F

OMPI

WCT-WPPT/IMP/3
ORIGINAL : anglais
DATE : 3 décembre 1999

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE

GENÈVE

ATELIER SUR LA MISE EN ŒUVRE DU TRAITE DE L'OMPI SUR LE DROIT D'AUTEUR (WCT) ET DU TRAITE DE L'OMPI SUR LES INTERPRETATIONS ET EXECUTIONS ET LES PHONOGRAMMES (WPPT)

Genève, 6 – 7 décembre 1999

MESURES DE PROTECTION TECHNIQUES : AU CROISEMENT DE LA TECHNIQUE, DE LA LEGISLATION ET DES LICENCES COMMERCIALES

Exposé de Dean S. Marks[*] *et Bruce H. Turnbull*[**]

[*] Conseiller principal en propriété intellectuelle, Time Warner Inc., Burbank, Californie

[**] Partner, Weil, Gotshal & Manges LLP, Washington

TABLE DES MATIÈRES

Introduction[1]

Les progrès des techniques analogiques comme des techniques numériques offrent aux "propriétaires de contenu" de nouvelles possibilités de distribuer leurs œuvres, et aux consommateurs de nouveaux moyens de recevoir et d'apprécier ces œuvres[2]. Toutefois, de tels progrès représentent aussi un défi majeur : en effet, comment ces œuvres peuvent-elles être protégées dans un monde où i) la reproduction est aisée et peu coûteuse; ii) chaque copie effectuée (qu'elle le soit à partir de l'original ou d'une autre copie) est parfaite; et iii) la distribution aux utilisateurs du monde entier peut être réalisée pratiquement gratuitement et sans aucun délai par le biais de l'Internet? Ce défi est particulièrement crucial dans le monde d'aujourd'hui où le consommateur n'est plus simplement le destinataire des œuvres, mais peut aussi transmettre et redistribuer ces œuvres à autrui. Pour le compliquer encore, les œuvres protégées par le droit d'auteur circulent désormais dans un environnement qui comprend à la fois les appareils électroniques grand public, les ordinateurs, les satellites et les réseaux mondiaux tels que l'Internet.

Au fur et à mesure que les législateurs, les propriétaires de contenu et les fabricants d'électronique grand public et d'informatique (à la fois de matériels et de logiciels) s'efforçaient de relever ce défi, plusieurs points devenaient évidents. En premier lieu, ni la technique ni les mesures juridiques ne peuvent prises séparément offrir une solution viable. En deuxième lieu, la conception et la mise en œuvre de techniques et de structures de protection contre la copie nécessitent une coopération et des compromis entre les secteurs du contenu, de l'électronique grand public, de l'informatique et les autres secteurs pertinents. En troisième lieu, la protection contre la copie doit répondre à deux préoccupations clés : i) celle du traitement des œuvres à l'intérieur des appareils (notamment des lecteurs, appareils d'enregistrements, ou ordinateurs personnels), et ii) celle du traitement des œuvres lorsqu'elles sont transmises d'un appareil à l'autre (par exemple d'un décodeur à un téléviseur puis à un appareil d'enregistrement) ou par le biais de réseaux avec ou sans fil (tels que l'Internet). En quatrième lieu, la mise en œuvre de la protection contre la copie doit tenir compte des attentes légitimes du consommateur et de considérations financières. En cinquième lieu, les techniques et structures de protection contre la copie doivent prendre en compte l'innovation, la vitesse et l'esprit d'ouverture qui ont caractérisé la révolution de l'information et de l'Internet. Le défi qui consiste à fournir une protection appropriée aux œuvres est à la fois difficile et complexe; aussi, les solutions ne sont ni simples ni unidimensionnelles.

---

[1] Les auteurs ont participé activement au débat sur les questions législatives et techniques relatives aux licences qui sont abordées dans le présent document : M. Marks au nom de la Time Warner, du point de vue du secteur des « propriétaires de contenu » et M. Turnbull au nom de son client, Matsushita Electric Industrial Co., Ltd., du point de vue du secteur de l'électronique de grand public. Toutefois, les avis exprimés dans le présent document appartiennent strictement à leurs auteurs et ne reflètent pas nécessairement les positions de leurs entreprises ou clients respectifs.

