fig. 3.9. – Architectures de *DRMS* et *PRMS*



L. Korba, S. Kenny, *Towards Meeting the Privacy Challenge: Adapting DRM* [http://crypto.stanford.edu/DRM2002/KorbaKennyDRM20021.pdf]

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

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

i. Les systèmes décentralisés.

Les systèmes décentralisés, ne possèdent pas, par définition, de base de données des utilisateurs et excluent par conséquent tout risque de constitution d'un fichier nominatif. Toutefois, il faut distinguer les situations possibles :

– **Les systèmes sans remontée de données personnelles.** C'est le cas du système *Smartright* qui ne vise qu'à protéger la copie des contenus, et non l'accès. Les cartes à puce servant à l'authentification sont mises en place en série lors de la fabrication des téléviseurs, et puisque ceux-ci sont vendus de façon anonyme, il n'est pas possible de relier un numéro de carte à puce avec un nom d'utilisateur. Par la suite, le système *Smartright* fonctionne sans voie de retour. Les données sur l'utilisation des œuvres remontent jusqu'à la carte puce située au sein de chaque téléviseur, mais ne sont pas acheminées hors du foyer.[92]

– **Les systèmes matériels avec remontée éventuelle de données personnelles** Le projet TCPA (*Trusted Computing Platform Alliance*) est une alliance industrielle regroupant depuis 1999 *Microsoft*, *Intel*, *IBM*, *Compaq*, et *HP* pour chercher à doter les ordinateurs personnels de fonctionnalités de sécurité : authentification, intégrité, respect de la vie privée, notamment pour des applications de *B2B* ou d'administrations électroniques.[93] En tant que tel et à ce jour, il pourrait ne pas poser de problème sur ce dernier point. Fondé sur une option d'*opt-in* et des fonctions d'anonymisation, TCPA permettrait aux utilisateurs de protéger les fichiers placés sur leurs ordinateurs, en rendant par exemple impossible leur lecture sur d'autres ordinateurs.[94]

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

---

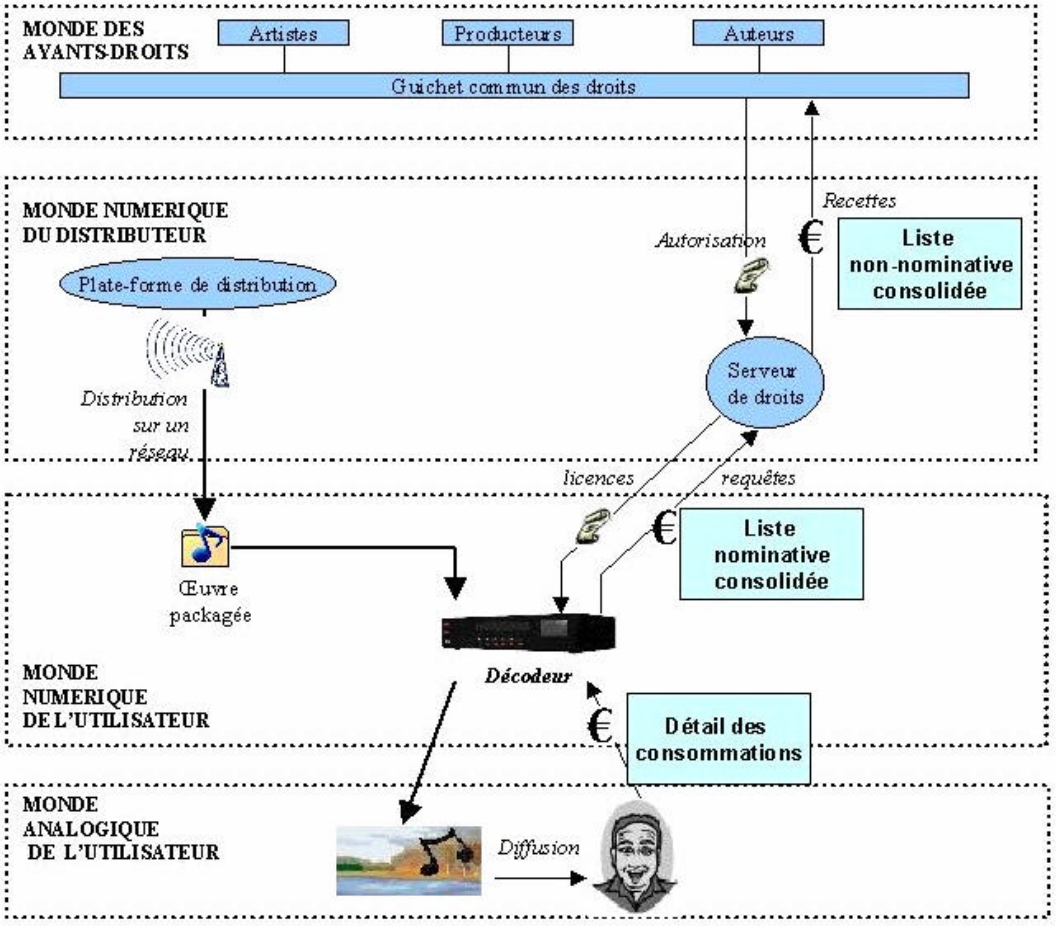
(92) *Smartright* ne prévoit l'existence que d'une base de données *a posteriori*, relative aux opérations de maintenance sur les cartes à puce. (cf. 2.3.2.3).
(93) *Trusted Computing Platform Alliance* [http://www.trustedcomputing.org/tcpaasp4/index.asp]
(94) Spécifications, oct, 2002 [http://www.trustedcomputing.org/docs/TCPA_TPM_PP_1_9_7.pdf]

données personnelles, sauf si l'utilisateur l'admet en bénéficiant des conditions d'informations nécessaires.

ii. Les systèmes partiellement centralisés

Les systèmes de gestion numérique des droits et virtuellement centralisés aujourd'hui existants réalisent une consolidation des achats au niveau des consommateurs ou bien à un niveau intermédiaire, mais pas au niveau du serveur central. Par conséquent, mis à part l'utilisateur lui-même, **personne dans la gestion numérique des droits ne peut avoir accès à la connaissance des actes de consommation effectués par tel ou tel utilisateur des œuvres ainsi distribués et contrôlés**. Au-delà du graphique suivant, quelques exemples peuvent être précisés :

Fig. 3.10. – La consolidation des données personnelles dans un *DRMS.*



– **Les services de films à la demande sur les réseaux de télévision par câble ou par satellite**. La consolidation se fait au niveau du décodeur. Un consommateur doit préalablement acheter des jetons, le serveur central enregistre alors le nombre de jetons achetés pour chaque utilisateur. Le nombre de jetons est stocké dans chaque foyer au niveau de la carte à puce insérée dans le décodeur. **Lorsqu'un achat de programme a lieu, sans aucune répercussion sur le serveur central**, le nombre de jetons est décrémenté au sein de la carte à puce.

– **Les réseaux de télévision par ADSL** en cours d'édification, qui permettront la mise à disposition de services à la demande sur les téléviseurs reliés à une prise téléphonique par

un décodeur spécifique, prévoient **une consolidation à un niveau intermédiaire du détail des consommations**. Chaque DSLAM pilote les flux audiovisuels envoyés à chaque foyer en fonction des requêtes envoyées par les décodeurs situés dans les foyers, et des informations sur les clients envoyées par le serveur central.[95] Les opérateurs envisagent de consolider au niveau de chaque DSLAM les consommations effectuées par chaque utilisateur. Une telle option est dans leur intérêt dans la mesure où le protocole de communication n'est pas le même entre d'une part les décodeurs et les DSLAM, et d'autre part, entre les DSLAM et le serveur central. Faire remonter des informations relatives à chaque consommation jusqu'au serveur central serait pour les opérateurs une stratégie coûteuse en termes de bande passante sur les liaisons de dessertes, sur le *backbone*, et au niveau du serveur central.

iii. Les systèmes matériels potentiellement centralisés.

Les systèmes centralisés sont très répandus en ce qui concerne la protection des œuvres diffusées sur internet. Ils devraient donc faire l'objet d'un maximum de vigilance, conformément aux principes énoncés plus haut (cf. 3.1.4.1). On notera d'ailleurs que les systèmes de *peer to peer* sur internet posent des problèmes similaires.[96]

Le projet de *Microsoft* « *Palladium* » rebaptisé *« Next Generation Secure Computing Base »* a été reconfiguré quant à ses objectifs initiaux qui tendaient à accroître les fonctionnalités du système d'exploitation *Windows* en terme de sécurité.[97] Les nouvelles fonctionnalités intéressant notamment les professionnels reposeraient sur des composants matériels et logiciels et tendraient à accroître la sécurité des ordinateurs personnels, notamment en garantissant la confidentialité des fichiers. **La gestion numérique des droits et *Palladium* sont deux technologies indépendantes, l'une pouvant fonctionner sans l'autre.**

Cependant, il existe une forte synergie entre elles. Si *Palladium* était installé sur les ordinateurs des particuliers, il pourrait renforcer de manière très significative les systèmes de *DRMS*, en premier lieu celui protégeant le logiciel d'exploitation *Windows.* Cependant, dans une telle hypothèse, *Palladium* pourrait — par effet de bords — sécuriser d'autres services, y compris des services libres de droits ou mettre en difficulté l'interopérabilité du système d'exploitation et de sécurité avec certains logiciels. Comme d'autres systèmes centralisés (*Windows Media Player* par exemple, en ce qui concerne la consommation d'œuvres sécurisées) *Palladium* pourrait présenter des risques de centralisation de données nominatives. Toutefois, les fonctionnalités de sécurité nouvellement au centre de *Next Generation Secure Computing Base* devraient se distinguer des *DRMS* de *Microsoft,* notamment de *Microsoft Windows Rights Management Services* (RMS). En toutes hypothèses, ces techniques de sécurisation n'échappent pas – intrinsèquement – à l'application des dispositions relatives à la protection de la vie privée.[98]

---

[95] Équipement installé dans les répartiteurs de France Télécom et qui permet de transformer les lignes téléphoniques en lignes DSL.

[96] Cette question est d'autant plus délicate que le comportement des sociétés gérant ces systèmes, telle *Sharman Networks* à l'origine de *Kazaa,* est plus difficile à contrôler juridiquement que celui des éditeurs de *DRMS* comme *Microsoft* ou *Real Networks.*

[97] *Microsoft Next-Generation Secure Computing Base — Technical FAQ* [http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/news/NGSCB.asp]

[98] Les inquiétudes qu'un tel projet a suscitées ou continue de susciter sont plutôt relatives aux risques présentés par l'influence accrue par des facteurs techniques et économiques de voir son champ d'action atteindre des services libres de droit ou en rendre l'accès incompatible. Le

Encadré 3.3. — « *Palladium* » : conditions techniques d'acceptabilité

La reconfiguration du projet « *Palladium* » **a** commencé à tracer des limites d'un contrôle potentiel que *Microsoft* serait en mesure d'avoir sur le système Un certain nombre de conditions au développement d'un tel projet serait désormais prévu : [99]

– que **les composants matériels et logiciels de *Palladium* soient désactivés par défaut** lors de la livraison d'un ordinateur ;

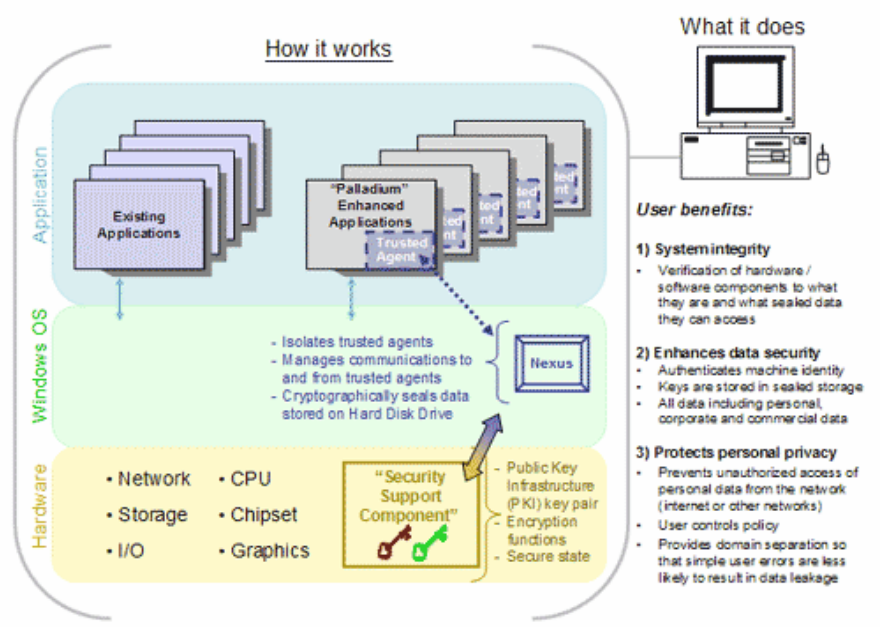
– que soit **publié et validé par un tiers de confiance le code source** du composant logiciel « *nexus* » [100] ;

– que le matériel *Palladium* soit **compatible** avec tous les « *nexus* », que le « *nexus*» de *Palladium* soit compatible avec tous les « *agents de confiance* » [101] de tous les éditeurs et tous les fournisseurs de services Internet ;

– que de **libres développements alternatifs** des « *nexus* » et « *agents de confiance* » soient rendus possibles ;

– que la **certification d'un un matériel ou logiciel par quiconque ayant la confiance des consommateurs** puisse être réalisée.

Fig. 3.11. – Architecture initiale de « Palladium »



---

développement de ces services pourrait alors être affecté et les risques d'interférence avec des données personnelles seraient amplifiés.

[99] cf. « *Microsoft Palladium : A Business Overview* », août 2002. [http://www.microsoft.com/PressPass/features/2002/jul02/0724palladiumwp.asp]

[100] Un « nexus » est un module de *Microsoft Windows* qui gère les fonctions de sécurité pour les « agents de confiance ». Il s'exécute en mode « noyau » dans l'espace de confiance, qui est un composant matériel installé dans l'ordinateur. Il fournit aux « agents de confiance » des services sécurisés, comme des mises en relations avec les autres « agents de confiance » et applications, ou la délivrance d'attestations.

[101] Un « *agent de confiance* » est une application, ou morceau d'application, qui s'exécute en mode utilisateur dans l'espace de confiance. Il fait appel au « *nexus* » pour les opérations sensibles ou critiques, comme la gestion de la mémoire. Un « *agent de confiance* » est capable de mettre à l'abri des secrets, et s'authentifie en utilisation les fonctionnalités du « nexus ». Chaque « *agent de confiance* » contrôle sa propre sphère de confiance.

S'ils sont tenus, **de tels engagements, seraient en mesure d'assurer techniquement des garanties à un niveau de protection des données personnelles, pourvu — bien sûr — que le(s) tiers de confiance soi(en)t une/des autorité(s) neutre(s) et indépendante(s).** Sans la réunion de ces conditions, et **cela vaut naturellement pour tous les systèmes de cette nature**, la perspective du déploiement simultané de composants matériels de sécurité sur une part importante du parc d'ordinateurs personnels et d'**un système d'exploitation propriétaire protégé par ces composants, laisse entrevoir des conséquences potentiellement délicates en termes de protection des données personnelles, voire de liberté de communication.**

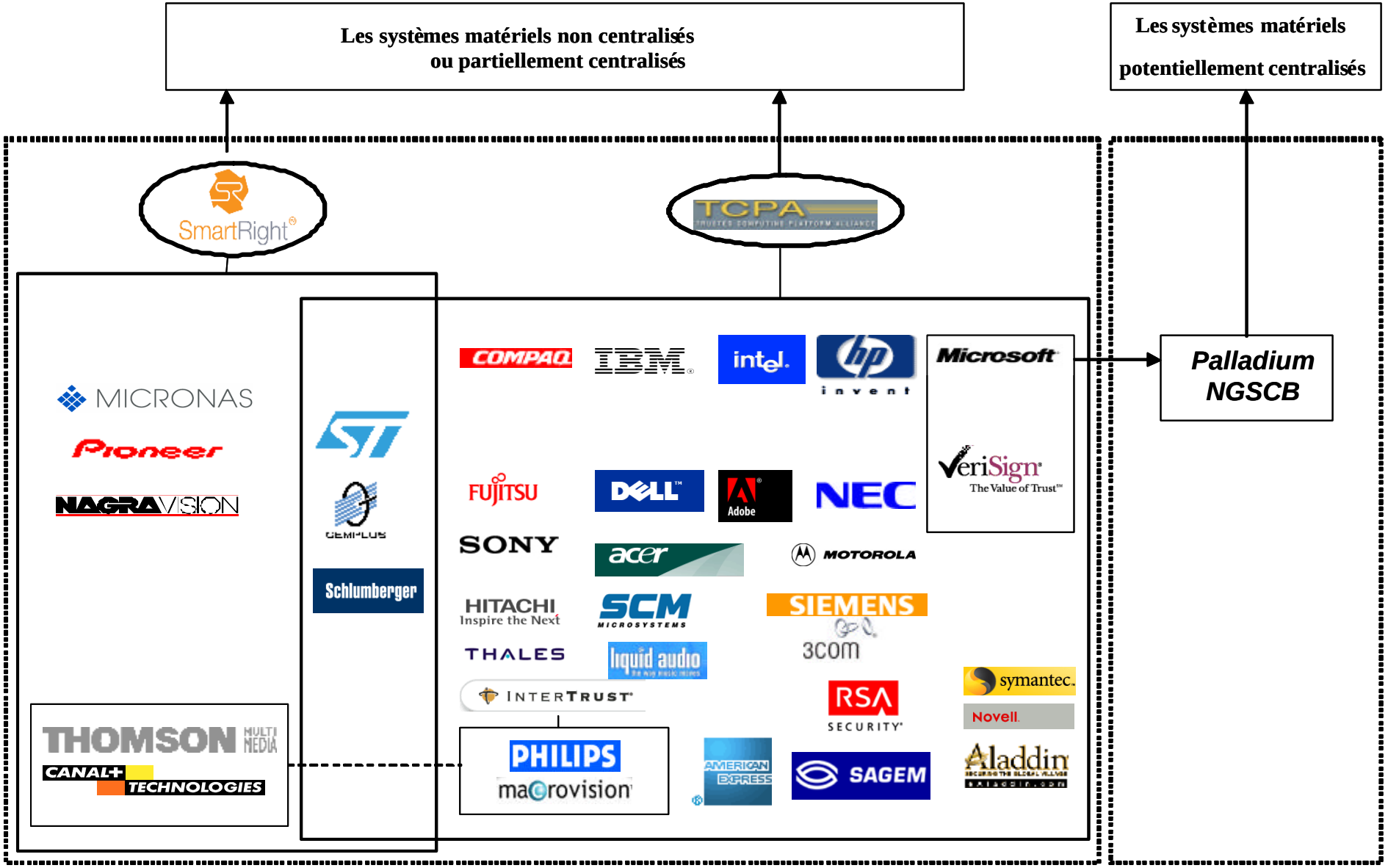
En toute hypothèse, tout système matériel relevant d'un *DRMS* reste soumis à la combinaison de l'application des articles 3 de la *loi du 30 septembre 1986 relative à la liberté de communication*, de la *loi 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, et de la transposition de la *Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*. [(102)] La résolution des questions techniques d'articulation des architectures des *DRMS* et des *PMRS* ne sauront sans doute pas se substituer à l'application de ces règles et à une information précise des utilisateurs sur la nature exacte des données nominatives nécessaires et surtout sur les traitements de celles-ci.

L'ensemble de ces questions en partie récentes appelle une attention d'autant plus particulière que chacun des systèmes proposés est en évolution rapide et concentre des enjeux de compétition industrielle importants ainsi que des enjeux économiques et culturels centraux. Elles combinent en effet non seulement des objectifs de sécurité des contenus mais aussi de robustesse des solutions industrielles proposées ou projetées, mais aussi les clefs de succès des *DRMS* tant pour leur fiabilité que pour leur faculté à satisfaire les utilisateurs pour leurs consommations de contenus culturels.

* * *

[(102)] Sur ces aspects juridiques à l'occasion de la transposition de la directive 2001/29, cf. 2e partie de l'étude : *La régulation du droit des mesures techniques*. (2.3. La protection de la vie privée).

Fig. 3.12. – L'univers industriel du chiffrement

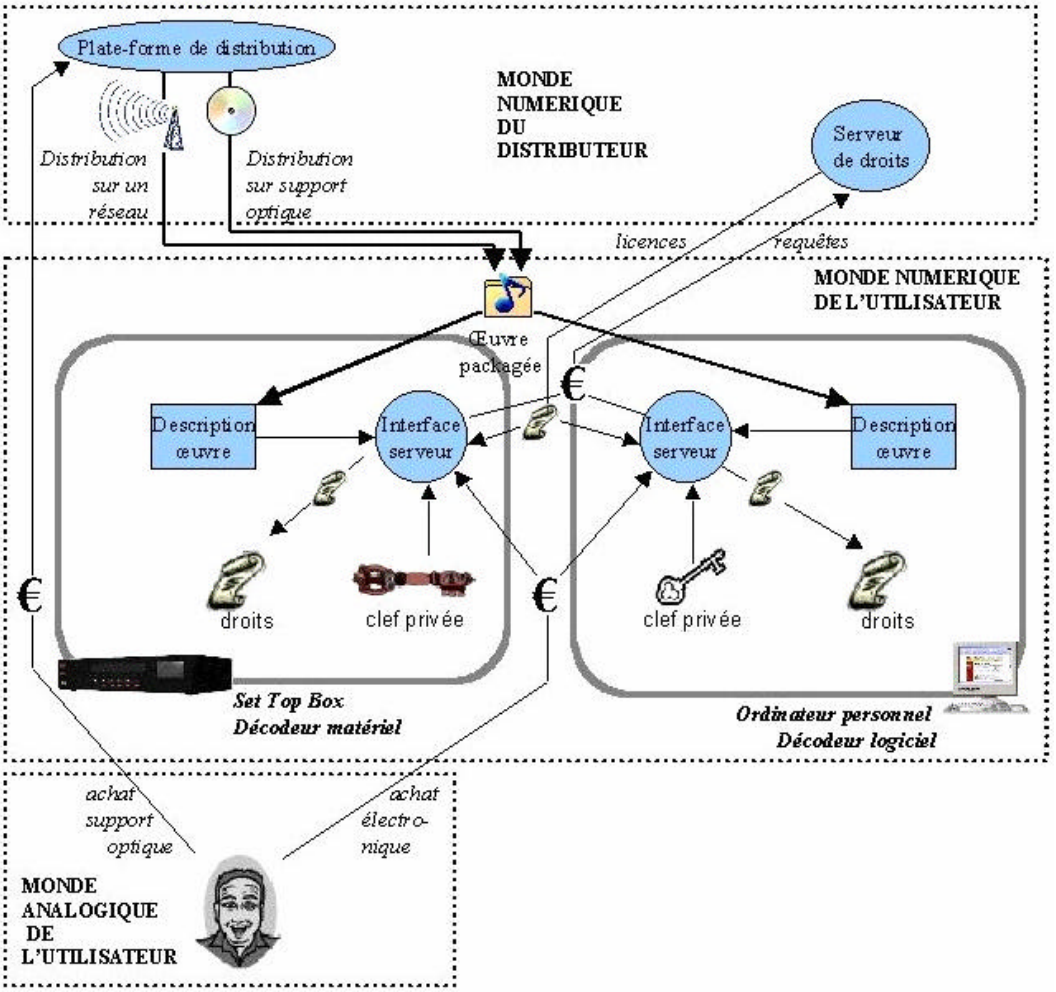


3.2. LA PROCURATION DES DROITS.

La première étape d'un système numérique de gestion de droits consistait, d'une part à définir numériquement les droits (identification, description), d'autre part à chiffrer les contenus numériques, en respectant le principe de séparation de la fourniture des droits et des contenus numériques.

La seconde étape d'un système de gestion numérique des droits consiste à assurer d'une part la distribution des contenus numériques chiffrés, et d'autre part la procuration des droits aux utilisateurs.

Fig. 3.13. – Fonction de procuration des droits à l'utilisateur.

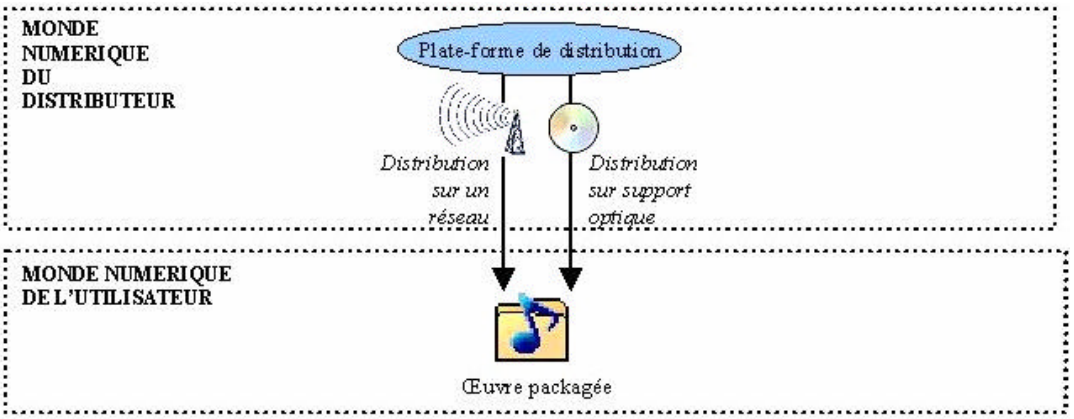


3.2.1. LA DISTRIBUTION PAR RESEAUX.

L'essentiel de la distribution des contenus numériques est assuré par des voies non sécurisées en tant que telles. La distribution sur les réseaux a ce caractère qu'il s'agisse naturellement du réseau hertzien, mais aussi du satellite, du câble, et du réseau Internet. [103]

La distribution par réseaux de télécommunications fonde l'essentiel des mesures techniques d'accès, mais justifie aussi des mesures techniques anti-copie, la distribution ayant été effectuée. Les contenus sous forme sécurisée sont censés être inutilisables, ou seulement partiellement utilisables. En tant que tels, ils peuvent donc circuler librement sur les réseaux de télécommunications. Dans ce cas, les critères de choix pour le transport de l'information n'incluent pas seulement la sécurité, mais aussi le coût de la bande passante, le mode de consommation de l'œuvre, et le parc de matériels installés chez les utilisateurs. Le niveau de sécurisation des contenus numériques est en revanche hétérogène s'agissant de la distribution sur supports optiques (CD Audio, DVD, DVD, SACD). Il est fonction de l'application de mesures techniques de protection, notamment anti-copie, natives ou non.

Fig. 3.14. – Les modes de distribution.



3.2.1.1. La distribution sur réseau de télécommunications.

Contrairement à la distribution sur support optique où l'œuvre est inerte, la distribution sur un réseau de télécommunication peut permette un certain degré d'interactivité, qui peut être mis à profit des usages comme de la sécurité. En termes d'usages, il existe différents niveaux d'interactivité : diffusion en continu d'une œuvre sur un canal donné, transmission à la demande d'une œuvre sur un canal donné, ou encore circulation à la demande des œuvres entre les utilisateurs. On peut aussi distinguer deux grandes catégories de réseaux : les réseaux fermés (par exemple pour les services audiovisuels accessibles par câble, satellite, ADSL, ou hertzien terrestre, l'*i-mode* ou *Xbox live*) et le réseau Internet (où l'établissement d'un service est libre).

---

[103] Concernant le réseau Internet, le protocole IPv6 (*Internet Protocol Version 6*, [http://www.ipv6.org/] et [http://www.ipv6forum.com/]), destiné à remplacer IPv4 aujourd'hui mis en œuvre, comporte des fonctionnalités de sécurité. Celles-ci visent par exemple la stabilité du réseau, l'authentification ou la confidentialité des données, avec certaines extensions. En revanche, elles ne concernent pas la gestion numérique des droits.

Tableau 3.1. Les catégories de réseaux.

	Diffusion en continu	**Transmission à la demande**	**Échange entre utilisateurs**[104]
Réseau Internet	Diffusion (ex. *LCI* sur TF1.fr)	Films et *singles* (ex. *Club-Internet.fr*)	*Peer to peer* (*Kazaa*, *Morpheus*…)
Réseaux fermés	Bouquets de chaînes (*TPS*, *Canalsatellite*)	Films à la demande (ex. *Multivision*)	Échange de vidéos (ex. utilisateurs *Replay*)

i. Distribution sur un réseau fermé de télécommunications.

Les réseaux fermés de télécommunications comme les réseaux hertziens terrestres et satellitaires, les réseaux câblés, les réseaux audiovisuels sur ADSL et les réseaux GSM, GPRS et UMTS ont des impératifs de sécurité similaires. Dans chaque cas, l'utilisateur a besoin, pour se connecter au réseau, d'utiliser un terminal spécifique qui prolonge le réseau fermé. L'ensemble du terminal peut être fermé et propriétaire (cas d'une console *Xbox* par exemple), ou bien simplement une carte à puce insérée dans un terminal standardisé (cas d'un terminal GSM par exemple).

Encadré 3.4. — Diffusion sécurisée de la télévision numérique sur le réseau hertzien

La numérisation de la distribution des œuvres audiovisuelles concerne également la diffusion hertzienne des chaînes de télévision. Le rapport de M. Boyon sur la « Télévision numérique terrestre » d'octobre 2002 estime que l'ouverture nationale des programmes, sur les 25 premiers sites, aura lieu en décembre 2004. [105] Les mesures techniques de protection actuellement prévues pour ce support sont similaires à celle employées sur les autres réseaux de télévision à péage, câble ou satellite. La consultation des chaînes payantes de la télévision numérique hertzienne se ferait grâce à un décodeur muni d'une carte à puce.

En l'état actuel du marché, les services fournis sur les réseaux fermés correspondent surtout à la diffusion en temps réel d'œuvres audiovisuelles. **Ayant donc à protéger le même type d'œuvre dans des conditions similaires, les industriels ont essayé de se mettre d'accord pour adopter ensemble un système unique de protection**. Disposer d'un système unique présente pour les industriels l'intérêt de réduire le coût de la puce électronique réalisant l'opération de déchiffrement. En Europe, le système de chiffrement des œuvres est celui de DVB.

Encadré 3.5. — *Canal+ technologies* : distribution sécurisée sur un réseau de diffusion audiovisuelle

La sécurisation des réseaux de télévision numérique par câble et par satellite repose sur l'utilisateur de décodeurs matériels, dans lesquels est insérée une carte à puce. Les programmes sont chiffrés selon l'algorithme symétrique normalisé par DVB qui présente l'avantage d'être rapide. [106] La clef symétrique ainsi utilisée doit être transmise de façon sûre au décodeur installé chez l'utilisateur. Cette clef est chiffrée, selon un algorithme asymétrique, de façon personnalisée pour chaque décodeur, en fonction de la clef privée stockée dans chaque carte à puce. Ainsi, la carte à puce est capable de déchiffrer le message contenant la clef symétrique, qui représente les droits de l'utilisateur sur les programmes, et de stocker cette clef. Si un utilisateur cesse de payer son abonnement, le serveur central peut envoyer un nouveau message crypté au décodeur correspondant, afin de suspendre ses droits.

[104] Pour l'analyse, dans le respect des droits d'auteur et droits voisins ; donc de contenus protégés ou de copies issues du trou analogique (cf. *infra*).
[105] http://www.ddm.gouv.fr/rapports_etudes/documents/RAPPORTBOYON.rtf
[106] Les algorithmes retenus par DVB sont décrits dans la partie II.1.3.1.

Ce système est très robuste puisque, après plus de dix années d'exploitation, il n'a toujours pas été cassé. Aujourd'hui cet algorithme n'est pas soupçonné de faiblesse. Les déchiffreurs DVB sont extrêmement répandus, mais uniquement sous forme matérielle et non logicielle, tandis que les chiffreurs DVB sont réservés aux professionnels. L'algorithme est suffisamment complexe pour résister aux attaques tout en étant suffisamment souple pour qu'un déchiffreur DVB puisse déchiffrer le flux en temps réel. À chaque contenu chiffré selon l'algorithme DVB, est associée une clef permettant de le déchiffrer (cf. *supra*).

Encadré 3.6. — Diffusion sécurisée de la télévision sur ADSL.

Le déploiement de la télévision par ADSL a démarré en France en 2002, par exemple dans le cadre de l'offre *Freebox de Free Telecom*, et du test lancé par *TF1* pour son projet « *Dream-TV* ». Ces offres utilisent deux flux distincts dans la bande passante rendue disponible par la technologie ADSL : l'un pour l'accès à l'Internet haut débit, l'autre pour les programmes audiovisuels.
Les principales caractéristiques de cette technologie sont :
– l'accès aux programmes audiovisuels sur le poste de télévision moyennant un modem ADSL spécifique ;
– une qualité d'image équivalente à la diffusion par satellite ;
– la nécessité de déployer un réseau spécifique qui s'appuie, dans le cas des opérateurs concurrents à *France Télécom*, sur le dégroupage de la boucle locale.
Les technologies de contrôle d'accès mises en œuvre sur les autres réseaux et reposant sur un chiffrement avec l'algorithme DVB, comme *Viaccess*, peuvent être réutilisées dans le cadre de la diffusion TV sur ADSL, moyennant une adaptation au monde IP. Les utilisateurs disposent en effet d'un décodeur, ou d'un modem ADSL spécifique, dans lequel ils pourront insérer une carte à puce contenant leur clef privée et leurs droits. De plus, la liaison bidirectionnelle et privative entre le DSLAM[(107)], totalement sous le contrôle de l'opérateur, et le décodeur, totalement propriétaire, autorise la mise en place de mesures de protection supplémentaires. Contrairement au cas des réseaux câblés et satellite, le décodeur situé chez l'abonné est techniquement un prolongement du DSLAM, ce qui permet :
– de mettre en place des mesures de contrôle d'accès au niveau de la couche réseau, en tenant compte par exemple du numéro de la ligne, du numéro du plot de renvoi au répartiteur, et de l'identifiant réseau du décodeur,
– de prévoir un système de mise à jour des droits plus rapide et plus élaboré,
– de détecter plus facilement les opérations malveillantes qui pourraient être conduites sur un décodeur.
Enfin, il est prévu que les décodeurs ne soient munis que d'une sortie analogique du type PAL, évitant ainsi toute copie numérique.

Contenu	**Technologie de cryptage** - Protection de la diffusion : accès conditionnel - Protection de la production / DRM
Application	***Middleware*** - Authentification (code d'accès : login) - Identification personnelle (code PIN)
Réseau	**Couche réseau** (ATM et IP) - Identification unique de l'utilisateur par un VC ATM - Adressage IP fixe du terminal

(107) Équipement installé dans les répartiteurs et qui permet de transformer les lignes téléphoniques en lignes DSL

ii. La distribution sur un réseau de communication ouvert : Internet.

Le réseau Internet ouvert autorise quiconque à s'y connecter librement pour émettre et recevoir des contenus de toute nature sans qu'une spécification matérielle relative au terminal ne puisse constituer une limitation. Les réseaux correspondant sont interconnectés et constituent ce que l'on appelle Internet. Un tel réseau étant totalement ouvert physiquement. Ce sont donc des logiciels qui assurent le contrôle d'accès aux services non libres de droits.

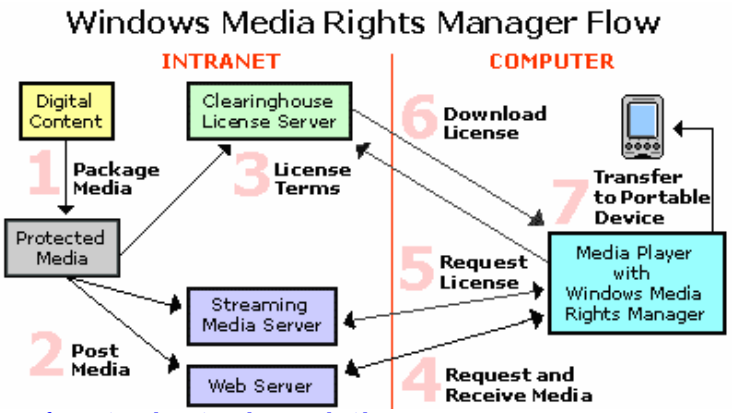
Sur le réseau Internet, l'opération de déchiffrement assurant la même fonction que dans le cas des réseaux fermés, se fait nécessairement de manière logicielle. Par exemple, lorsqu'un utilisateur consulte une œuvre sur son ordinateur personnel via Internet, un programme logiciel installé réalise l'opération de déchiffrement. Ce logiciel est généralement fourni gratuitement conjointement avec les œuvres chiffrées. Le monde de l'informatique et des logiciels offre davantage de flexibilité. En particulier les économies d'échelle qui inciteraient les industriels à utiliser un système de chiffrement unique sont moins évidentes. Les algorithmes sont donc, en général, propres à chaque système et sont privés.

Encadré 3.7. — *Windows Media Player* : distribution sécurisée sur Internet

Le logiciel de lecture d'œuvres numériques multimédias développé par *Microsoft*, *Windows Media Player*, est dans sa dernière version partie intégrante d'un système de gestion numérique des droits : *Microsoft® Windows Media™ Rights Manager*. Ce système permet une distribution sécurisée des œuvres numériques. Le plan d'affaires pour *Microsoft® Windows Media™ Rights Manager* repose sur les principes — devenus classiques — suivants :

- *Windows Media Player* étant systématiquement livré avec Windows, la plupart des utilisateurs disposent déjà d'une version de cet outil sur leur ordinateur, *activée par défaut*, ce qui supprime la barrière ergonomique de l'installation d'un décodeur ;
- la plupart des utilisateurs disposent déjà sur leur ordinateur d'une installation de *Windows Media Player*, ce qui supprime la barrière ergonomique de l'installation d'un décodeur ;
- le décodeur *Windows Media Player* est livré « gratuitement » avec le système d'exploitation *Windows*, l'encodeur correspondant est mis à disposition des distributeurs à un coût très attractif ;
- les droits sur les œuvres étant entièrement centralisés au niveau d'un serveur informatique, il est aisé de les faire évoluer en fonction des conditions du marché,
- des formules d'abonnement et de location peuvent être proposées aux utilisateurs.

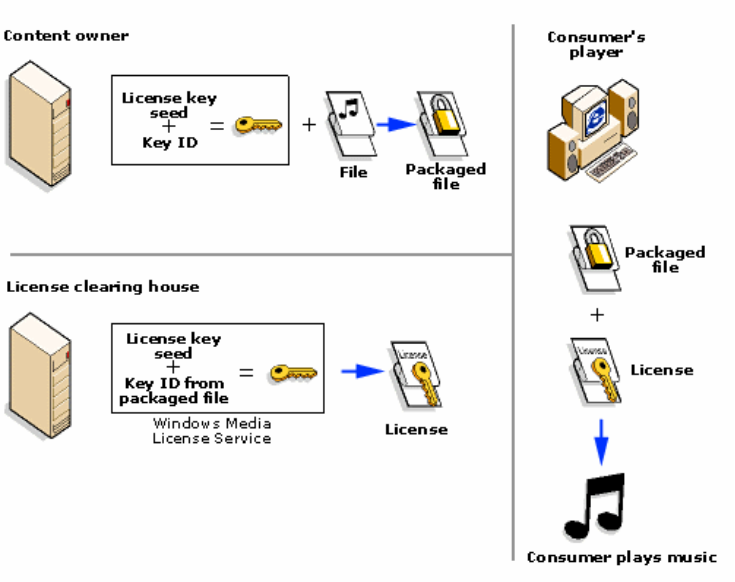
Fig. 3.15. – Gestion des flux de *Windows Média Rights Manager*



http://www.microsoft.com/windows/windowsmedia/drm.asp

Microsoft® Windows Media™ Rights Manager met en œuvre des techniques de chiffrement, si bien que seul un lecteur *Windows Media* valide et muni d'une une licence peut déchiffrer une œuvre sécurisée. L'envoi et la mise et jour des droits se fait sur Internet, grâce à une connexion à un serveur de droits. Chaque version de *Windows Media Player* installée sur chaque ordinateur possède une licence qui lui est propre, permettant ainsi une gestion individualisée des droits, et rendant possible une révocation des lecteurs compromis. Cette licence contient un secret propre à chaque utilisateur qui permet une transmission sécurisée des droits.