[2] Le présent document porte sur les œuvres audiovisuelles et les enregistrements sonores. Toutefois, des préoccupations similaires existent pour les œuvres écrites ou littéraires (y compris les logiciels informatiques) et certains des principes généraux exposés dans le présent document peuvent s'appliquer dans ces autres contextes.

Les efforts qui sont actuellement déployés pour renforcer les structures de protection contre la copie ont démontré qu'il était nécessaire d'adopter une approche en trois volets. Le premier volet consiste dans l'élaboration de mesures de protection techniques et dans leur mise à disposition à des conditions raisonnables. Le deuxième volet est constitué des lois qui soutiennent les techniques de protection et interdisent le contournement de ces techniques. Le troisième volet est composé des négociations intersectorielles et des licences relatives aux mesures de protection techniques. Ces licences imposent des obligations visant à garantir que lorsque l'accès à des œuvres protégées par des mesures techniques est octroyé, des règles appropriées en matière de lutte contre la copie et d'usage sont suivies. Le présent document a pour objet d'examiner ces trois volets et d'expliquer pourquoi les différents éléments qui les composent sont indispensables.

Afin de placer ces questions dans leur contexte, nous décrirons brièvement certaines des évolutions qui sont à l'origine du défi à relever. Nous examinerons ensuite les trois volets de manière générale. Dans le cadre de notre présentation du deuxième volet, nous exprimerons notre avis sur la manière dont les dispositions anticontournement des deux traités de l'OMPI devraient être mises en œuvre. Ensuite, nous décrirons de manière relativement détaillée un certain nombre de techniques et de structures de protection contre la copie qui ont récemment vu le jour ou qui sont en cours de mise au point et de négociation. Bien que de nombreuses questions politiques, techniques voire juridiques restent irrésolues, les travaux accomplis à ce jour ont apporté certains résultats concrets et permis de poser des jalons pour aller de l'avant.

GÉNÉRALITÉS : LES EVOLUTIONS TECHNIQUES QUI CONSTITUENT LE DEFI ACTUEL A LA PROTECTION DES ŒUVRES

Les évolutions techniques sont souvent une lame à double tranchant pour les créateurs et les propriétaires de contenu. D'une part, elles fournissent des instruments plus sophistiqués pour la création et une diffusion légitime des œuvres. D'autre part, ces mêmes techniques facilitent souvent la reproduction et la distribution illicites d'œuvres, en violation des droits des propriétaires de contenu. Ce dilemme n'est pas nouveau; il a vu le jour avec l'apparition de la presse écrite. Au cours des dernières années toutefois, certains progrès techniques lui ont donné une nouvelle dimension d'importance . Il s'agit notamment des progrès suivants :

La reproduction numérique : Les copies analogiques d'œuvres audio ou vidéo voient leur qualité se dégrader à chaque reproduction. Ainsi si une personne fait une copie d'une vidéocassette analogique et la donne à un ami, cette copie ne sera pas aussi bonne que l'original. Une nouvelle copie faite à partir de la première sera de qualité encore plus médiocre. La technique analogique comporte ainsi un obstacle intrinsèque aux reproductions multiples et donc un obstacle à la reproduction massive et illicite par les consommateurs. La reproduction numérique quant à elle est une reproduction bit par bit. Cela signifie que chaque copie est parfaite et que des copies parfaites peuvent être faites à partir d'autres copies, de manière illimitée. En outre, la reproduction numérique peut être faite à des vitesses très élevées sans perte de qualité. La menace de reproduction illicite est par conséquent beaucoup plus sérieuse avec l'apparition de la reproduction numérique. Actuellement, la facilité avec laquelle un signal analogique peut être converti sous un format numérique pour être ensuite diffusé rapidement signifie que la transmission par voie analogique pose également des problèmes et doit être prise en compte dans le cadre des efforts de protection contre la copie.