Fig. 3.16. – Chiffrement de *Windows Média Rights Manager*



http://www.microsoft.com/windows/windowsmedia/drm.asp

Conçu en étroite relation avec les systèmes d'exploitation *Microsoft Windows® Millennium Edition* et *Microsoft Windows XP*, *Windows Media Player* assure la protection du flux lorsqu'il circule en clair entre le logiciel de déchiffrement et les pilotes des cartes son et vidéo. Même si ce système de sécurité est totalement logiciel, il est suffisamment robuste pour que la quasi-totalité des utilisateurs ne puisse pas le contourner. Des pirates professionnels ont parfois réussi à le mettre en défaut, dans ce cas *Microsoft* a publié une mise à jour rétablissant la protection des œuvres.

Encadré 3.8. — Distribution sécurisée sur les réseaux mobiles GPRS, EDGE et UMTS

Les réseaux mobiles de nouvelle génération, comme le GRPS, permettent la distribution d'œuvres audiovisuelles ayant une valeur commerciale. Il s'agit par exemple de sonneries, de logos et de fonds d'écran pour personnaliser son terminal. Les terminaux mobiles étant naturellement dotés de moyens de communication, notamment via l'envoi d'e-mails vers un autre terminal ou un ordinateur, ou via une liaison « *bluetooth* », la question de la protection technique de ces œuvres se pose. Les protocoles de communication employés sur les réseaux mobiles de nouvelle génération, comme l'« *i-Mode* », sont proches de ceux de l'Internet. Il en résulte que les mesures techniques de protection sont proches de celles développées pour le réseau Internet. Elles tiennent toutefois compte des différences entre un ordinateur et un terminal mobile, en particulier en termes de puissance de calcul et de bande passante. Les terminaux mobiles étant munis d'une carte à puce, la carte SIM, il est possible de concevoir des mesures techniques de protection mettant à profit cette carte à puce. Un niveau de robustesse plus élevé pourrait ainsi être atteint, mais les conditions de développement et de fonctionnement seraient également différentes, puisque la carte à puce est la propriété de l'opérateur. Dans le cas d'une solution purement logicielle, l'opérateur est neutre vis-à-vis du système de protection. Un travail de normalisation à ce sujet est effectué au sein de l'*Open Mobile Alliance*.[108].

[108] cf. [http://www.openmobilealliance.org/]

Encadré 3.9. — *Medialive* : sécurisation de la vidéo par une connexion à un serveur

De manière générale, la séparation de la transmission de l'œuvre de celle de la représentation numérique des droits du destinataire sur cette œuvre, principe à la base des systèmes de DRM, n'exclut pas que ces transmissions aient lieu simultanément, en temps réel et sur un même réseau. Dans ce cas :

– le niveau de sécurité est supérieur, d'abord parce qu'il n'existe pas de copie locale de l'œuvre mais surtout (un utilisateur averti pourra toujours enregistrer un flux numérique) parce que la transmission point à point, par oppposition à la diffusion, renforce l'identification de l'utilisateur, les paramètres de sécurité de chaque copie originale transmise peuvent être personnalisés et le dialogue continu entre le lecteur et le serveur, au moment de la jouissance des droits, permet de suspendre la distribution de l'œuvre si un incident de sécurité survient ;

– le débit requis sur un réseau de télécommunication est plus elevé puisque la transmission d'une œuvre en temps réel nécessite une large bande passante.

Dans ce contexte de recherche d'un *optimum* entre débits nécessaires et niveau de sécurité, Medialive propose une technologie singulière applicable aux vidéos. Le flux vidéo est découpé en deux morceaux: un flux vidéo de format identique, contenant 99% du «sens » de l'œuvre originale, mais inintelligible pour un œil humain, et un fichier plus petit contenant le 1% restant. Lors de la vision de l'œuvre, seul ce dernier est transmis en temps réel sur le réseau, simultanément à la transmission de la représentation des droits. Ainsi:
– le niveau de sécurité au moins aussi bon que si la totalité de l'œuvre était envoyée en temps réel, il est même supérieur puisque le réassemblage des deux flux est sécurisé ;
– une connexion bas débit suffit, puisque la représentation des droits et le fichier contenant 1% du sens de l'œuvre sont peu volumineux.

Champ d'application de la technologie

Cette technologie s'applique aux fichiers de sons ou de vidéos. Elle est dépendante du codage utilisé, mais sera rendue compatible avec tous les types de codage. Le prototype fonctionne avec MPEG 2, qui est aujourd'hui le codage le plus largement utilisé. Les utilisateurs doivent être équipés d'un décodeur spécifique conçu pour la technologie *Medialive*. Ce décodeur doit être relié à un réseau de télécommunications, afin de consulter les droits de l'utilisateur, et comporte une prise péritel sur laquelle peut être branché un téléviseur. Les services de télévision personnalisée, où l'utilisateur n'est plus tributaire d'une grille de programmation, pourraient constituer un cadre d'application de cette technologie. Dans ce cas, le décodeur contiendrait un disque dur, faisant office de magnétoscope numérique.

Cette technologie pourrait également être portée vers les ordinateurs personnels, qui devraient alors s'équiper d'une carte spécifique. Par ailleurs, cette technologie permet d'identifier et de localiser les utilisateurs souhaitant accéder à un programme. Elle permet donc d'ajuster les tarifs en fonction du profil de l'abonné, de son lieu de résidence et de l'heure. Les éditeurs et distributeurs pourraient alors adapter leur offre pour qu'elle corresponde plus précisément à la demande des utilisateurs. Enfin, la technologie autorise la prévisualisation d'une œuvre, avec éventuellement un brouillage progressif. La solution de Medialive peut s'intégrer facilement dans les systèmes actuels de distribution de la vidéo, qu'ils mettent en œuvre des supports optiques, des réseaux fermés de télécommunications ou le réseau internet.

Le système *Medialive* peut être adapté localement aux différentes législations, et cela au moment de la visualisation de l'œuvre et non pas uniquement au moment de la production de l'œuvre.
La copie privée est possible, selon des modalités paramétrables par les titulaires de droits. Elle présente l'avantage d'être totalement liée à l'utilisateur par l'intermédiaire de la carte à puce. Ainsi, un utilisateur peut « voyager » avec ses copies privées en emportant la carte à puce avec lui, mais ne peut diffuser de façon incontrôlée les copies réalisées auprès d'autres personnes.
Principes de fonctionnement

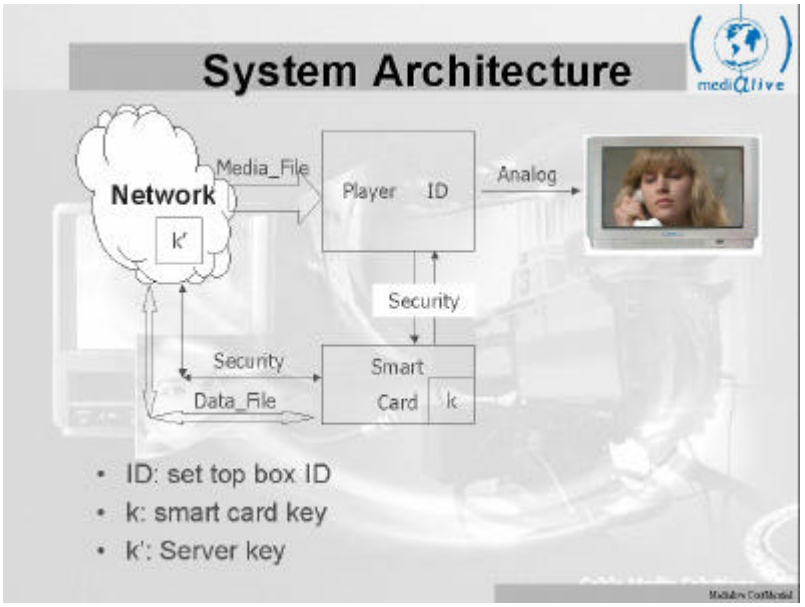
Édition de l'œuvre. Lorsqu'un éditeur souhaite protéger une œuvre dont il dispose un exemplaire sous forme numérique, le logiciel d'extraction *Medialive* lui permet, à partir de cet exemplaire, de générer :

– un fichier *Media_Files* de même nature que l'œuvre dont le volume est équivalent. La lecture de ce fichier est possible mais le contenu est brouillé, non visible par un œil humain ;
– un fichier crypté *Data_Files*, dont le volume représente environ un centième du volume de l'œuvre. Le fichier *Data_Files* est placé sur le serveur de droits, appelé *Data_Files_Server*.

Distribution de l'œuvre. Le fichier *Media_Files* est distribué librement par des moyens de télécommunications (ADSL, câble, fibre optique, satellite) ou bien par les circuits de distribution classique (CD, DVD) jusqu'au lecteur *Medialive* situé chez l'utilisateur. Ce lecteur, relié au réseau Internet, peut comporter un lecteur CD/DVD et/ou un disque dur sur lequel plusieurs fichiers *Media_Files* peuvent être stockés. Un téléviseur peut être branché directement sur ce lecteur.

Visualisation de l'œuvre. Le lecteur se connecte au serveur *Data_Files_Server* grâce à une liaison Internet moyen ou haut débit (ADSL, câble, GPRS, UMTS). Ce lecteur, identifié par un numéro unique, et contenant une carte à puce identifiée elle-aussi par un numéro unique, reçoit de la part du *Data_Files_Server* un flux de données cryptées. Le décryptage de ce flux en temps réel permet à partir du fichier *Media_Files*, de visualiser le contenu de l'œuvre.

Fig. 3.17. – Architecture du système *Medialive*



Robustesse du système *Medialive*

Piratage du fichier *Media_Files.* L'absence totale de protection lors de la distribution du fichier *Media_Files* ne pose pas de problèmes car la visualisation de ce fichier est brouillée. Ce brouillage ne résulte pas d'un chiffrement des données, mais de l'absence d'une part des données. Sans les données manquantes, le flux vidéo perd son sens pour un utilisateur humain et il est garanti que le possesseur d'un fichier *Media_Files* ne pourra pas visualiser l'œuvre originale.

Interception du flux de données envoyé par le *Data_Files_Server* au lecteur. Une telle interception est physiquement possible. Cependant ce flux de données, s'il était enregistré et rejoué auprès d'un autre lecteur, ou du même lecteur à un autre instant, ne permettrait pas de visualiser le contenu de l'œuvre. En effet, ce flux de données résulte du dialogue entre trois éléments :
– le serveur des droits *Data_Files_Server ;*
– le processeur situé à l'intérieur du lecteur ;
– la carte à puce située à l'intérieur du même lecteur.
Puisque le processeur et la carte à puce situés à l'intérieur du lecteur génèrent dynamiquement et de façon aléatoire des clefs servant à identifier le dialogue, les flux de données qui pourraient être

enregistrés lors de la visualisation d'une œuvre ne pourraient pas être réutilisés afin de commander une nouvelle visualisation. En effet, ces flux de données ne répondraient pas aux requêtes du processeur et de la carte à puce et seraient ignorés.

Piratage des éléments sécurisés. La visualisation d'une œuvre résulte du dialogue sécurisé entre le *Data_Files_Server*, le processeur et la carte à puce. Une attaque possible consisterait à comprendre le fonctionnement de l'un de ces trois éléments, afin de le contrôler.
Le processeur et la carte à puce sont des éléments matériels. Le traitement des données par ces éléments est réalisé par des circuits intégrés miniaturisés dont l'architecture est extrêmement complexe. L'intrusion à l'intérieur d'un processeur ou d'une carte à puce afin d'en comprendre le fonctionnement nécessite des moyens informatiques et matériels extrêmement lourds, hors de portée des pirates amateurs ou professionnels.
Le serveur est logiciel, mais physiquement inaccessible. Des pirates pourraient envisager de prendre le contrôle du serveur en utilisant la liaison qui sert normalement au dialogue avec le lecteur. Cependant les techniques de protection des serveurs aujourd'hui existantes sont suffisamment fiables pour qu'une telle attaque soit très difficile, même pour des pirates professionnels.

Piratage du dialogue entre les éléments sécurisés. Les clefs de cryptage utilisées pour les échanges entre le serveur, le processeur et la carte à puce ont une longueur de 128 bits. Par conséquent, il faudrait des moyens informatiques importants pour arriver à briser ce dialogue. De plus les technologies qui sont utilisées au moment de la visualisation de l'œuvre peuvent être adaptées et optimisées en permanence, ceci est un avantage par rapport à des solutions de cryptage qui sont utilisées une fois pour toutes pour protéger une œuvre diffusée.
Dans l'hypothèse improbable où des pirates professionnels y parviendraient, ils auraient piraté le contenu d'une œuvre, qu'ils pourraient reproduire et diffuser librement. Cela ne signifie pas pour autant qu'ils pourraient donner à tous les internautes une information qui leur permettrait, à leur tour, de pirater d'autres œuvres. En effet, chaque dialogue est propre au processeur du lecteur, à la carte à puce, et à chaque œuvre. De plus, même la lecture des autres exemplaires de l'œuvre piratée pourrait être à nouveau sécurisée en réalisant une nouvelle extraction des *Data_Files* et en mettant à jour le *Data_Files_Server*, rendant obsolètes tous les *Media_Files* précédemment distribués.
La communication permanente entre les éléments sécurisés, dont le serveur, contribue à la détection des attaques dont pourrait faire l'objet le système. Le niveau de sécurité peut être régulièrement amélioré par des mises à jour logicielles, pilotées depuis le serveur central, voire par un envoi de cartes à puce plus perfectionnées.

3.2.1.2. La distribution sur supports optiques.

La distribution sur support optique concerne surtout les œuvres musicales et les œuvres audiovisuelles et cinématographiques. Elle peut naturellement concerner aussi d'autres contenus numériques comme les logiciels, les produits multimédias, notamment les jeux vidéos, les bases de données, etc. fixés sur des formats de supports optiques différents (Cédérom DVD Rom).[109]

i. Distribution sur support optique d'œuvres musicales.

L'essentiel du piratage numérique dans le domaine musical tient à l'absence native de mesures techniques de protection appliquées aux CD Audio, notamment par comparaison au format du DVD qui comporte la mesure technique de protection qu'est le CSS (*Content Scrambling System*). Le lancement de nouveaux supports audio numériques peut

[109] L'analyse de la sécurisation des supports optiques X Rom sort du champ de l'étude réalisée dans la perspective de la directive 2001/29 qui vise des mesures techniques de protection des œuvres, sans préjudice des « mesures spéciales de protection » des logiciels qui relèvent de la directive 91/250 ou du droit des bases de données établi par la directive 96/9.

être l'occasion de combler cette différence entre le secteur de l'audio et du cinéma. Cependant, si le standard DVD devait s'imposer pour le cinéma comme pour l'audio, il n'est pas certain que cet écart demeure. En pratique, cela signifierait que la copie numérique audio resterait aisée, tandis que la copie numérique d'œuvres audiovisuelles et cinématographiques resterait – principalement et techniquement – très limitée voire impossible.

Encadré 3.10. — Les « précédents » non sécurisés du DVD : vidéodisques, vidéo CD Audio.

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

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

– Le CD Audio : un format nativement non sécurisé.

L'introduction du standard CD Audio développé par *Sony* et *Philips* marque le point de départ de la distribution de la musique sous forme numérique.

– **Le « livre rouge** », publié en 1980, définit le **CD Audio,** dont la capacité utile est de 750 Mo, à travers le système de codage et les procédures de corrections d'erreur ;

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

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

Le standard du CD Audio ne prévoit nativement aucun système de protection de l'œuvre. Normalement, tout lecteur peut accéder aux données, et les transmettre vers un graveur ou un ordinateur, sans avoir besoin de demander les droits sur l'œuvre. De plus, ce standard laisse aux industriels une très faible marge de manœuvre pour mettre en place des systèmes d'accès ou de protection contre la copie [(110)]. Ils sont donc obligés d'inscrire les mesures techniques à la frontière de la norme, allant parfois au-delà. Les écarts avec la norme qui en résultent sont à l'origine des problèmes de «jouabilité » des supports optiques, c'est-à-dire de compatibilité entre les CD Audio protégés et certains lecteurs, notamment des lecteurs de CD Audio dans les autoradios. Dans ce contexte, les standards successifs du CD Audio conduisent à exclure du sein d'un système numérique de gestion de droits la distribution des contenus numériques musicaux sous formes de CD Audio.[(111)]

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

[(110)] Les systèmes de protection pour les CD Audio sont décrits dans la partie II.3.2.
[(111)] cf. aussi *supra*.

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

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

– Des avantages de qualité et de pureté de la restitution sonore grâce à un procédé d'enregistrement : le DSD *(Direct stream digital)* plus efficace que le PCM (*Pulse Code Modulation*).[112]

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

– Un format de haute définition qui ne diminue pas l'offre de titres puisque la précision de gravure étant plus fine, le stockage d'informations (4,7 Go) est plus élevé que celle d'un CD Audio (780 Mo).

La protection technique du SACD et sa robustesse relèvent d'une solution essentiellement cryptographique. Les données audio sont enregistrées sur le support de façon cryptée. Le procédé physique de gravure est en revanche le même que pour enregistrer un CD Audio classique, mais **les données numériques ne peuvent être interprétées que si on possède la clé de décryptage**. Cette clé comporte une partie commune à tous les disques SACD et une partie propre à chaque titre. La partie commune se trouve dans les lecteurs SACD, inscrite physiquement dans la puce de lecture. La partie propre au titre est inscrite sur le disque par un procédé de gravure spécifique.[113] De plus, **les données d'en-tête d'un disque SACD sont cryptées et inscrites avec le même procédé de gravure spécifique**. Ces données indiquent le nombre de pistes, leur durée et leur position sur le disque, elles sont indispensables à la lecture. La clé et les données d'en-tête, imprimées sur le disque de façon inhabituelle, constituent un « filigrane » (la clé de décryptage se trouve inscrite en dur sur la puce de lecture d'un lecteur SACD).

La robustesse de la protection technique est fondée sur le cumul de plusieurs types de sécurité et notamment la licence. En premier lieu, un SACD ne peut-être utilisé sur un lecteur dépourvu de licence. Son utilisation requiert la lecture des données d'en-tête qui, étant gravées sur le filigrane, ne peuvent pas être lues avec un lecteur ordinaire de CD Audio. Ces données d'en-tête sont cryptées et donc inutilisables si l'on ne dispose pas d'un lecteur SACD muni d'une licence. En second lieu, si un SACD est copié avec un enregistreur en vente libre, il ne fonctionnera pas. En effet, **les enregistreurs CD Audio que l'on trouve sur le marché n'ont pas la capacité de graver le filigrane caractéristique des SACD.** Or, les enregistreurs SACD produits

(112) Les filtres utilisés pour l'enregistrement garantissent une plus grande fidélité et la fréquence d'échantillonnage (nombre d'enregistrements du signal sonore par seconde) est égale à 2,82 GHz contre 44,1 MHz pour le CD, les hautes fréquences ne sont donc plus perdues. Enfin le SACD apporte une innovation en matière de dynamique (écart entre le son le plus bas et le son le plus fort), celle-ci est égale à 122 dB pour un enregistrement SACD, contre 96 dB pour enregistrement CD.

(113) PSP (*Pit signal processing*) : la largeur du sillon et non plus seulement la profondeur est porteuse d'informations.

exclusivement par *Philips* et *Sony* ne devraient être que l'objet d'une location aux professionnels et jamais mis à la vente. Enfin, dans tous les cas, les données audio restent cryptées, par conséquent sans la clé inscrite pour une partie sur le filigrane du SACD et pour l'autre sur la puce de décodage d'un lecteur, les données audio sont illisibles. **La clé utilisée mesure 80 bits et n'apparaît jamais de façon explicite sur un bus de données à l'intérieur d'un lecteur. L'algorithme de chiffrement est gardé secret et il est implanté en dur ce qui rend impossible une tentative de rétro-conception**.[114] Ainsi, le piratage d'un SACD nécessiterait de lourdes infrastructures.

Encadré 3.11. — La compatibilité entre CD Audio et SACD

Les lecteurs de SACD. Tous les lecteurs SACD mis sur le marché permettront de lire les CD Audio ordinaires, afin que les utilisateurs puissent continuer à utiliser ceux qu'ils possèdent. Chaque lecteur SACD possède deux émetteurs lasers, un à 780 nm pour lire les CD Audio traditionnels et un à 650 nm pour lire les SACD.

Les lecteurs CD Audio. Un lecteur CD Audio ne peut pas lire un disque SACD, en effet il lui manque entre autres éléments, un émetteur laser à 650 nm, la technologie pour lire le filigrane, les clés de décryptage et la puce de lecture spécifique. Il est inconcevable de faire évoluer simplement un lecteur CD Audio vers un lecteur SACD, les utilisateurs doivent donc acheter un nouvel équipement.

Les lecteurs hybrides. Certains éditeurs mettent sur le marché des CD Audio hybrides qui sont compatibles à la fois avec les lecteurs CD Audio et les lecteurs SACD. Toutefois un CD Audio hybride lu avec un lecteur CD Audio ordinaire ne permet de bénéficier ni de la qualité sonore du SACD ni du *Surround*. Il peut également être piraté très facilement.

La commercialisation du SACD depuis plusieurs années traduit de réelles difficultés qui tiennent à trois éléments : l'étroitesse du catalogue (moins de 200 titres disponibles dont la moitié bénéficie de l'enregistrement en Multi-channel *Surround*), l'écart de prix entre SACD (~20€) et CD Audio (~15€), enfin le coût des lecteurs SACD (~250 €) dont la gamme est encore réduite en sorte que le lancement du SACD reste dérisoire : ~ 6600 lecteurs SACD ont été vendus dans le monde en 2001. L'échec commercial pour le moment constaté tient en réalité beaucoup aux choix des standards techniques – incompatibles – proposés aux *majors* entre le SACD et le DVD-Audio (DVD-A). L'incertitude pèse autant sur la formation d'un catalogue attractif que sur les attitudes d'attente des consommateurs.

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

Le DVD audio est le standard DVD Audio publié par le Forum DVD en 1990.[115] *BMG Entertainment*, *EMI Music*, *Universal Music* et *Warner Music* se sont engagés à éditer des DVD Audio. Une entreprise similaire a été conduite par le DVD Forum, conduisant à la publication de la norme DVD-Audio en 1999, révisée en 2000 pour tenir compte du fait que le système de protection des DVD ait été cassé.

Au sens de la norme, un DVD-Audio ne peut en général pas être lu sur un lecteur DVD-Video. La plupart des DVD Audio mis en vente sont cependant compatibles avec les lecteurs de DVD Video, ils présentent alors le même niveau de sécurité que les DVD Vidéo, c'est-à-dire qu'ils peuvent être copiés en utilisant un lecteur DVD d'ordinateur. De plus, contrairement aux films, les extraits sonores peuvent circuler facilement sur les réseaux *peer to peer* car leur taille est plus modeste. Les DVD-Audio non compatibles

(114) Obtention de l'algorithme de cryptage par une lecture des instructions envoyées au processeur à l'intérieur du lecteur SACD.

(115) DVD Forum [http://www.dvdforum.org/forum.shtml]

avec les DVD-Video, donc plus robustes, sont protégés grâce la technologie CPPM (*Content Protection for Precorded Media*) développée par le consortium « 4C entity » Il cherche à partir d'un cadre de sécurité de la plupart des contenus numériques (CSPA) à établir des technologies de protection du DVD A.[116] La technologie CPPM remplace la technologie CSS2 qui était initialement prévue pour le DVD-Audio avant que CSS ne soit cassé.[117] Elle est plus robuste, notamment au niveau de la gestion des clefs, mais reprend les concepts fondamentaux de CSS.[118]

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

Encadré 3.12. — Un exemple de couplage entre distribution sur support optique et *DRMS*

Même si la distribution d'une œuvre est réalisée sur supports optiques, il est possible de la coupler avec un système en ligne de gestion des droits. Dans un tel système, les droits présents sur le support optique sont réglés lors de l'achat du support, ils permettent de déchiffrer une partie des œuvres présentes sur le disque. Pour accéder aux autres œuvres présentes sur le disque, il faut télécharger en ligne d'autres droits grâce à un système classique de DRM, comme celui de *Microsoft*. Cette idée a été exploitée lors de la diffusion gratuite d'un single du groupe *Oasis* à l'intérieur du *Sunday Times* en Angleterre. Les droits présents sur le disque permettaient d'écouter le titre une seule fois. Afin de l'écouter à volonté, il fallait acheter en ligne des droits supplémentaires. De même, le dernier album de *Daft Punk* est livré avec un code qui permet, en se connectant en ligne à un serveur de droits, d'avoir accès à des œuvres supplémentaires.

ii. Distribution sur support optique des œuvres audiovisuelles.

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

Les principales protections prévues par la norme DVD sont les suivantes :
– Le « système *Macrovision* », qui fait en sorte que le signal vidéo analogique émis par un lecteur DVD ne soit pas enregistrable sur une cassette VHS ;[119]

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

Aujourd'hui il est possible de télécharger sur Internet des « *rippers* » de DVD, c'est-à-dire des logiciels capables de déchiffrer un DVD et d'inscrire en clair le contenu de l'œuvre sur un autre support. On peut remarquer que le premier « *ripper* » a été écrit

[116] CSPA (*Content Protection System Architecture*) [http://www.4centity.com/data/tech/cpsa/cpsa081.pdf]
[117] CSS2 était une version de CSS améliorée et adaptée au DVD Audio cf. *supra*.
[119] *Video Copy Protection* [http://www.macrovision.com/solutions/video/copyprotect/index.php3]

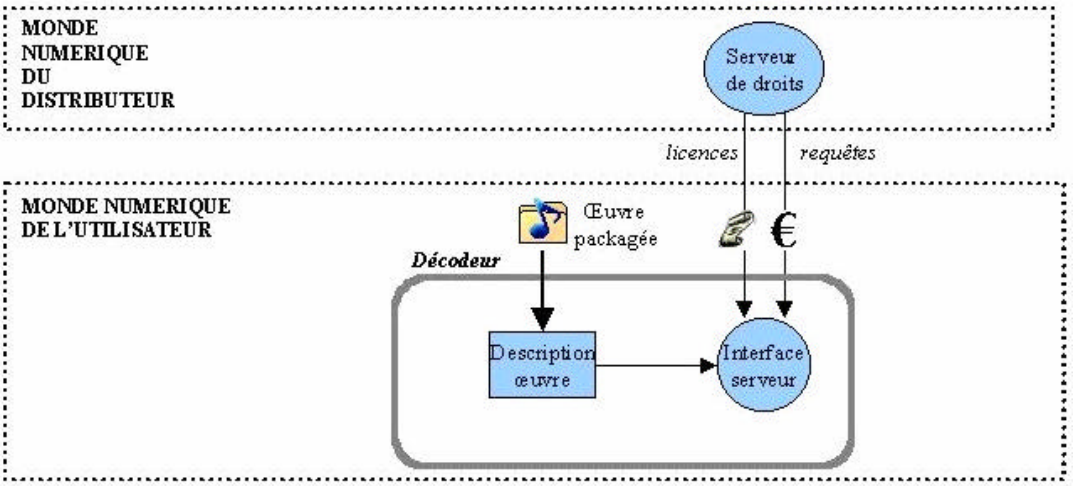
après la décompilation d'un logiciel de lecture de DVD, livré avec un lecteur de DVD pour ordinateur personnel. On peut s'interroger si le système CSS aurait été cassé si aucun lecteur DVD pour PC, nécessairement accompagné d'un pilote donc d'un lecteur logiciel, n'avait été mis en vente. L'impact de ce piratage est toutefois resté assez limité, dans la mesure où les réseaux d'échange ne sont encore ni assez rapides ni assez ergonomique pour permettre le téléchargement de film, et où les graveurs de DVD-ROM restent encore assez chers.

3.2.2. LA RECONNAISSANCE DES CONTENUS ET LA REQUETE DES DROITS

Quel que soit le mode de distribution mis en œuvre, réseau de télécommunications électroniques ou support optique, s'il existe un système de protection, l'utilisateur dispose sur son équipement de l'œuvre sous forme chiffrée.

Pour exploiter l'œuvre, l'utilisateur doit acquérir les droits correspondants auprès d'une autorité certifiée par les titulaires de droits pour délivrer ceux-ci. Dans le cadre d'un système numérique de gestion de droits, cette autorité se matérialise généralement sous la forme d'un serveur de procuration des droits.

Fig. 3.18. – Fonction d'acquisition de droits.



La requête formulée par l'utilisateur au serveur de droits doit inclure un identifiant de l'œuvre, afin que le serveur puisse lui fournir la clef qui correspond bien à l'œuvre. Cela suppose que le programme réalisant la requête sache reconnaître une œuvre sous sa forme chiffrée, qu'il connaisse l'adresse d'un serveur autorisé à donner ces droits, et qu'il utilise le même vocabulaire que ce serveur pour décrire les œuvres. Plus précisément ils doivent partager les mêmes langages de description des œuvres et des droits.

Les éléments d'interopérabilité entre le programme réalisant la requête des droits et le serveur de droits sont les suivants : le langage de description de l'œuvre, le langage de description des droits, et enfin, l'adresse des serveurs autorisés à procurer ces droits. Cette interopérabilité nécessite, soit qu'un même industriel produise ces deux éléments, soit que des industriels se donnent et respectent des normes. Outre des identifiants de l'œuvre et de la nature des droits demandés, la requête doit comporter un identifiant de l'utilisateur, et une authentification de l'utilisateur, c'est-à-dire une preuve que l'identité présentée par l'utilisateur est bien conforme à la réalité.

3.2.3. LA SECURISATION DE LA PROCURATION DES DROITS.

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

3.2.3.1. L'authentification.

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

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

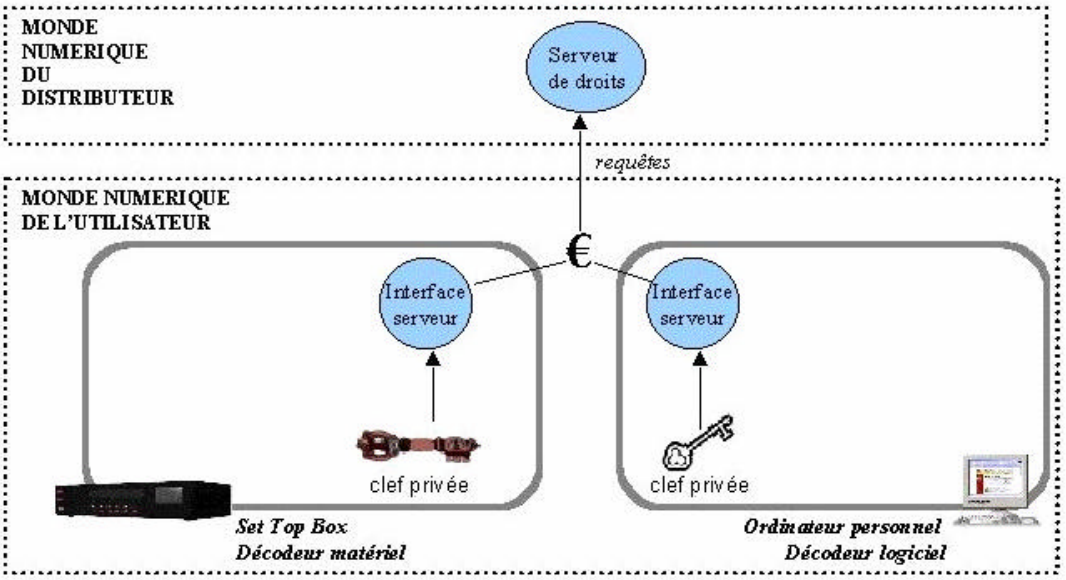
– L'authentification est une mesure technique de protection. Elle repose en général sur un système de clefs publiques et privées. L'utilisateur possède chez lui un secret, sous forme de clef privée, qui lui est propre et connu seulement de son processus technique d'identification. Cela signifie qu'il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

i. Existence physique de l'authentification.

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

Le processus technique d'authentification doit répondre aux exigences suivantes : **le secret ne peut être divulgué à personne, pas même à l'utilisateur**, et le processus technique d'authentification doit pouvoir, à la demande de l'utilisateur, établir avec le serveur de droits un dialogue authentifiant l'utilisateur. **Il existe deux grandes catégories de systèmes d'authentification, en fonction de la représentation du secret associé à chaque utilisateur.** La représentation de ce secret peut être matérielle (située par exemple, dans une carte à puce ou une puce électronique) ou bien logicielle (située par exemple, la dans la mémoire vive ou le disque dur d'un ordinateur).

Fig. 3.19. – Fonction de protection de l'authentification.



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

– *Situation d'un authentifiant logiciel.* Dans ce cas, le secret est le plus souvent généré de façon aléatoire, puis est stocké dans une mémoire informatique, mémoire vive ou disque dur par exemple.

ii. Robustesse des solutions d'authentification.

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

Une rétro-conception (*reverse engineering*) logicielle est une opération complexe, hors de portée de la quasi-totalité des utilisateurs. Toutefois, elle est aisément réalisable par un pirate puisqu'il existe des outils de « *débugage* » et de décompilation. Celle-ci est

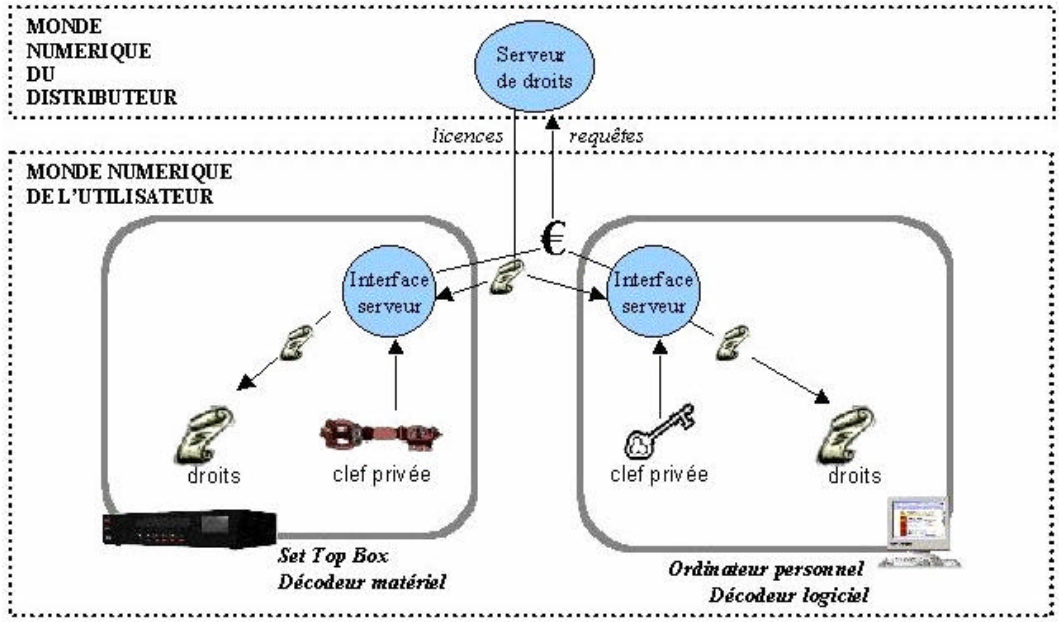
autorisée à des fins d'interopérabilité.[120] Les concepteurs de solutions logicielles d'authentification mettent en place des « *anti-débugueurs* » capables de vérifier l'intégrité de l'exécution d'un programme. Face aux outils de **décompilation**, il n'existe pas de solution autre que de concevoir un système très complexe, dont le pirate mettra beaucoup de temps à comprendre le fonctionnement.[121] De manière générale, lorsqu'une mesure technique est purement logicielle, l'utilisateur qui a le contrôle de son matériel et de son environnement, se voit ouvrir un large champ d'attaques possibles. La question pertinente porte alors sur le caractère dissuasif du temps nécessaire à la mise en cause de la robustesse de la mesure technique.

En revanche, un système d'authentification matériel est beaucoup plus robuste aux tentatives de rétro-conception. **Pénétrer à l'intérieur d'une carte à puce ou d'un circuit intégré est une opération extrêmement complexe en raison de la miniaturisation de ces matériels. Cette opération ne peut en aucun cas être réalisée de manière artisanale** par un pirate, et il n'existe pas d'outil bon marché permettant de la faciliter. Il existe des techniques de retro-conception des systèmes matériels, reposant par exemple sur des procédés de radiographie, mais elles nécessitent des moyens financiers très élevés. De plus, il est beaucoup plus difficile de réaliser une attaque sans laisser de traces lorsque la mesure technique est de nature matérielle, par conséquent la menace de poursuites judiciaires a un plus grand pouvoir de dissuasion.

3.2.3.2. Le chiffrement de la procuration des droits.

Après que la requête authentifiée a été envoyée au serveur de droits, celui-ci consulte la base de données des droits ou la base de données commerciale, puis retourne une représentation de ces droits à l'utilisateur. Ces droits autorisent cet utilisateur à exploiter certains des droits de l'œuvre.

Fig. 3.20. – La fonction de chiffrement de la procuration des droits.



[120] *Directive 91-250 et du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur* (art. 6) ; article L. 122-6-1 du CPI. (cf. 2e partie de l'étude : 2.2.1.)

[121] Ce point n'est pas neutre juridiquement : la protection juridique des mesures techniques d'accès aux œuvres assurée par la Directive 2001/29 y compris quant au processus d'identification qui revêt un caractère central dans un *DRMS*, s'établit sans préjudice du droit à décompilation.

Il s'agit en général d'une clef synthétique qui dépend des droits, de l'œuvre, de l'utilisateur, afin de garantir que la clef ne pourra pas être utilisée pour d'autres droits, d'autres œuvres ou d'autres utilisateurs. Il est indispensable que la transmission de cette clef soit chiffrée afin que ces trois paramètres ne puissent pas être modifiés, y compris par l'utilisateur destinataire de cette clef. Même si le serveur de droits est parfaitement sécurisé, le chiffrement de cette transmission suppose qu'il existe : un secret détenu par l'utilisateur mais auquel il n'a pas accès en lecture : une interface sécurisée entre ce secret, le serveur de droits, l'utilisateur, et l'œuvre.

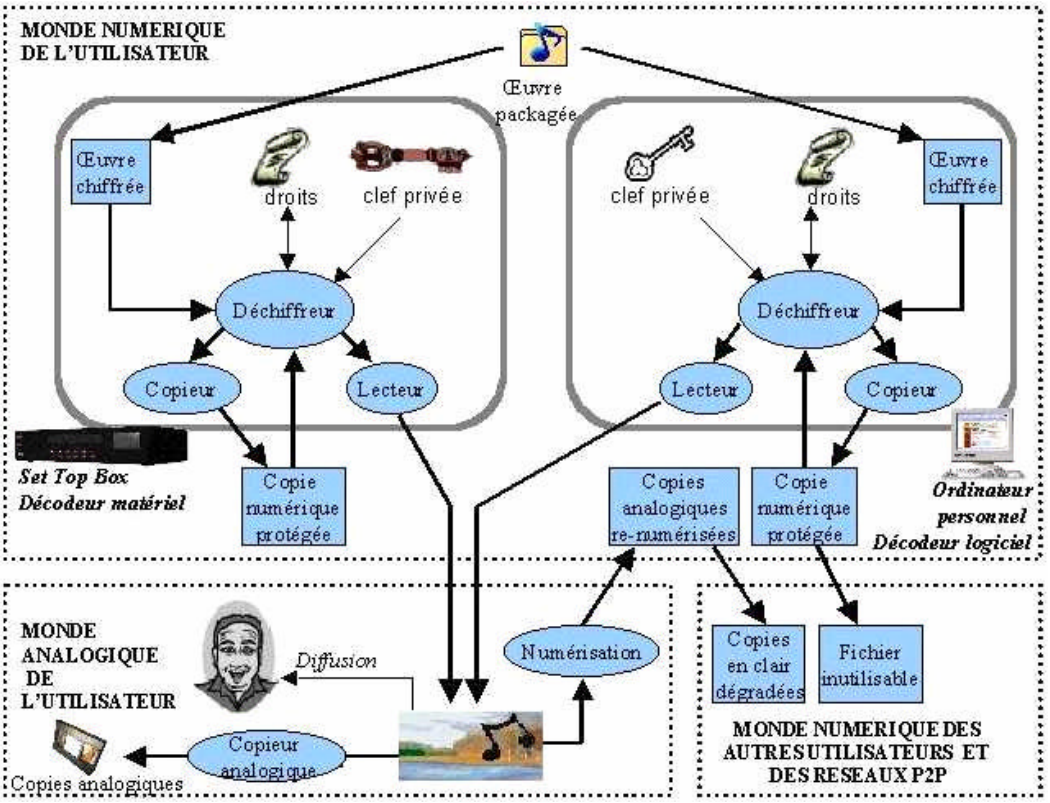
La problématique est donc exactement la même que dans le cas de l'authentification. L'implémentation du secret et de l'interface peut être soit matérielle, soit logicielle, avec les mêmes caractéristiques que l'authentification en termes de robustesse. Il se peut tout à fait que le secret utilisé pour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

* * *

3.3. L'EXPLOITATION DES DROITS

Le contrôle de l'exploitation des droits se subdivise en deux grandes catégories qui répondent à des problématiques différentes et donnent lieu à des solutions complémentaires de protection technique : le contrôle de l'accès aux œuvres, le contrôle de la copie des œuvres.