La compression : Lorsqu'elles sont converties sous forme numérique à résolution intégrale, les œuvres audio et vidéo comportent de grandes quantités de données. Avant l'apparition des techniques de compression numérique, il était nécessaire de disposer d'une bande passante substantielle ou de longues périodes de temps pour transmettre ce type d'œuvres par réseau. Les techniques de compression, telles que les techniques MPEG-2 pour la vidéo et MP-3 pour la musique, ont modifié cette situation. Certaines techniques de compression permettent actuellement la création de copies parfaites "sans perte" dont la taille est inférieure à 25% de la taille numérique de l'original. Cela signifie que ces copies peuvent être transmises dans un délai représentant un quart du temps nécessaire à la transmission des originaux non comprimés. On prévoit que de nouvelles techniques de compression permettront d'obtenir des copies pratiquement sans perte, représentant 5% de la taille de l'original. Il convient de noter que certaines méthodes de compression aboutissent à une copie "avec perte" d'une qualité légèrement inférieure. Ce type de copie, tout en n'étant pas une réplique parfaite de l'original, comporte généralement des défauts qui ne peuvent pas être perçus par le spectateur ou l'auditeur. Aujourd'hui, la compression avec perte type fournit des copies qui représentent moins de 2% de la taille numérique de l'original, les prévisions tablant sur une réduction équivalant à 0,5% de la taille de l'original à l'avenir. Ces progrès immenses dans les techniques de compression signifient qu'il deviendra de plus en plus facile, rapide et pratique de transmettre, dans leur intégralité, des œuvres audio et vidéo de grande qualité, par le biais de réseaux tels que l'Internet.

Bande passante : Les élargissements de la bande passante sont synonymes de capacité accrue, permettant la transmission de davantage de données plus rapidement. Les modems câbles et lignes téléphoniques DSL à grande vitesse sont désormais à la disposition des consommateurs pour leurs connexions à l'Internet. Ces services permettent la transmission de données à une vitesse environ neuf fois supérieure à celle fournie par le modem téléphonique classique de 56K bauds. Selon certains, les capacités de bande passante continueront à croître au point de fournir des vitesses qui seront plusieurs centaines de fois supérieures à celles des modems utilisés actuellement. Ces progrès en matière de bande passante rendront largement plus aisée la distribution d'œuvres de grande qualité à de nombreuses personnes, dans des délais très courts et moyennant un coût réduit.

Les réseaux : Comme de plus en plus de personnes sont désormais "connectées" et reliées au réseau Internet, de plus en plus nombreux sont ceux qui disposent de liaisons duplex entre le monde extérieur et leur domicile. L'installation en réseau des appareils personnels chez soi (tels que les ordinateurs, les appareils d'enregistrement et les systèmes haute fidélité) se développe au fur et à mesure que les utilisateurs exigent une plus grande interactivité des appareils qu'ils achètent. Cela permet aux utilisateurs à la fois de recevoir et de transmettre les œuvres à partir de leur domicile et de les faire circuler de l'un de leurs appareils à l'autre (par exemple d'un ordinateur personnel vers un enregistreur numérique). Grâce à ces réseaux, il est aisé pour un non-professionnel de faire et de distribuer de multiples copies d'œuvres audio ou vidéo de grande qualité. De fait, chaque consommateur qui est relié à l'Internet peut devenir un rééditeur pirate et publier des œuvres.

Les progrès techniques décrits ci-dessus signifient que la piraterie visant le contenu n'est plus uniquement l'apanage de pirates opiniâtres utilisant un matériel coûteux pour reproduire des œuvres puis des circuits matériels de distribution (depuis les marchés aux puces et vendeurs à la sauvette jusqu'aux boutiques de revente au détail) pour distribuer ce type de copies illicites. Aujourd'hui, un consommateur possédant quelques milliers de dollars de matériel chez lui peut faire et distribuer un nombre illimité de copies d'œuvres illicites de grande qualité.