Fig. 3.21. –Les mondes de l'utilisateur.



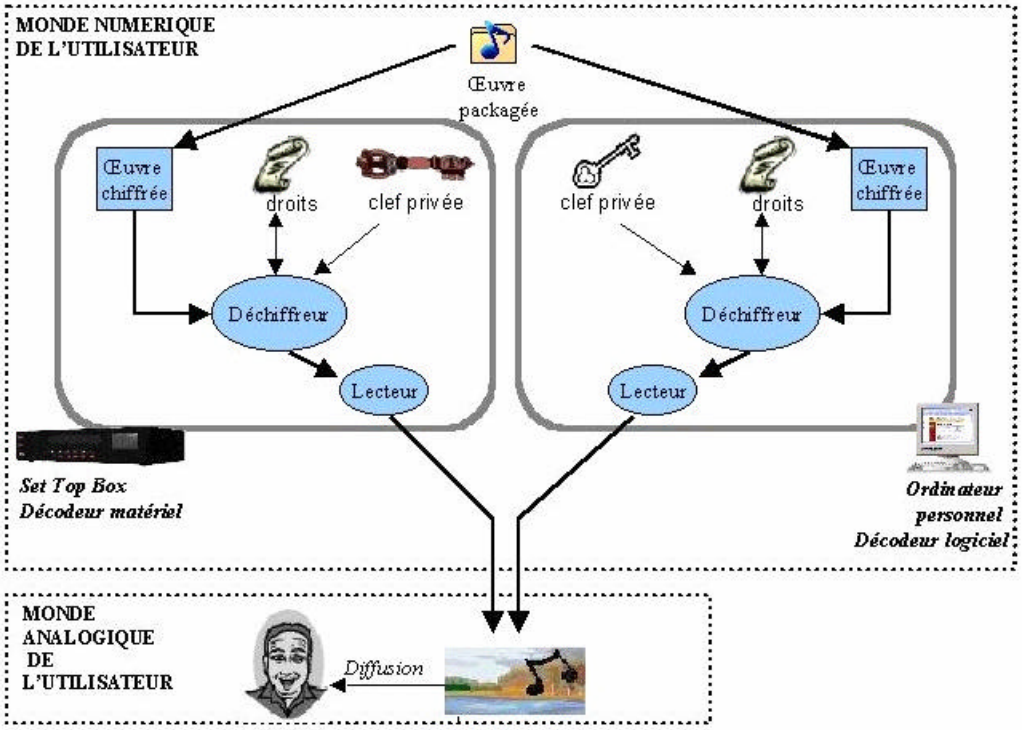
3.3.1. LE CONTROLE DE L'ACCES A L'ŒUVRE.

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

3.3.1.1. L'opération de déchiffrement.

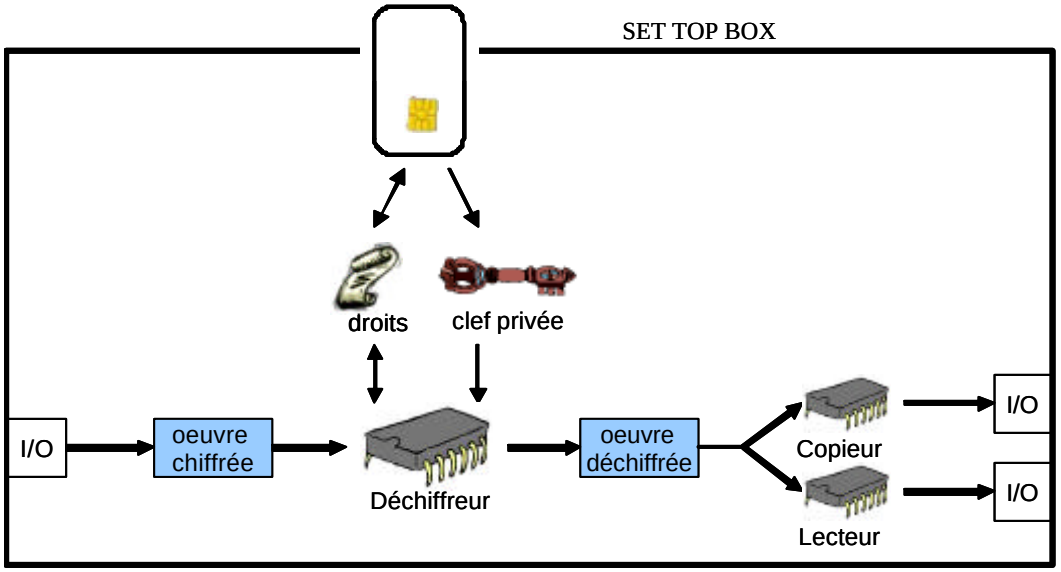
Un décodeur, ou une interface d'exploitation des droits, placé chez l'utilisateur, confronte une œuvre chiffrée, la représentation des droits de l'utilisateur, et l'authentification de l'utilisateur. Si l'utilisateur possède les droits adéquats, le module de déchiffrement du décodeur procède au décryptage de l'œuvre, la rendant ainsi compréhensible par le lecteur proprement dit, c'est-à-dire le module du décodeur chargé de mettre l'œuvre sous une forme analogique intelligible à l'utilisateur.

Fig. 3.22. – Le déchiffrement dans le monde de l'utilisateur.



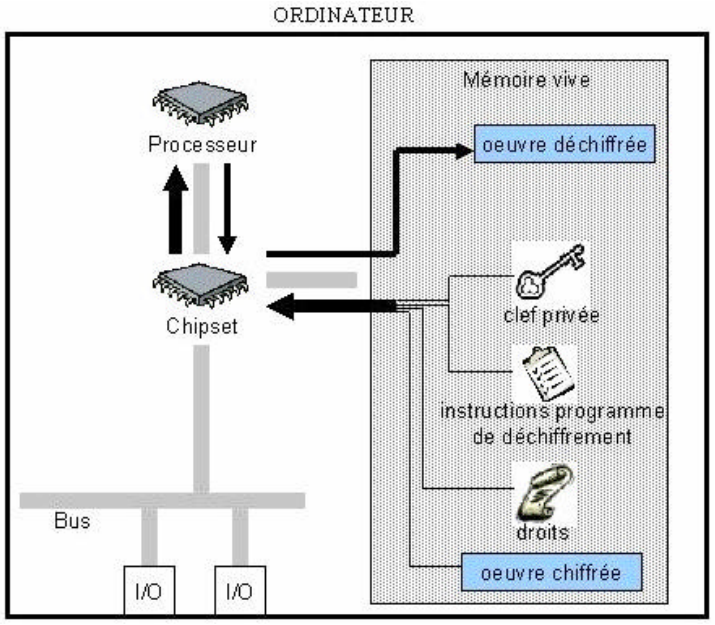
– **Dans le cas où le déchiffreur est matériel, il s'agit simplement d'un circuit intégré**. Celui-ci reçoit, en entrée, les signaux numériques représentant l'œuvre sous forme chiffrée, la représentation des droits de l'utilisateur sur cette œuvre et la clef privée du décodeur. En sortie, il génère les signaux numériques représentant l'œuvre sous forme non chiffrée. La représentation des droits et la clef privée peuvent être stockées sur une carte à puce insérée dans un lecteur de carte à puce intégré au décodeur. Il se peut également que la représentation des droits et la clef privée soient stockées eux aussi dans un circuit intégré, éventuellement le même que celui qui contient la fonction de déchiffrement.

Fig. 3.23. – La solution matérielle de déchiffrement.



– **Dans le cas où le déchiffreur est logiciel**, on retrouve les mêmes modules, mais implémentés de façon logicielle. Le déchiffreur est représenté par une suite d'instruction stockée dans la mémoire de l'ordinateur, et qui seront exécutées par le processeur. La représentation des droits et la clef privée sont stockées dans la mémoire de l'ordinateur.

Fig. 3.24. – La solution logicielle de déchiffrement.



Les considérations sur la robustesse des solutions d'authentification restent ici valables.[122] La clef privée joue en effet un rôle similaire dans les fonctions d'authentification et de déchiffrement. Les contraintes de sécurité pour la représentation des droits sont similaires : celle-ci est plus en sécurité dans une carte à puce ou dans un circuit intégré que dans la mémoire vive d'un ordinateur, à condition naturellement que ni la clef, ni la représentation des droits, ne circulent sans protection sur un bus de données.

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

3.3.1.2. Types de décodeurs et exemples.

Le mode d'implémentation, matériel ou logiciel, du cœur des fonctions de sécurité est un paramètre essentiel d'un décodeur. Indépendamment de cette caractéristique, un autre paramètre est l'ensemble des supports de distribution avec lesquels ce décodeur est compatible. Quelques exemples sont donnés dans le tableau ci-dessous.

[122] cf. 2.2.3.1.

Tableau 3.2. – Exemples d'implémentation de systèmes de sécurité.

	Distribution sur supports optiques	**Distribution sur des réseaux fermés de télécommunications**	**Distribution sur internet**
Implémentation matérielle du cœur de sécurité	– Lecteur DVD de salon – Lecteur SACD ou DVD-A de salon	– décodeur de télévision par câble ou par satellite muni d'une carte à puce	- lecteur installé sur un PC équipé de TCPA et Palladium[123]
Implémentation logicielle du cœur de sécurité	– Lecteur DVD installé sur un PC	– certains téléphones portables multimédias	- lecteur installé sur un PC, cas général

En matière de contrôle d'accès, une autre caractéristique importante d'un décodeur est son degré d'interopérabilité avec les serveurs de droits. Celle-ci dépend du langage de description des droits utilisé par le décodeur, et de la capacité des serveurs de droits à utiliser ce langage.

3.3.2. LE CONTROLE DE LA COPIE NUMERIQUE DE L'ŒUVRE.

On peut distinguer différents types de copie numériques :

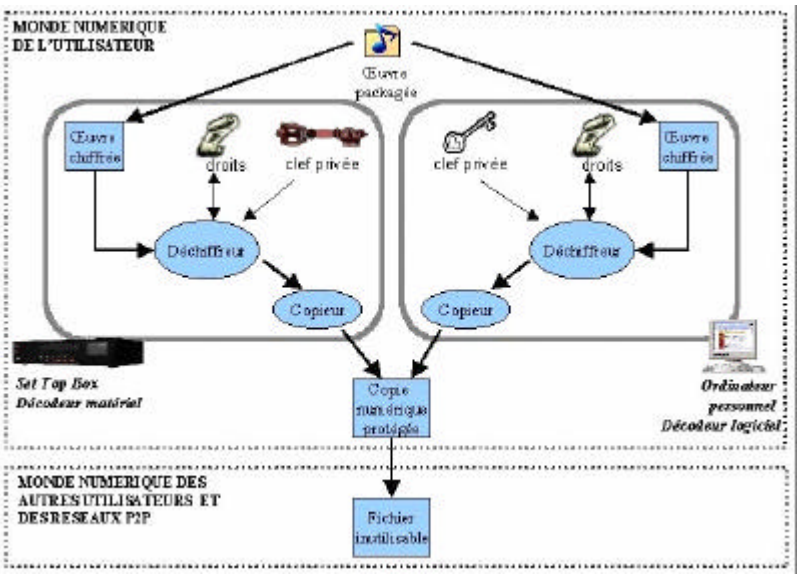
– la copie de l'œuvre sous sa forme protégée, lors de la distribution ;

– la réalisation de copies par le décodeur, situé chez l'utilisateur et fourni par le distributeur ;

– la réalisation de copies par les équipements numériques du réseau privé de l'utilisateur ;

– la réalisation de copies analogiques lors de la lecture de l'œuvre.

Fig. 3.25. – Le périmètre de la copie numérique contrôlée.



(123) Dans le cas où ces projets seraient commercialisés et tels qu'ils sont présentés aujourd'hui.

3.3.2.1. Contrôle de copie numérique de l'œuvre protégée.

Par définition, le contenu numérique protégé n'est exploitable qu'en fonction des droits associés. Les titulaires de droits peuvent donc bénéficier d'une garantie technique de l'expression du droit exclusif d'autoriser ou d'interdire la copie privée numérique, soit en l'autorisant (de 1 à ?), soit en l'interdisant.[124] Les titulaires de droits peuvent également fixer le nombre exact de copies numériques autorisées, sauf dans le cas où la représentation des droits de l'œuvre est sur le même support que l'œuvre (certains supports optiques, mais ils peuvent alors décider d'autoriser ou d'interdire les copies subséquentes).

Dans la pratique, la copie numérique de contenus numériques sous leur forme protégée n'est pas contrôlée, sauf dans le cas des supports optiques où la représentation des droits est gravée sur le même support que l'œuvre protégée. Les œuvres protégées circulent donc librement sur les réseaux de télécommunications électroniques, qu'ils fonctionnent en diffusion continue, à la demande, ou par échange entre utilisateurs. Une libre circulation des œuvres protégées peut répondre de surcroît à l'intérêt des titulaires de droits lorsque l'œuvre protégée est conçue comme un objet commercial, par exemple à des fins de publicité, permettant de faire bénéficier d'une version bridée de l'œuvre dans des conditions préétablies (nombre de lectures, durée d'accès à la lecture, etc.).

i. le contrôle de la copie numérique par le décodeur.

Le décodeur (logiciel ou matériel) étant une partie intégrante du système de gestion numérique des droits, il est possible de contrôler la copie à ce niveau grâce à un paramétrage du décodeur. En théorie, un décodeur non compatible avec le système de gestion numérique des droits ne permet pas de déchiffrer l'œuvre. Le paramétrage de décodeur peut être mis à jour, ou évoluer en fonction des paiements de l'utilisateur, si le décodeur est relié à un serveur de droits.

Lorsque l'utilisateur désire copier une œuvre, le décodeur vérifie dans sa mémoire interne si l'utilisateur possède les droits de copie sur cette œuvre. S'il les a, alors l'utilisateur peut réaliser une copie, et en cas de limitation, le nombre de copies restantes autorisées est décrémenté. Si l'utilisateur ne possède pas les droits, l'issue dépend de la possibilité qu'a l'utilisateur de connecter son décodeur à un serveur de droits :

– si le décodeur peut être connecté à un serveur de droits (par exemple un décodeur logiciel installé sur un ordinateur relié à Internet, ou bien un décodeur de télévision par satellite relié à une prise de téléphone), alors l'utilisateur peut demander à acheter ces droits. Selon le régime des droits propres à l'œuvre, la livraison des droits sur le décodeur permet ou non à l'utilisateur de réaliser le nombre de copies autorisées.

– si le décodeur ne peut pas être connecté à un serveur de droits (par exemple un lecteur DVD de salon), alors l'utilisateur n'a aucun moyen de réaliser une copie.

---

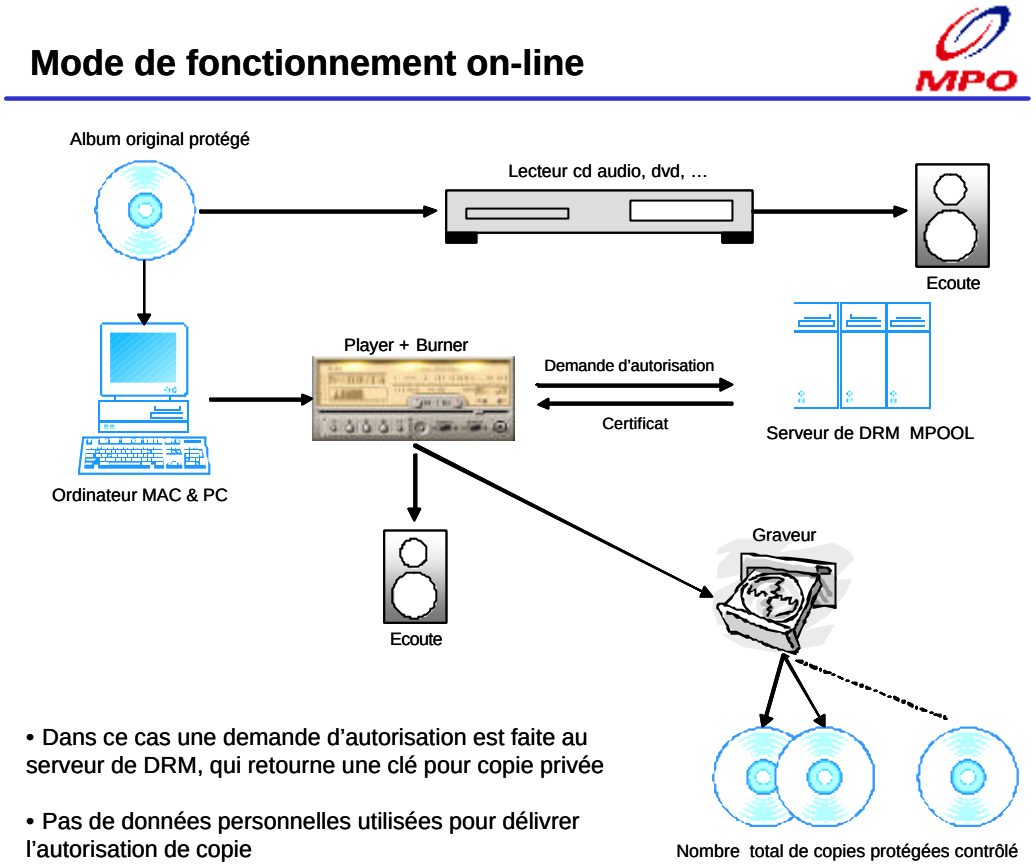
[124] Cette faculté technique de garantie des droits exclusifs a pour champ d'application principal l'article 6.4 §4 de la directive 2001/29 relatif aux « *œuvres ou autres objets protégés qui sont mis à la disposition du public à la demande* ». cf. 2e partie de l'étude : 2.1.1 et 3.1.2.

Ce système très efficace repose entièrement sur l'idée que le parc de décodeurs respecte les règles de la gestion numérique. Les moyens les plus efficaces de contourner le contrôle de la copie numérique d'une œuvre par le décodeur sont donc :

– découvrir ou concevoir un décodeur capable de lire l'œuvre, mais ne respectant pas les règles de la gestion numérique des droits ;

– modifier sans altérer l'œuvre de manière à pouvoir la lire sur un décodeur ne respectant pas les règles de la gestion numérique des droits.

Fig. 3.26. La copie privée sur support optique par décodeur logiciel : exemple de MPO



L'existence d'un secret à l'intérieur du décodeur, généralement sous forme de clef privée, empêche les utilisateurs de mettre en œuvre ce genre de techniques. Ce secret établit un lien de confiance entre le distributeur et le parc de décodeurs existants, en lui donnant un minimum de garanties sur les opérations qu'un décodeur n'a pas le doit de faire.

Le principe de la protection contre la copie est de ne diffuser des œuvres qui ne sont compatibles qu'avec des décodeurs qui interdisent la copie, ou bien ne l'autorisent que sous certaines conditions.

Encadré 3.13. *Sealed Media* & *Réunion des Musées Nationaux* : l'image en ligne.

La Réunion des Musées Nationaux (RMN) a mis en place un site Internet dédié à Matisse et Picasso. Ce site Internet permet de consulter une reproduction numérique en haute définition d'œuvres de ces artistes. [125] Afin d'assurer un respect des droits d'auteur sur ces œuvres, une mesure de protection technique a été mise en place. Celle-ci vise à empêcher les utilisateurs d'imprimer ou copier les images qui s'affichent sur leur écran lors de la consultation du site web.

La mesure technique de protection est fondée sur un produit de *Sealed Media*.[126] Ce produit offre ne nombreuses fonctionnalités, et permet en particulier une gestion de la chaîne complète des droits. Dans ce cadre, il n'est toutefois utilisé qu'en tant que système de protection anti-copie. Lorsqu'un utilisateur consulte le site Internet, il doit télécharger un *viewer*, petit logiciel spécifique permettant d'afficher les images. Les images sont transmises sous forme chiffrée, et le rôle de ce *viewer* est d'assurer le déchiffrement dans des conditions sécurisées.

Pendant que le *viewer* réalise l'opération de déchiffrement en vue d'un affichage à l'écran, la stabilité du système et en particulier de la mémoire est vérifiée. Ainsi le *viewer* s'assure qu'aucun autre logiciel lancé en même temps ne viendra intercepter l'image sous sa forme déchiffrée. En particulier, la touche « imprime écran » est désactivée. La licence étant sauvegardée en local chez les utilisateurs, ceux-ci peuvent continuer à consulter les images même lorsqu'ils ne sont plus en ligne. Ce système de protection n'apparaît pas, en tant que *DRM*, particulièrement robuste : puisque l'utilisateur contrôle l'environnement et en particulier le système d'exploitation, il doit exister un moyen de contourner la protection technique, ne serait-ce qu'en essayant de contrer les fonctions « anti-debuger » du *viewer*. Toutefois, cette mesure de protection répond à son objectif de sécurité, elle est suffisamment robuste pour que la quasi-totalité des utilisateurs n'ait pas les moyens de copier les images.

3.3.2.2. Contrôle de copie numérique dans le « réseau privé personnel».

Chaque utilisateur peut posséder au sein de son foyer ou dans ses poches, un ensemble d'équipements d'électronique grand public intervenant dans la lecture ou la copie de musique et de films. La plupart de ces équipements sont désormais numériques, par exemple : un décodeur de réception par câble, satellite ou DSL, un lecteur de CD Audio, de DVD ou de SACD, un graveur de CD Audio ou de DVD, un téléviseur numérique, par exemple à écran plasma, un baladeur MP3, un téléphone cellulaire, un caméscope numérique, une console de jeux, un ordinateur personnel.

Aujourd'hui, ces éléments ne sont en général pas raccordables, ce qui limite le champ de la copie. Or les utilisateurs ayant acheté une œuvre souhaitent, en général, pouvoir procéder à sa lecture, voire sa reproduction, sur l'ensemble des équipements. **La tendance actuelle est donc un accroissement de la connectabilité et de l'interopérabilité des équipements électroniques grand public**. À terme, cela peut conduire à la constitution, pour chaque utilisateur, d'un « **réseau numérique privé personnel** » ou « **réseau privé domestique** » reliant l'ensemble des équipements.

Dans ce contexte, **le risque tient à ce que la multiplication des passerelles entre les équipements puisse conduire à l'apparition de nouveaux réseaux d'échanges**, comme le *peer to peer* sur Internet. Face à ce risque il existe une solution : rendre non interopérables des réseaux numériques qui n'appartiennent pas à un même utilisateur, ou foyer, lequel peut cependant être en des lieux physiques différents (habitation principale, secondaire). Un tel système de contrôle de la copie sur un réseau numérique privé personnel doit donc présenter les caractéristiques suivantes :

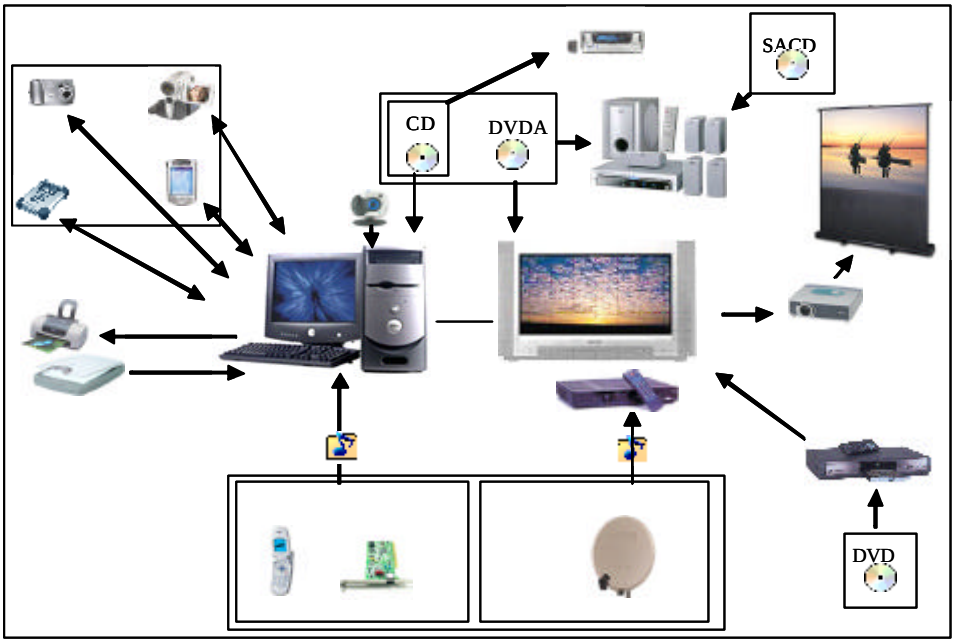
[125] cf. [http://www.matissepicasso.org]
[126] *Sealed Media* [http://www.sealedmedia.com/]

– permettre le transfert de données entre équipements d'un même utilisateur ;

– interdire le transfert de données entre équipements d'utilisateurs distincts.

Cela suppose que les équipements appartenant à un même utilisateur sachent se reconnaître, c'est-à-dire partagent un secret.

Fig. 3.27. – Le réseau privé personnel étendu.



i. La sécurité des connexions : cœur de la protection du réseau privé personnel.

Si l'on suppose qu'un lecteur dont l'architecture interne est parfaitement sécurisée ne permette pas la copie, le système de sécurité ne sert à rien s'il est possible de brancher sur ce lecteur un copieur non-protégé compatible. Par exemple, certaines des platines CD Audio de salon possèdent une sortie numérique, coaxiale ou optique, sur laquelle il est possible de brancher un graveur de CD Audio. Il existe même des lecteurs SACD possédant une sortie numérique, ne permettant certes pas de bénéficier du son multicanal, mais à partir de laquelle il est possible de graver un CD Audio.

De même, dans le domaine de la vidéo, **les connecteurs IEEE 1394**, appelés aussi *FireWire*® par Apple et *i.LINK*® par Sony, permettent de relier toutes sortes d'équipements capables de lire ou d'enregistrer des œuvres audiovisuelles. **Si un décodeur sécurisé, au sens où il respecte un schéma de gestion numérique des droits, possède une sortie 1394 sur laquelle il est possible de brancher un graveur de DVD, alors la protection contre la copie ne sert plus à rien.** Il est indispensable que ces connecteurs soit eux aussi sécurisés, c'est-à-dire ne diffusent pas les œuvres sans chiffrement. L'interopérabilité entre différents équipements d'électronique grand public sécurisés n'est pas en soi une source de vulnérabilité, à condition que la liaison soit elle-même protégée. Cette protection portant sur le protocole et non sur les caractéristiques physiques de la liaison, filaire ou aérienne, elle peut être adaptée à tous types de liaisons. De manière technique, la protection porte sur le protocole de transmission entre deux appareils, qui doit à la fois :

– être compréhensible par les deux appareils, ce qui suppose qu'il existe une norme ou au moins des accords de compatibilité entre les industriels ;

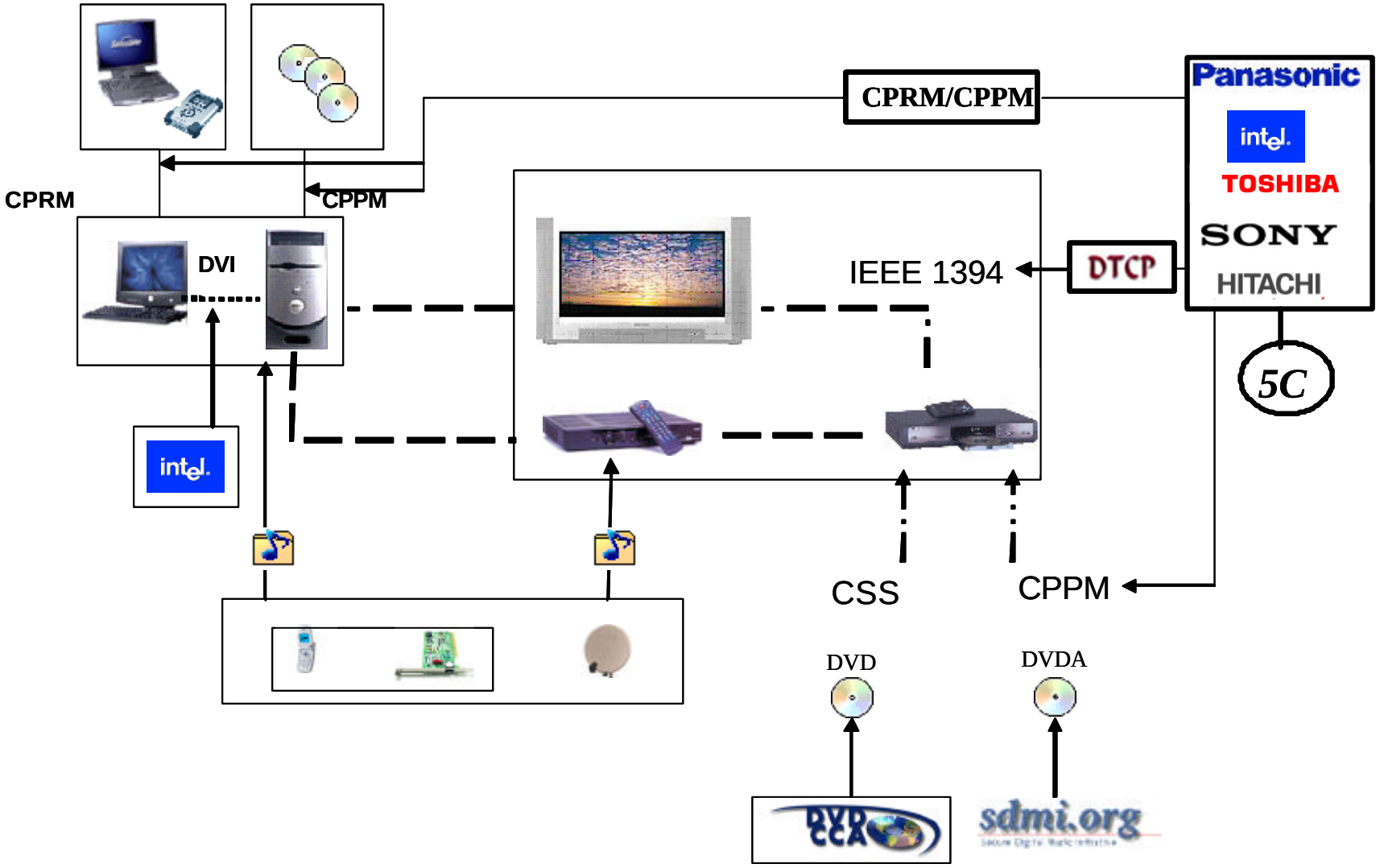
– être indéchiffrable par un utilisateur n'ayant pas acquis les droits correspondants.

Encadré 3.14. — L'IEEE 1394

« IEEE 1394 » est le nom donné par l'IEEE (*Institute of Electrical and Elecronic Engineers*) au connecteur universel à haute vitesse (jusqu'à 300 Mbytes/sec), pour les appareils de l'électronique grand public comme pour les ordinateurs personnels avec une compatibilité pour le *P2P*, adaptables avec 63 catégories d'appareils (caméra numérique, son *surround*, scanners, imprimantes, disques durs, enregistreurs de musiques, imprimantes, etc.) et plus particulièrement tous les appareils du réseau domestique privé (TV, Hifi, etc.). Il joue un rôle stratégique dans la protection des contenus numériques parce qu'il constitue la passerelle entre les univers industriels de l'électronique grand public et celui de l'informatique. Il est promu par la *1394 Trade Association* qui regroupe plus de 170 entreprises.[(127)]

(127) *1394 Trade Association* [http://www.1394ta.org/]

Fig. 3.28. – Les enjeux industriels de la connectique.



Enfin, dans le cas où deux appareils sécurisés communiquent via une liaison sécurisée, il suffit qu'il existe une faille de sécurité sur l'un des deux appareils pour qu'un usage frauduleux de l'ensemble soit possible. Par conséquent, il est dans l'intérêt d'un producteur d'un produit très sécurisé de refuser l'interopérabilité de ce dernier avec des produits moins sécurisés. En particulier, **l'ouverture de l'interopérabilité d'un équipement électronique grand public sécurisé avec les ordinateurs personnels est très risquée**. Ainsi, par exemple, les attaques réussies sur le système de protection des DVD se sont fondées sur l'existence de lecteurs de DVD compatibles avec les micro-ordinateurs.

ii. La protection au sein du réseau privé domestique.

Un système de contrôle de la copie sur un réseau numérique privé personnel est complémentaire d'un système de contrôle d'accès, c'est-à-dire d'un système de gestion numérique du droit d'accès à l'œuvre. Le fonctionnement d'un système local de contrôle de la copie repose sur le partage d'un secret entre les différents équipements appartenant à un utilisateur, ce secret permettant de chiffrer la transmission des œuvres d'un équipement à l'autre.

– **Exemple de norme pour un système de protection globale : *Smartright*.**[(128)] Dans ce cas, le secret partagé entre les équipements appartenant à un même utilisateur est protégé au sein d'une carte à puce située sur chacun des équipements.

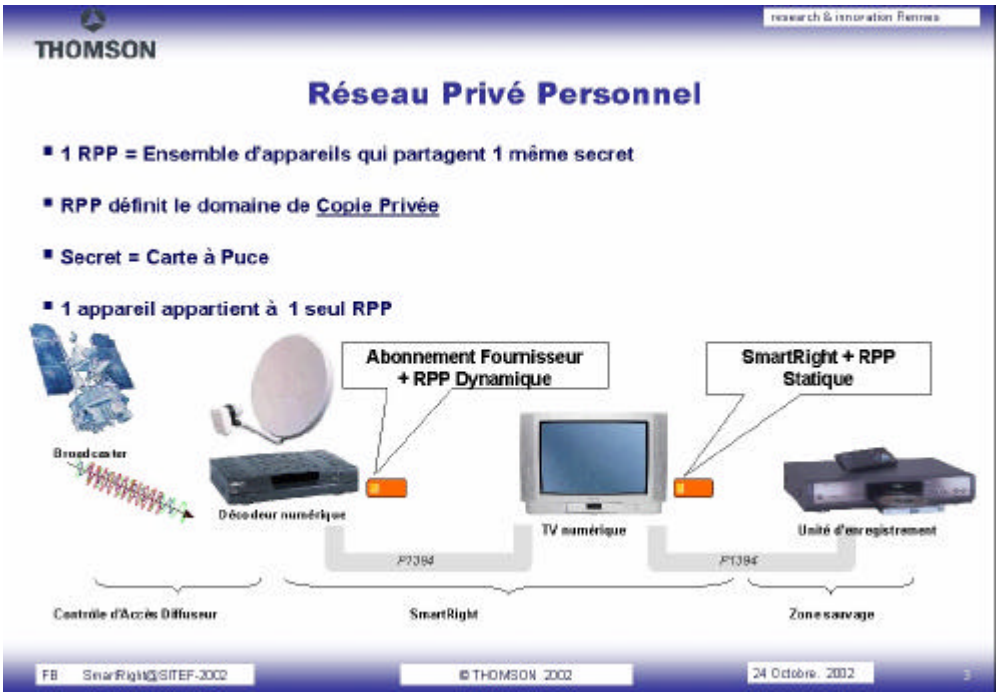
Fig. 3.29. – L'architecture de *Smartright*.

Le décodeur réalisant le contrôle d'accès se trouve à l'interface entre le monde extérieur et le réseau privé personnel. Dans le monde extérieur, ce sont les systèmes de protection mis en place par le distributeur qui protègent des œuvres. *Smartright* est un système complémentaire, il protège les œuvres au sein du réseau privé personnel.

(128) *Smartright* [http://www.smartright.org/SMR_Homepage/0,7380,LNFR,00.html]

L'équipement principal, celui qui porte l'identité d'un utilisateur, est le téléviseur. Si un deuxième téléviseur est présent dans le réseau privé personnel, il détecte le premier et coordonne son comportement. Tous les autres équipements utilisent la clef privée diffusée par le téléviseur pour chiffrer les œuvres, ou plus exactement le mot de contrôle (ou clef symétrique) qui sert à chiffrer les œuvres proprement dites. Ainsi, aucune œuvre ne circule sans protection sur le réseau privé personnel.

Fig. 3.30. – La copie privée dans le réseau privé par *Smarthright*.



Le système *Smartright* autorise les titulaires de droits à décider si la copie privée est autorisée ou interdite. Dans le cas où elle est autorisée, elle est illimitée, au sens où le nombre de copie n'est pas contraint, mais elle est sécurisée. Si par exemple un utilisateur possède un graveur de DVD au sein de son réseau privé personnel, et qu'il grave des DVD à partir des programmes diffusés sur le satellite, le chiffrement sera réalisé en fonction de la clef privée du téléviseur de cet utilisateur. Par conséquent, il pourra visionner les DVD obtenus sur un lecteur de DVD faisant partie du même réseau privé personnel, mais pas sur un lecteur appartenant à une autre personne, à moins de prêter sa carte à puce à cette autre personne.

Dans le cas où la copie privée est interdite, l'enregistrement est toujours physiquement possible, mais les copies obtenues seront indéchiffrables, même au sein d'un même réseau privé personnel. Cette fonctionnalité est gérée au niveau du décodeur.

D'autres normes sont en développement pour la protection des œuvres sur les réseaux domestiques. C'est le cas par exemple de la norme DTCP proposée par le consortium *5C entity*. Le cas des liaisons domestiques sans fil pourrait bénéficier de solutions spécifiques en raison des contraintes techniques qu'impose ce moyen de transmission. Philips semble particulièrement actif sur ce sujet.

– **Des protections spécifiques : exemple de la liaison avec les baladeurs MP3. Un utilisateur crée un réseau privé personnel en reliant** son ordinateur avec un

baladeur MP3. Après avoir acheté de la musique sous forme de compact disque, un utilisateur peut la transférer sur son ordinateur sous forme de fichiers MP3. Ces fichiers peuvent ensuite être transférés sur un baladeur MP3. Un phénomène de contrefaçon peut apparaître si un utilisateur connecte le baladeur MP3 sur de nombreux ordinateurs appartenant à d'autres utilisateurs. La solution consiste à faire en sorte que les fichiers transférés d'un ordinateur vers un baladeur MP3 ne puissent pas être lus par d'autres ordinateurs. Cette solution a été techniquement mise en œuvre pour plusieurs modèles de baladeurs MP3. Par exemple, le terminal « *iPod* » d'*Apple* comporte un tel système de protection contre la copie. C'est également de cas de certains appareils construits par *Sony*.

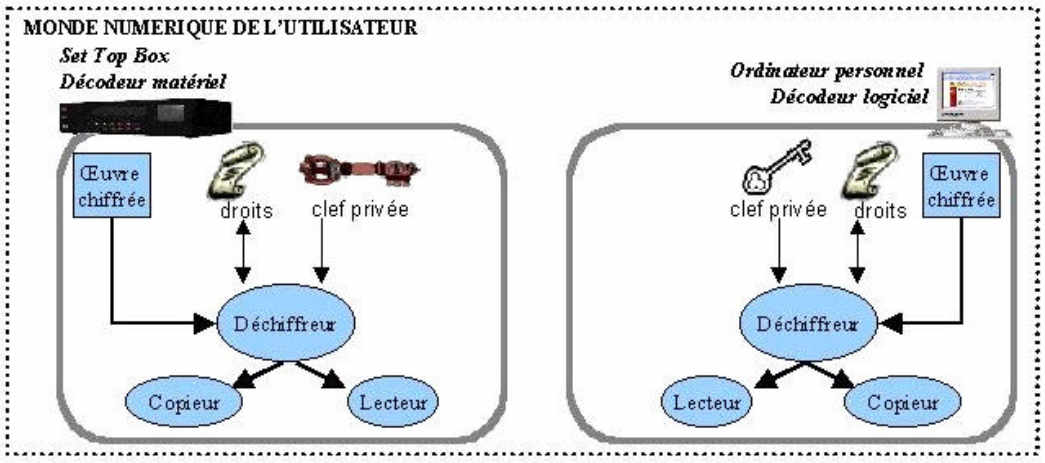
3.3.3. LE CONTROLE DE L'UTILISATION DES COPIES NUMERIQUES.