PREMIER VOLET : LES MESURES DE PROTECTION TECHNIQUES : LA REPONSE TECHNIQUE AU DEFI LANCE PAR LA TECHNIQUE ET LES LIMITES DES TECHNIQUES DE PROTECTION CONTRE LA COPIE

Selon l'expression de Charles Clark, souvent entendue dans les enceintes de débat, "la réponse à la machine est dans la machine elle-même". De fait, un ensemble de mesures techniques ont été mises au point pour contribuer à la protection des œuvres. Ces mesures sont brièvement décrites à l'annexe A. Même s'il est vrai que les mesures techniques existantes ou les nouvelles mesures en cours d'élaboration peuvent être utilisées pour répondre à certaines des préoccupations soulevées par les progrès des techniques numériques et analogiques décrites ci-dessus, les techniques de protection contre la copie ne constituent pas à elles seules une solution, pour plusieurs raisons.

En premier lieu, les mesures de protection techniques – quelle que soit leur efficacité – seront toujours vulnérables aux attaques de pirates opiniâtres, notamment parce que les capacités de traitement des matériels et logiciels informatiques continuent à croître rapidement. Par conséquent, il faut qu'il y ait des garde-fous juridiques au contournement des techniques de protection contre la copie. En outre, il existe de réelles contraintes économiques à l'efficacité des mesures de protection techniques susceptibles d'être mises en œuvre au sein des œuvres protégées par le droit d'auteur et des dispositifs de lecture. Les mesures de protection technique ne peuvent par conséquent pas empêcher la piraterie lorsqu'elle est le fait d'individus ou d'organisations disposant d'importantes ressources. Elles serviront plutôt surtout simplement à "faire en sorte que les honnêtes gens le restent" – à faciliter le respect des droits sur les œuvres – et à ériger des obstacles face à ceux qui cherchent à porter atteinte à de tels droits.

En deuxième lieu, les propriétaires de contenu tirent des bénéfices du fait que leurs œuvres sont vues, écoutées et lues par le public. Les créateurs souhaitent généralement que leurs œuvres soient connues du public et, pour les investisseurs comme pour les créateurs, l'encouragement à la création et à la distribution des œuvres passe par l'existence d'un large public composé de consommateurs légitimes et payants. Les œuvres de création ne sont pas comparables à l'or; il n'y a aucun intérêt à les enfermer dans un coffre fort. Par conséquent, les techniques de protection contre la copie doivent être mises en œuvre de façon à ne pas interférer avec la distribution et la communication légitimes des œuvres au public. Cet impératif rend d'autant plus complexe la mise au point et l'utilisation de ces techniques de protection. Il signifie qu'à toutes fins utiles, elle ne peuvent pas être unilatérales. Les enregistrements sonores et les œuvres audiovisuelles ne peuvent être appréciés que par l'utilisation d'appareils de réception et de lecture, tels que les téléviseurs, les lecteurs de cassettes ou de disques compacts, les magnétoscopes, les ordinateurs personnels, etc.. Les propriétaires de contenu ne peuvent donc pas appliquer à leurs œuvres des mesures techniques qui empêcheraient tout appareil de réception ou de lecture de recevoir ou de retransmettre ces œuvres. Il convient aussi de noter que l'objectif consistant à protéger les œuvres ne peut être atteint si les appareils de réception, de lecture ou d'enregistrement au lieu de reconnaître les techniques de protection contre la copie et d'y réagir, ne font que les ignorer. En conséquence, pour fonctionner de manière appropriée, ces techniques doivent être à double sens : les techniques utilisées par les propriétaires de contenu doivent fonctionner avec les appareils électroniques et informatiques utilisés par les consommateurs et ces appareils doivent respecter les techniques appliquées et réagir à ces techniques. Cette double condition signifie que les solutions ne sont pas simplement une question d'innovation technique. Des techniques de protection efficaces contre la copie nécessitent aussi un degré élevé de concertation et elles doivent être mises en œuvre à la fois par les fournisseurs de contenu et

les fabricants d'électronique grand public et de produits informatiques. Il est possible de parvenir à cet objectif par le biais de la législation, qui pourra exiger que certains types d'appareils répondent à des techniques particulières de protection contre la copie, ou par le biais de la négociation d'accords intersectoriels.