À l'issue de la chaîne de distribution, la question de l'existence possible ou non, et la question de l'utilisation des copies numériques sont les plus essentielles aujourd'hui, notamment pour les utilisateurs et le bénéfice de la copie privée numérique.

3.3.3.1. Le stockage et la mise à jour des droits par le lecteur

Le décodeur reçoit, en général depuis un serveur de droits, une représentation des droits qu'il transmet au module de déchiffrement pour réaliser les fonctions de lecture et de copie. Afin de continuer à exploiter les droits même après la fin de la connexion entre le décodeur et le serveur de droits, certains décodeurs sont conçus pour stocker les droits qu'ils ont obtenus, suivant des conditions fixées à l'avance ou par le serveur de droits.

Fig. 3.31. – Les modes de stockage des clefs.



Lorsqu'une carte à puce est présente sur le décodeur pour stocker la clef privée, elle peut être mise à profit pour stocker également la représentation des droits. C'est notamment le cas des décodeurs de télévision à péage, et du « G2 » en cours de *Canal+ Technologies*. Lorsque le décodeur est logiciel, la représentation des droits est stockée de la même manière que la clef privée, c'est-à-dire dans une mémoire, avec des techniques de dissimulation.

3.3.3.2. La traçabilité de la copie numérique.

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

i. Le contrôle des copies subséquentes.

Le contrôle des copies subséquentes repose sur les mêmes principes que le contrôle des copies numériques produites à partir de l'original, puisque les copies numériques sont protégées de la même manière que les œuvres originales.

ii. Principe et applications de la traçabilité des copies numériques et analogiques.

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

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

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

– ***Le contrôle de diffusion cinématographique***. Dans le cas du cinéma, il est de même possible de tatouer sur le film un identifiant de la salle de cinéma, voire même la date et l'heure de projection. Si un exploitant de salle de cinéma laisse un spectateur filmer l'œuvre avec un caméscope, et que ce spectateur diffuse l'œuvre sur un réseau d'échange, alors l'identité de l'exploitant pourra être révélée dans le cadre d'une enquête judiciaire ou simplement constatée dans le cadre des compétences des agents assermentés.[(129)]

– ***Le contrôle de diffusion audiovisuelle***. Dans le cas de la vente de programmes audiovisuels à des chaînes de télévision, il est techniquement difficile de détecter si toutes les chaînes de télévision ont réellement payé les droits pour les œuvres qu'elles diffusent. L'emploi des techniques d'identification, telles que la signature ou le tatouage, permet d'automatiser cette opération.

[(129)] cf. P. Chantepie, *La lutte contre la contrefaçon dans l'environnement numérique*, Sept.2002. MCC-IGAAC. [http://www.culture.fr/culture/cspla/rapcontrefacon.pdf]

Encadré 3.15. L'INA : un système de signatures sémantiques.

L'Institut National de l'Audiovisuel [130] a développé un système de signature sémantique pour les images et les vidéos, incluant notamment : un outil de calcul de signature, se basant sur les éléments de l'image qui sont porteurs de sens, un outil de comparaison des signatures, permettant d'identifier une œuvre à partir d'une base de données de signatures. Le traitement d'une image par un système de signature peut en théorie donner lieu à deux types d'erreurs : une fausse alerte : le système croit reconnaître une image qui n'est pas dans la base, un manquement : le système ne reconnaît pas une image qui est dans la base. Le système développé par l'INA est particulièrement performant, au sens où il génère très peu d'erreurs de ce type. Il est particulièrement robuste aux modifications des images. Ainsi, le système pourra établir une correspondance entre une image qu'on lui présente, et une image de la base, même si l'image présentée a subi des modifications telles que : un changement de contraste et de luminosité, l'ajout de cadres ou de logos, des zooms, des troncatures ou des incrustations. L'ensemble des modifications propres à la diffusion des œuvres audiovisuelles, en particulier la transmission par voie hertzienne et le passage en mode analogique, ne perturbe pas le système. De plus, une séquence animée n'a pas besoin d'être particulièrement longue pour que le système sache la reconnaître. Le système développé par l'INA pourrait être utilisé dans un contexte de surveillance de l'ensemble des œuvres diffusées, dans le but d'établir une liste des œuvres diffusées, notamment en vue de réclamer le paiement des droits sur ces œuvres. Le fait que le système puisse reconnaître des œuvres qui n'ont pas été préalablement marquées, à la différence des systèmes de tatouage, est un atout essentiel pour une institution comme l'INA.

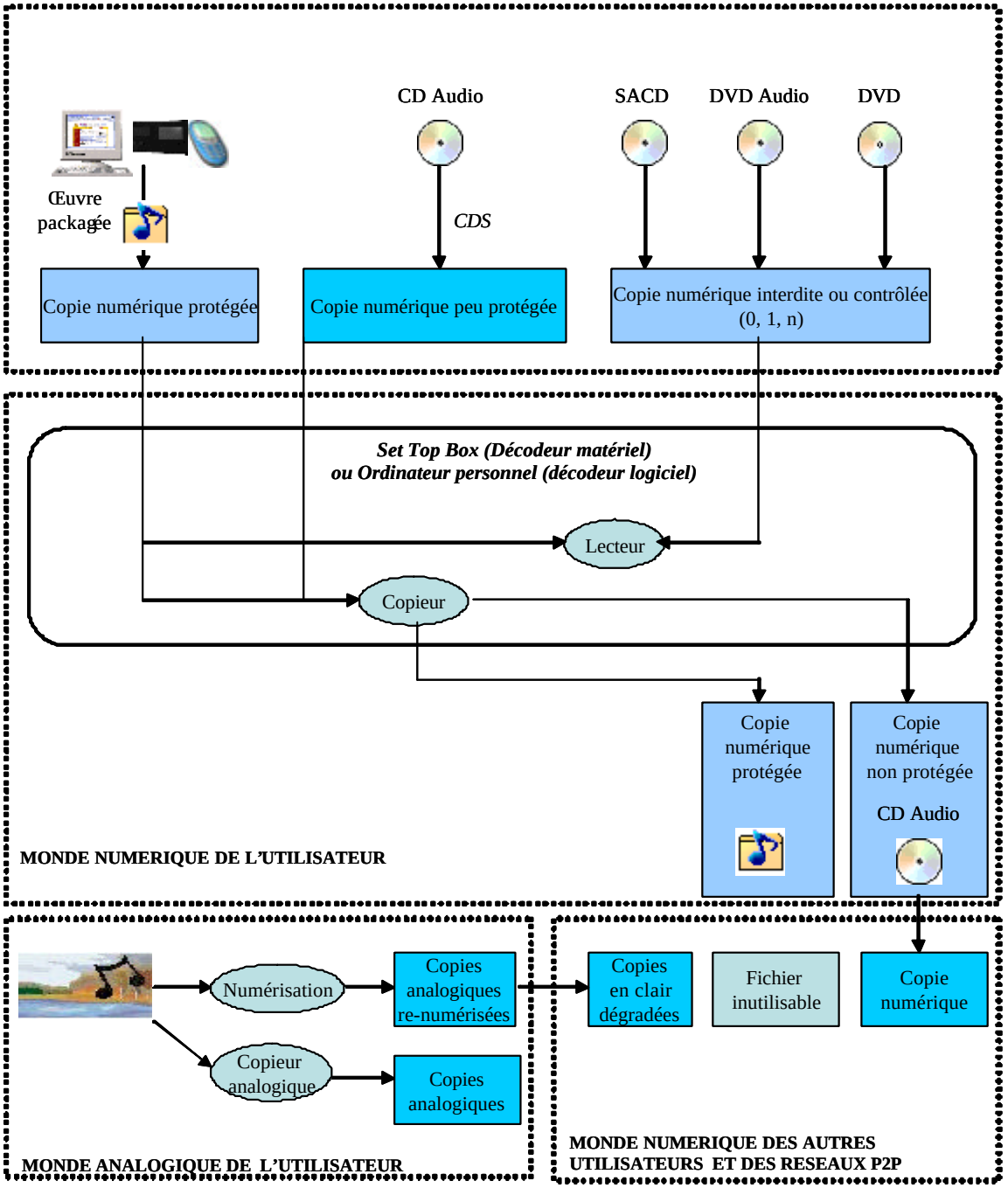
– **La mesure d'audience**. Une autre application du suivi de la copie des œuvres et la réalisation de mesures d'audience. Il peut s'agir de mesures d'audience sur des œuvres audiovisuelles, par exemple sur les chaînes de télévision et dans les salles de cinéma, ou sur des œuvres sonores, diffusées par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

Encadré 3.16. L'IRCAM et la traçabilité des œuvres sonores grâce à un système de signature.

L'outil développé par l'IRCAM (Institut de Recherche et Coordination Acoustique/Musique) [131] permet de calculer pour chaque œuvre sonore une signature. Ainsi un exploitant du système peut constituer une base de données de signatures, et utiliser cet outil comme un mécanisme d'identification des œuvres en effectuant des comparaisons de signatures. La signature d'une œuvre est calculée en fonction de données statistiques extraites du signal. Le système est particulièrement sensible, ainsi il est capable de faire la différence entre deux interprétations d'une même œuvre. Cette sensibilité peut toutefois être gênante lorsque l'outil est utilisé pour opérer une reconnaissance automatique des œuvres. Ce système d'identification peut être utilisé pour des applications de mesures d'audience. Il permet en effet d'obtenir de façon automatique des listes de diffusions correspondant à ce qui passe à la radio, à la télévision et dans les boîtes de nuit. Associé à une technologie de «web monitoring» il permet de collecter des informations sur l'offre musicale sur Internet, sur les goûts des utilisateurs et la proximité culturelle de certains morceaux. En revanche, un tel système pourrait difficilement être utilisé comme un moyen de protection contre la copie.

[130] INA [http://www.ina.fr/recherche/theme/images_sons.fr.html]
[131] IRCAM [http://www.ircam.fr/]

Fi . 3.32. – Univers technique de la copie privée numérique.



3.3.4. LES LIMITES DES PROTECTIONS DES ŒUVRES NUMERIQUES.

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

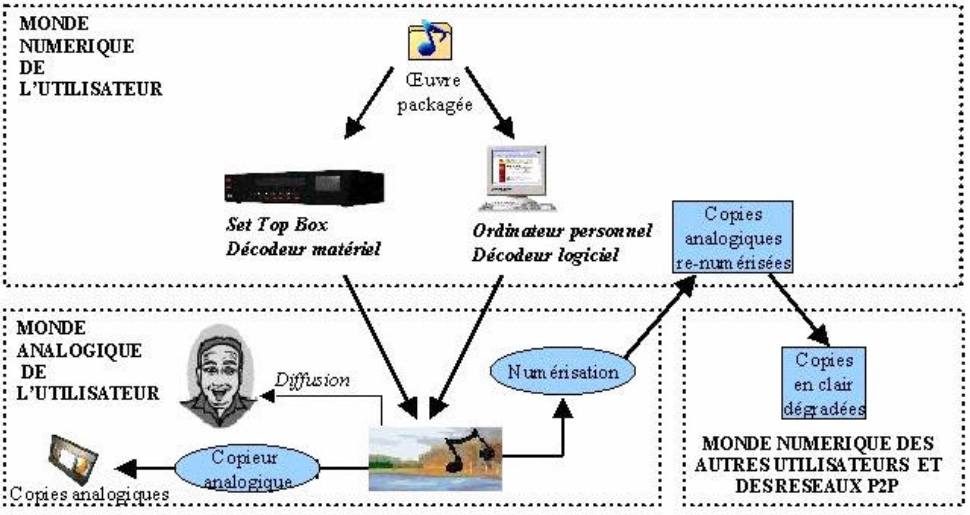
3.3.4.1. La libre copie analogique : contrainte ou choix ?

Les questions posées par le « monde analogique de l'utilisateur » sont, au regard de la nature et des objectifs d'un système de gestion numérique des droits, relativement accessoires du point de vue de la sécurité des contenus numériques. Or, dans tous les cas, **la lecture de l'œuvre suppose que l'œuvre, transmise sous forme numérique, soit convertie sous forme analogique. En effet, les sens humains sont analogiques et les systèmes de gestion numériques des droits ne peuvent s'appliquer qu'aux œuvres sous forme numérique**.

i. Le « trou analogique ».

Cela signifie, qu'entre l'extrémité de la chaîne de gestion numérique des droits, et les sens de l'utilisateur, **il existe un espace lors duquel l'œuvre circule sous forme non protégée : le « trou analogique » qui est aussi un trou de sécurité incompressible et inévitable.**

Fig. 3.33. – Le « trou analogique ».



Dans la pratique, des moyens techniques très simples permettent d'exploiter ce « trou analogique », comme enregistrer les signaux sonores avec des microphones à la sortie des haut-parleurs d'une chaîne hi-fi, enregistrer un film avec une caméra devant un écran de cinéma, saisir le contenu numérique présent sur l'écran d'un ordinateur, etc.

Des moyens un peu plus complexes existent cependant aussi. Ils consistent par exemple, lorsque c'est possible de brancher des capteurs directement à la sortie d'un décodeur, ou à l'intérieur d'un décodeur, et de traiter les signaux obtenus de manière à supprimer les parasites.

Dès lors qu'il est possible d'intercepter les signaux analogiques correspondant à une œuvre, il est possible d'enregistrer ces signaux, et de reconstituer une forme numérique de l'œuvre. **La re-numérisation d'un signal analogique réalise une reproduction numérique dégradée par rapport au contenu numérique originale**, mais indéfiniment reproductible sans dégradation supplémentaire.

ii. La désutilité de combler le « trou analogique ».

Même s'il est impossible techniquement de combler le « trou analogique » de manière parfaite, il est possible d'identifier les moyens les plus utilisés d'exploitation du trou analogique, et de modifier en conséquence les œuvres de façon à ce que ces moyens soient induits en erreur.[132] Toutefois, les mesures techniques de protection correspondantes sont peu robustes. Pour un consommateur, la valeur d'une œuvre est la valeur des signaux analogiques qu'il perçoit, en provenance du lecteur dans lequel elle est insérée. Cependant, si une capture puis une re-numérisation de ces signaux analogiques sont réalisées, la copie en résultant a une valeur commerciale inférieure, qui peut varier selon le type de contenu :

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

– ***En matière d'enregistrement musical***. Concernant les programmes musicaux diffusés à la radio, la situation est la même que pour les programmes audiovisuels. En revanche, il semblerait que les lecteurs CD Audio présents sur le marché présentent en sortie des signaux analogiques d'une excellente qualité lorsqu'il n'existe pas — tout simplement — une sortie numérique non protégée, comme c'est le cas sur de nombreuses platines de CD Audio de salon, permettant de reconstituer une copie de l'œuvre fidèle à l'original. C'est d'ailleurs l'objectif des systèmes de restitution haute fidélité (hi-fi).

Il est donc techniquement extrêmement difficile d'empêcher la copie analogique des œuvres. En revanche, des techniques existent pour savoir quel utilisateur serait impliqué dans la réalisation de cette copie (par exemple l'emploi de *watermarking* d'œuvres cinématographiques diffusés en salle). Les techniques utilisables poursuivent principalement des objectifs de dissuasion [133], ou bien, participent à la constitution de preuves dans le cadre de la lutte contre la contrefaçon.[134] Surtout, l'intérêt économique de développer des techniques de limitation du trou analogique semble assez faible. Enfin, la mise en œuvre de protection technique de la copie analogique pourrait rencontrer une hostilité des consommateurs sans rapport avec l'intérêt économique recherché, d'autant que les niveaux de dégradation de reproduction sont élevés et que la distinction entre contenu numérique et œuvre re-numérisée est assez importante et devrait s'accroître.

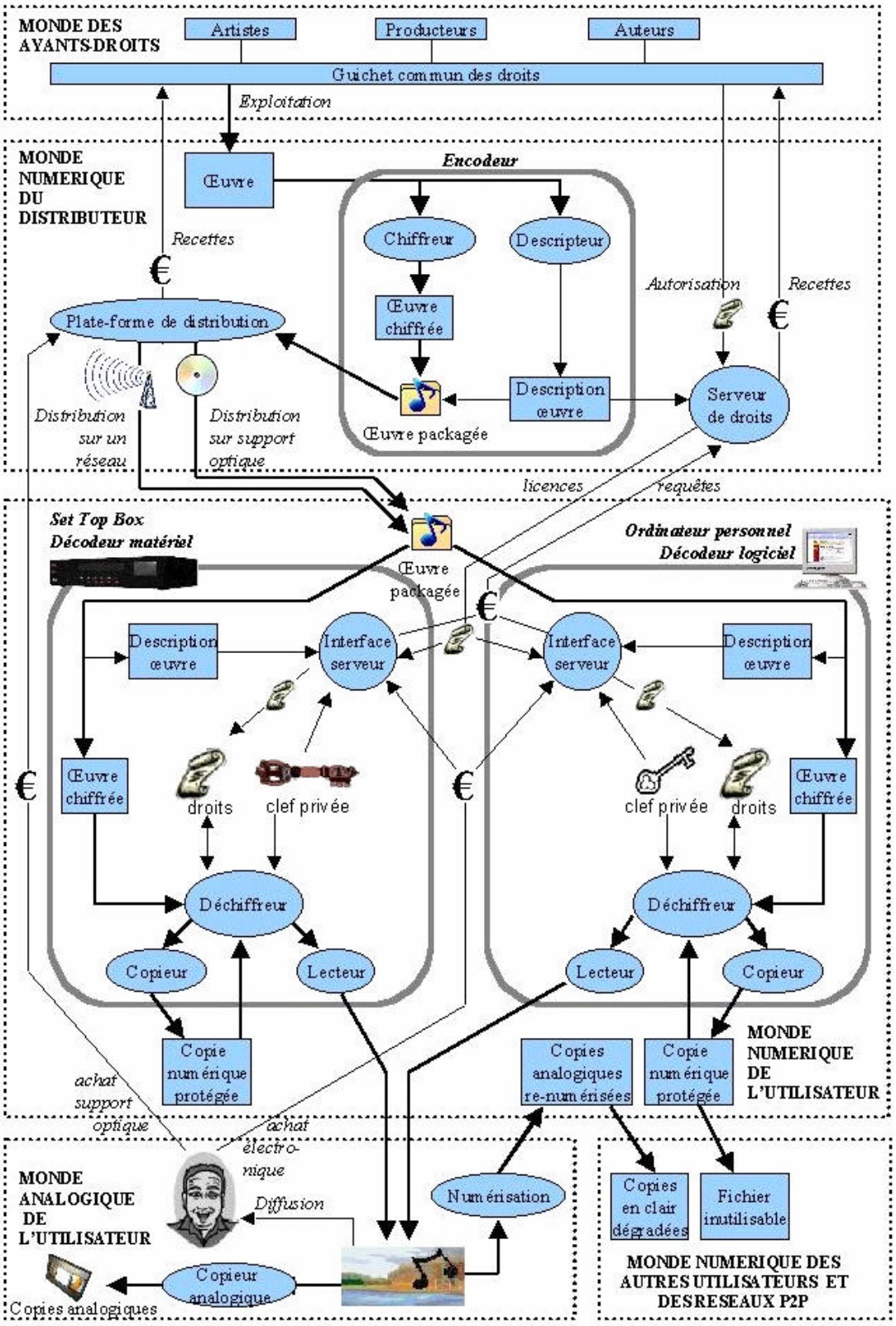
---

[132] Les mesures techniques de protection contre la copie analogique sont détaillées dans la partie I.3.1.

[133] Même si la probabilité que ce genre de technique résiste à une attaque est faible, le contrefacteur ne peut pas vérifier si son attaque a réussi et il court le risque de subir des poursuites judiciaires s'il diffuse des copies illégales.

[134] Les techniques à base de *watermarking* sont détaillées dans la partie I.2.2.

3.34. – Schéma synthétique d'un *DRMS*.



3.3.4.2. La mise à jour technique face au piratage.

Par nature et presque par définition aucune mesure technique de protection n'est inviolable mais chacune participe à des objectifs de sécurité, en principe définis par les titulaires de droits des contenus numériques, ce qui permet de les qualifier ou non d'« efficaces ».

i. Le « temps caractéristique » de protection.

En dernier ressort, même si un protocole de transmission de la clef privée se révèle inviolable, la croissance rapide des capacités de calcul mises à disposition des utilisateurs pour un coût raisonnable implique que le système de sécurité finira par être cassé en un temps fini. **Pour chaque mesure technique de protection, les questions pertinentes ont donc affaire au temps** :

– combien de temps faut-il à un utilisateur averti pour acquérir un droit sur une œuvre précise de façon irrégulière ?

– combien de temps faut-il à un utilisateur averti pour développer un outil qui permet d'acquérir, sur toutes les œuvres, un droit de façon irrégulière ?

En fonction de ces «temps caractéristiques » propres à chaque technologie et à chaque génération d'utilisateurs, il est nécessaire de concevoir des solutions de mises à jour ou de remplacement. **La souplesse et l'« évolutivité » d'une technique de protection sont ainsi des critères de son « efficacité » aussi importants que sa robustesse ou que son coût.**

ii. Les critères de « renouvelabilité » : robustesse, coût.

En théorie, tout système de gestion numérique des droits, comme tout système de protection technique, peut être contourné par un utilisateur malveillant, dès lors que l'utilisateur est maître de l'environnement technique. Or, le «cœur de sécurité » d'un système de gestion numérique des droits repose sur les éléments d'architecture suivante :

– le mode de stockage du secret caché dans chaque décodeur ;
– l'interface entre ce secret et le serveur de gestion de droits ;
– l'interface entre ce secret et le module de déchiffrement.

Un système est piraté dès lors que l'un de ces trois éléments de l'architecture de sécurité passe sous le contrôle de l'utilisateur. Par conséquent, chacun de ces éléments doit pouvoir être remplacé facilement au moment où une faille du système est découverte. Les situations de « **renouvelabitilité** » diffèrent cependant selon la nature de l'implémentation de chaque élément dans le système de protection :

– ***Dans le cas d'une implémentation matérielle de l'un des trois éléments de l'architecture de sécurité, le remplacement est nécessairement physique :***

– S'il s'agit d'un circuit intégré, le remplacement est très coûteux puisqu'il faut changer au minimum un circuit imprimé, sur lequel peuvent se trouver d'autres circuits intégrés. Si par exemple le composant est sur la carte mère d'un ordinateur, alors il faut remplacer celle-ci. Cette solution suppose que la technique de protection soit extrêmement robuste ;

– S'il s'agit d'une carte à puce insérée dans un lecteur, il suffit de remplacer cette carte. Cette opération peut être réalisée manuellement, par un utilisateur néophyte. Une carte à puce peut aisément être envoyée par courrier à l'ensemble des utilisateurs. Toutefois le coût d'une telle opération n'est pas négligeable, et cette solution suppose aussi que la technique de protection soit très robuste.

– Dans le cas d'une implémentation logicielle de l'un des trois éléments de l'architecture de sécurité, le remplacement est rarement physique.

– S'il s'agit d'une protection logicielle de même niveau, le remplacement nécessite l'installation d'un nouveau code logiciel, qui peut être transmis aux utilisateurs soit par support optique, soit par un réseau de télécommunications. C'est une opération simple, à la portée de tous les utilisateurs, et peu coûteuse. Cette solution convient donc pour des techniques moyennement robustes ;

– S'il s'agit d'une protection logicielle qui requiert des moyens de calculs plus importants, au remplacement logiciel pourrait s'ajouter un remplacement matériel.

Encadré 3.17. — Exemples de solutions de protection sur supports optiques.

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

Au-delà de la simple mise à jour des lecteurs logiciels en réponse à la découverte de failles de sécurité, la connexion bidirectionnelle des lecteurs logiciels avec un serveur de droits autorise d'autres applications de protection du droit d'auteur. Il est ainsi possible de concevoir un système où les lecteurs installés sur les ordinateurs sont capables de détecter les œuvres piratées stockées sur les disques durs de ces ordinateurs, et procèdent à leur effacement.

Inversement, les solutions matérielles, par exemple les décodeurs de la télévision numérique à péage, sont plus robustes. Mais il est plus coûteux de modifier le système de protection, puisqu'il faut envoyé à chaque abonné une nouvelle carte à puce.

Or, les mesures de protection matérielles étant plus robustes que les mesures de protection logicielles, **une grille de choix d'objectifs de sécurité** peut s'établir facilement en fonction de la valeur économique du contenu numérique à protéger, de l'environnement technique et des usages des utilisateurs, du coût initial des techniques, de leur robustesse, et de leur renouvelabilité qui peut aussi s'appuyer à la renouvelabilité commerciale de l'environnement technique. S'agissant de la distinction principale entre les solutions de protection, on peut établir la grille suivante :

Tableau 3.3. – Evaluation des objectifs de sécurité

Solutions	Robustesse	Coût de renouvelabilité	Risque de « piratage fatal »
- matérielles	+	+	-
- logicielles	-	-	+

3.3.4.3. L'interopérabilité des décodeurs.

Qu'il soit matériel ou logiciel, un décodeur interagit avec les éléments techniques suivants :

– un serveur de droits, pour émettre des requêtes et recevoir des licences ;

– un médium de distribution donné, par lequel il reçoit les œuvres sous forme protégée ;

– des copies numériques protégées, qu'il lit ou bien qu'il crée.

Sachant que le langage du serveur de droits, et le codage de l'œuvre sur un médium sont généralement choisis simultanément par le distributeur, l'interopérabilité d'un décodeur se situe à deux niveaux :

– **La compatibilité entre un décodeur et un système de distribution**. On observe des situations très variables en fonction du médium :

– dans le cas des **réseaux de télévision par câble**, le décodeur est généralement fourni par le distributeur, et n'est compatible qu'avec son réseau,

– la situation sur les **réseaux par satellite est mixte**, chaque décodeur présentant une compatible partielle avec chacun des réseaux ;

– dans le cas des **supports optiques**, il existe des normes qui font que pour un standard donné, n'importe quel disque pourra être joué avec n'importe quel lecteur, et vice-versa ;

– sur **Internet**, les principaux décodeurs existants aujourd'hui utilisent un mode de codage différent. Un site web souhaite être compatible avec tous les utilisateurs doit donc juxtaposer des encodeurs et proposer des téléchargements de flux correspondant à chacun des décodeurs, par exemple *Real Player*, *Windows Media Player* et *Quicktime*.

– **La compatibilité entre deux décodeurs**.

Deux décodeurs sont interopérables entre eux lorsque les copies réalisées par l'un d'eux sont lisibles par l'autre, et vice-versa. De même, la situation dépend du médium :

– les décodeurs utilisés sur les réseaux de diffusion audiovisuelle ne sont en général pas munis de fonction de copie numérique. Des décodeurs munis de disques durs comment à apparaître, mais ils ne possèdent pas de sortie numérique : les copies sont forcément locales ; [135]

– les décodeurs associés aux supports optiques protégés comme le SACD ne possèdent pas de fonction de copie et n'en posséderont jamais, c'est en effet un principe qui est au cœur de la sécurité du SACD. Certains lecteurs de DVD Vidéo

[135] Par exemple le décodeur « G2 » de *Canal+ Technologies.*

disposent d'une fonction graveurs, ou bien peuvent être reliés à un graveur. La compatibilité des disques est alors totale ;

– certains décodeurs utilisés sur Internet permettent de réaliser des copies, éventuellement après acquisition des droits de copies. Il se peut que plusieurs distributeurs utilisent des décodeurs provenant du même constructeur, mais par exemple, les copies réalisées avec un décodeur logiciel de *Microsoft* ne seront pas lisibles avec un décodeur logiciel de *Sony*.

D'une manière générale, l'interopérabilité favorise la concurrence, elle permet d'abaisser les coûts de production et accroît la valeur d'usage de chaque produit. Elle est dans l'intérêt des industriels comme dans celui des utilisateurs, d'où l'importance des processus de normalisation qui peuvent conditionner l'avenir d'une technologie. De façon pratique, elle signifie que les consommateurs pourront utiliser leurs copies originales avec une plus grande part des leurs équipements électroniques, et auront un risque plus faible de ne plus pouvoir les utiliser lorsqu'ils renouvellent ces équipements.

Dans certaines conditions économiques, certains acteurs peuvent avoir intérêt de refuser l'interopérabilité de leurs produits en vue de constituer des marchés monopolistiques. Ce cas de figure est plus fréquent dans l'industrie des décodeurs logiciels, où les coûts marginaux de production sont très faibles.

L'interopérabilité ne nuit pas nécessairement à la sécurité, pourvu que les interfaces assurant celle-ci, fassent également l'objet d'une protection. La sécurité peut imposer des limites à l'intéropérabilité, dans la mesure où un système jugé «sûr » ne doit pas être compatible avec un système jugé « non sûr ». Cependant, lorsqu'un titulaire de droit juge que deux mesures techniques équivalentes sont, en fonction de ses objectifs de sécurité, « sûres », au point de les mettre en œuvre, il serait dans son intérêt que ces mesures techniques sont interopérables.

* * *
*

Fig. 3.34. – Périmètre technique des copies et utilisations dans un usage conforme.

		Accès illimité	**Copie numérique** *« à usage strictement privé »*	**Copie numérique** *« à usage non privé »*	**Prêt**	**Copie analogique**	**Interopérabilité**
	CD Audio	OUI	OUI	OUI	OUI	OUI	Totale
	CD Audio protégé (ex. *Macrovision*/*Midbar*)		NON	NON			Limitée à certains lecteurs (qu'ils soient CD Audio, CR-ROM, SACD ou DVD)
	SACD						Limitée aux lecteurs SACD
	DVD-A						Limitée aux lecteurs DVD-A
	DVD Vidéo						Totale
	TV Num en diffusion (Sat, Câble, TNT, ADSL)	OUI	CTL	NON	NON		Limitée au sein du réseau de l'opérateur, et des accords d'interconnexion
	TV Num à la demande (Sat, Câble, TNT, ADSL)	NON					
	Téléphone portable	CTL	CTL		CTL		
	Réseau privé personnel (ex. *Smartright*, *Sony*, *Philips*)	OUI	OUI		NON		Limitée aux matériels compatibles
	Internet (ex : *Wanadoo*, *Club-Internet*, *Tiscali*, *TF1.fr* …)	CTL	CTL	CTL	CTL		Limitée au logiciel de lecture choisi par le distributeur selon *DRMS*

CTL = contrôlé par l'opérateur, soit une fois pour toutes, soit à chaque consommation.

CONCLUSION

L'état des lieux des mesures techniques de protection des Systèmes numériques de gestion des droits réalisée réalisé ne constitue qu'une photographie des techniques mises en œuvre ou destinées à l'être dans les toutes prochaines années. Un point principal mérite d'être souligné dans le cadre d'une conclusion qui ne peut être que provisoire :

Par souci de clarté, la présentation précédente a distingué les mesures techniques des systèmes numériques de gestion des droits. Les premières ont tendance à procéder à l'intégration de techniques de cryptographie et de techniques de tatouage. Les systèmes numériques de gestion de droits privilégient les techniques de cryptographie mais peuvent aussi se combiner avec des techniques de tatouage. Plus encore, si les mesures techniques de protection ont d'abord cherché à interdire ou contrôler la copie numérique, elles tendent à présent à se combiner avec des systèmes numériques de gestion de droits pour établir les modes de contrôles de copie.

Dans ce contexte, les distinctions juridiques de la directive 2001/29, notamment celle qui distingue le domaine dans lequel, les Etats membres de l'Union européenne peuvent prendre des mesures appropriées pour rendre possible la copie privée numérique (art. 6.4 §§ 2 et 3) et le domaine dans lequel ils ne peuvent intervenir (art. 6.4. §4) en ce qui concerne les services interactifs à la demande, risquent de devenir obsolètes ou d'application difficile.[(136)]

* * *
*

[(136)] cf. deuxième partie de l'étude : La régulation des mesures techniques.

ANNEXES

Pour éviter des annexes qui pourraient prendre une place exorbitante, le choix a été fait d'indiquer le plus souvent dans le corps du rapport et en note de bas de page des références à des liens hypertextes féconds en références utilisées pour l'étude. En revanche, il apparaît très souhaitable qu'un site dédié aux mesures techniques de protection et aux DRMS puisse être mis en place communément par le Ministère de la Culture et de la Communication et le Ministère de l'industrie.

LISTE DES PERSONNES CONSULTÉES

Commission européenne.

- Jorg REINBOTHE, Chef d'Unité, Droits d'auteur et droits voisins, Commission européenne, DG Marché Intérieur.
- Barbara NORCROSS-AMILHAT, Droits d'auteur et droits voisins, Commission européenne, DG Marché intérieur.
- Julie SAMNADDA, 2nd National Expert, Droits d'auteur et droits voisins, Commission européenne, DG Marché intérieur.
- Timothy FENOULHET, Policy Planning Unit, Commission européenne, DG Société de l'Information.

Administrations françaises.

- Stéphane MIEGE, Relations industrielles, Secrétariat Général de la Défense National.
- Emmanuel CAQUOT, Chef du service des technologies et de la société de l'information, DiGITIP, Ministère de l'Industrie.
- Francois-Xavier GEORGET, Chef du Service des Techniques et des réseaux de communication, Direction du Développement des Médias.
- Jean Joseph MARIANI, Directeur du Département Technologies de l'information, Ministère de la Recherche, RNRT.
- Hélène de MONTLUC, Chef du Bureau de la propriété littéraire et artistique, Ministère de la culture et de la communication.
- Muriel FOULONNEAU, Relais Culture Europe.
- Jean MENU, Directeur du Multimédia, CNC.
- Marie-Joëlle ANTOINE, Ingénieur en normalisation Secrétaire de la commission de normalisation française Codage des Médias, AFNOR.
- Nicole CAPPEL-SOUQUET, Ingénieur en normalisation, Identification et numérotation des documents ; Évaluation des résultats ; Records Management, AFNOR.
- Christophe LEROUGE, Attaché pour la Science et la Technologie, Mission pour la Science et la Technologie, Consulat Général de France.
- Arnaud VUILLERMET, Chef de Secteur Audiovisuel — Musique — Nouveaux Médias.

Au titre des questions juridiques.

- Pierre SIRINELLI, Professeur, Paris I.
- André LUCAS, Professeur, Nantes.
- Christophe CARON, Professeur, Paris XII.
- Séverine DUSOLLIER, Professeur, Faculté universitaire de Louvain.
- Maurice VIENNOIS, Conseiller Honoraire à la Cour de Cassation, membre de la CNIL.
- Francis BRUN-BUISSON, Conseiller Maître à la Cour des Comptes, Président de la Commission L.311-5 du CPI.
- Luc DEREPAS, Maître des requêtes au Conseil d'Etat.
- Caroline COMBES, Avocat au Barreau de Paris, Benssoussan et Associés.
- Jean MARTIN, Avocat au Barreau de Paris.
- Marc MOSSE, Avocat au Barreau de Paris.
- Cyril ROJINSKY, Avocat au Barreau de Paris.

Chercheurs.

- Michel RIGUIDEL, Chef du Département Informatique et Réseaux, ENST.
- Jacques STERN, Directeur, ENS.
- Henri MAITRE, Responsable du Département Traitement du Signal et des Images, ENST.
- Yves DESWARTE, LAAS-CNRS
- Alain PUISSOCHET, IDATE, responsable de la veille techno-économique.
- Frédéric RAYNAL, chercheur, INRIA, Rédacteur en chef de www.security-labs.org.
- Bernard LANG, INRIA, Vice Président de l'AFUL

Industriels et représentants.

- Xavier AUTEXIER, Délégué général, SFIB.
- Bernard HEGER, Délégué général, SIMAVELEC.
- Francisco MINGOSRANCE, BSA Europe.
- Xavier BRINGUE, Senior Development Manager, New Media Platforms Division, Microsoft.
- Véronique ETIENNE-MARTIN, Conseiller auprès de la Direction générale, Microsoft.
- Jack JACQUET, Video and Broadcast Manger, Digital Media Solutions, Europe, Middler East and Africa, IBM.
- Jean-Charles HOURCADE, Senior Vice President, Research & Innovation, Thomson Multimédia.
- Olivier LAFAYE, Innovation Projects, Thomson Multimédia.
- Fabien BATTINI, Thomson Multimedia R&D, technical advisor.
- Michel CAMPIONI, Deputy CEO, Chief strategy Officer, Canal + Technologies.
- Pierre-Yves LE GUEN, Canal + Technologies.
- Gilbert BORELLI, Responsable de la sécurité des systèmes d'information, Canal+

- Didier GRAS, Responsable de la Sécurité, Noos.
- Frédéric CHARTIER, Chef de laboratoire multimédia Thales Communications.
-Jean-Michel MASSON, General Manager, Nextamp.
- Alain BELFILS, General Manager, Philips.
- Issa RAKHODAI, Senior Technology Expert, Philips.
- Emmanuel VIGOT, Software, Advanced development Manager Philips.
- Daniel LECOMTE, CEO, Medialive.
- Jens-Henrik JEPPESEN, Government Affairs Manager, Europe, Middle East & Africa, Intel.
- Philippe THOREL, Directeur Général, MPO.
- Gilles MATON, Mémotion
- Josiane MOREL, European Government Affairs Manager, Apple.
- Roland LOUSKI, Vice President Legal Department, Info2clear.
- Marta VILLAR, EU Regulatory Affairs Manager, HP.
- Roger VERCAMMEN, Director, External Relations Europe, Sony.
- Roger BRUNET, Directeur des Relations Extérieures, General Manager, External Affairs, Sony France.
- Jean BARDA, Project Technical Manager, Netimage, 2Kan.
- Claude L. ROLLIN, Chargé de mission Images Fixes.
- François-Xavier NUTTAL, Consultant, Conseiller normes et informatiques à la CISAC, fondateur d'Audiosoft.
- Vincent PUIG, Directeur des relations extérieures, IRCAM.
- Michel RICHARD, Responsable du Département Multimédia, RMN.
- Thomas BIJON, Coordinateur des productions en ligne, RMN.
- Daniel TERUGGI, Direction recherche et expérimentation, Directeur, INA.
- Frédéric DUMAS, Direction recherche et expérimentation, Chef de projet, INA.
- Didier GIRAUD, Direction recherche et expérimentation, Chargé de mission, INA.
- Jean-Christophe LE TOQUIN, Délégué général AFA.
- Jean-Michel GRAPIN, CEO, Yacast.
- Ali MOUHOUB, Directeur du marketing et du développement département musique, Yacast.

Distributeurs, utilisateurs et consommateurs.

- Stanislas HINTZY, Directeur général, OD2.
- Franck ABIHSSIRA, directeur général adjoint e-TF1.
- Julien DOURGNON, Chargé de mission, UFC-Que Choisir ?
- Frédérique PFUNDER, Chargée de mission, CLCV

Représentants des titulaires de droits. [(137)]

- Olivia REGNIER, Senior Legal Adviser European Affairs, IFPI
- Ted SHAPIRO, Vice president & General Counsel, MPA.
- Laurence DJOLAKIAN, Deputy Legal Counsel, MPA.

[(137)] Dans un premier temps, la réalisation de l'étude devant se consacrer aux aspects techniques, les points de vue ont été surtout exprimés au sein des travaux du CSPLA ou lors des rendez-vous pour la réalisation du rapport sur le guichet commun, voire sur la lutte contre la contrefaçon.

- Eric BAPTISTE, Secrétaire général, CISAC.
- Pascal NEGRE, Président Universal Music France.
- Loïc DACHARY, Fondation pour le Logiciel Libre.
- Bernard MIYET, Président, SACEM.
- Thierry DESURMONT, Vice Président, SACEM.
- Pascal ROGARD, Délégué général, ARP, CSPEFF.
- Olivier CARMET, Directeur général, SACD.
- Nicole ZMIROU, Directrice juridique, SACD.
- Philippe VINCENT, SACD.
- Hervé RONY, Syndicat National de l'Edition Phonographique.
- Frédéric GOLDSCHMIDT, Syndicat National de l'Edition Phonographique.
- Xavier BLANC, Directeur des Affaires Juridique et Internationales, SPEDIDAM.
- Laurent DUVILLIER, SCAM.
- Marc GUEZ, Secrétaire général, SCPP.
- Daniel DUTHIL, Président, APP.
- Jérôme ROGER, Directeur général, SPPF.
- Florence-Marie PIRIOU, Société des Gens de Lettres de France, Responsable juridique.
- Arlette STROUMZA, SNE.

* * *
*

TABLE DES MATIERES