En troisième lieu, la mise en œuvre de techniques de protection peut être sévèrement limitée par le problème de l'existence d'un parc d'appareils grand public installés antérieurement qui ne peuvent fonctionner avec ce type de techniques. Ainsi, sur les disques compacts, la musique n'est pas codée. Si les maisons de disques commençaient à coder les œuvres musicales figurant sur les disques compacts, celles-ci ne pourraient être lues par les lecteurs de disques que les consommateurs possèdent actuellement. Le moment idéal pour mettre en œuvre des techniques de protection contre la copie est celui de l'introduction de nouveaux supports ou systèmes de transmission, tels que le DVD ou la radiodiffusion numérique.

En quatrième lieu, les œuvres qui sont déjà sur le marché sans être équipées de techniques de protection contre la copie ne peuvent l'être a posteriori. Cependant, ce contenu non protégé peut être manipulé relativement aisément pour tirer parti des progrès des techniques de reproduction et de transmission. Ainsi, par exemple, les consommateurs peuvent désormais, à partir de disques compacts, enregistrer des œuvres musicales sur des disques vierges ou les télécharger sur l'Internet. Il est évident que ce type d'activité constitue une infraction aux lois sur le droit d'auteur et les droits connexes. Mais il faut reconnaître que la technique est quasiment – si ce n'est totalement – impuissante face à ce type de problème particulier.

Outre qu'il existe les limites décrites plus haut, il est peu probable que des protections techniques soient mises en œuvre dans tous les contextes et pour tous les supports. En conséquence, des régimes juridiques forts, composés de lois sur le droit d'auteur et les droits connexes renforcées par des moyens de sanction et de recours efficaces, restent indispensables. Le "Global Business Dialogue on Electronic Commerce" (GBDe) a récemment reconnu cet impératif[3]. Au nombre des principes et de recommandations consensuelles formulés par le GBDe en ce qui concerne la propriété intellectuelle, lors de la conférence de Paris de septembre 1999, figure notamment l'appel suivant :

"Le commerce électronique ne se développera pas au mieux de ses possibilités tant que les problèmes de sanction des lois sur le droit d'auteur ne seront pas résolus.

Action gouvernementale requise :

- fournir aux titulaires de droits des moyens efficaces et adaptés d'intenter des actions en sanction du droit d'auteur – quelle que soit la juridiction – lorsqu'il y a eu atteinte;

---

[3] Le « Global Business Dialogue on Electronic Commerce » (Dialogue des entreprises au niveau mondial sur le commerce électronique – GBDe) représente une collaboration au niveau international entre des entreprises actives dans le domaine du commerce électronique. Plusieurs centaines d'entreprises et d'associations commerciales ont participé au processus de consultation du GBDe. La représentation au sein du GBDe est diversifiée sur le plan géographique comme sur le plan sectoriel.

- favoriser, dans tous les pays, le renforcement des procédures judiciaires, des voies de recours, et des règles en matière de responsabilité en cas d'atteinte au droit d'auteur, afin de parvenir à une sanction efficace et de prévenir les atteintes; et
- promouvoir un programme de sensibilisation au droit d'auteur du public, des organisations du secteur et des organismes d'enseignement, de façon à informer les utilisateurs de l'importance de la protection au titre du droit d'auteur et du respect des lois sur le droit d'auteur, qui conjointement permettent d'encourager les activités créatrices."

Nous avons constaté que la technique ne peut à elle seule relever le défi de la protection des œuvres contre la reproduction et la distribution illicite massive dans les nouveaux contextes actuels. Nous avons également recensé certaines des difficultés rencontrées dans la mise en œuvre des techniques de protection contre la copie. Ces limites indiquent que des mesures de sauvegarde juridique particulières doivent être prévues à l'appui de ces techniques.

DEUXIEME VOLET : LA LEGISLATION A L'APPUI DES TECHNIQUES DE PROTECTION : IL EST INDISPENSABLE D'ELABORER DES LOIS ANTINEUTRALISATION EFFICACES ET DE METTRE EN ŒUVRE LES TRAITES DE L'OMPI

Les mesures de protection techniques doivent être appuyées de façon appropriée d'un point de vue législatif et juridique : i) de façon à garantir leur respect et ii) à empêcher leur contournement par des individus qui pourraient ainsi violer les droits des propriétaires de contenu. Cet impératif a été reconnu à la fois dans le Traité de l'OMPI sur le droit d'auteur et dans le Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes. Selon l'article 11 du Traité de l'OMPI sur le droit d'auteur, :

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

L'article 18 du Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes comporte une disposition similaire.

Bien que les traités de l'OMPI incluent une interdiction générale de la neutralisation des mesures de protection techniques, un débat s'est engagé sur la question de savoir comment ce principe général devait être mis en œuvre dans le cadre des législations nationales. Il a essentiellement porté sur trois questions : i) l'interdiction doit-elle s'étendre aux dispositifs aussi bien qu'aux actes de neutralisation? ii) faut-il exiger que le matériel satisfasse à certaines mesures de protection particulières? et iii) quelles sont les exceptions appropriées à cette interdiction? Nous estimons qu'en mettant en œuvre les dispositions antineutralisation des deux traités, la loi sur le droit d'auteur (Digital Millenium Copyright Act) adoptée en 1998 aux États-Unis d'Amérique a résolu chacune de ces questions de façon appropriée. Il n'est pas dans notre intention de décrire cette loi de manière très détaillée dans ces pages mais plutôt de tirer parti des notions et solutions qu'elle définit dans le cadre de notre approche des trois questions ci-dessus et de notre réflexion sur les éléments indispensables à l'obtention de lois antineutralisation efficaces et équilibrées.

Actes ou dispositifs?

Les deux traités de l'OMPI restent silencieux sur la question de savoir si les dispositions antineutralisation s'appliquent uniquement aux actes visant à la neutralisation ou également aux dispositifs et services qui sont conçus ou distribués pour contourner les techniques de protection. Pour plusieurs raisons, une approche centrée uniquement sur les actes est insuffisante. Généralement, ces actes ne sont pas publics; ils sont habituellement entrepris dans l'intimité des foyers ou des lieux de travail. Alors que les résultats de ce type d'activité – par exemple un logiciel utilitaire qui va neutraliser une mesure de protection contre la copie – peuvent être rendus publics, l'acte conduisant au démantèlement du système de protection est habituellement privé. Il n'est ni faisable ni souhaitable d'entreprendre un suivi systématique des actes privés afin d'empêcher les activités de neutralisation. De toutes façons, la plupart des gens ne consacreront ni le temps ni les efforts nécessaires au démantèlement d'une mesure de protection contre la copie de leur propre chef. Si, toutefois, ils peuvent légalement acheter (ou recevoir gratuitement) des dispositifs ou des services qui neutralisent ces mesures, il devient alors beaucoup plus difficile de résister à la tentation et de satisfaire à l'objectif visé par les techniques de protection. Cette notion n'est pas nouvelle. De nombreux pays interdisent par exemple la fabrication, la vente ou la distribution de cartes à mémoire ou de décodeurs pirates qui sont utilisés pour décrypter et recevoir, sans autorisation ni paiement, les émissions de télévision par satellite ou par câble dont l'accès est réservé. En conséquence, pour qu'il existe des sanctions efficaces contre la neutralisation, la législation doit proscrire les appareils et produits qui sont conçus ou distribués dans le but de contourner les techniques de protection.

Le GBDe a également recommandé que les législations nationales mettant en œuvre les deux traités de l'OMPI "interdisent les activités nuisibles liées à la neutralisation en réglementant à la fois les actes et les dispositifs, tout en prévoyant des exceptions appropriées... qui permettent de préserver l'équilibre global entre titulaires de droits et utilisateurs" (soulignage ajouté).

S'il est clair qu'une législation efficace de lutte contre la neutralisation doit s'appliquer aux dispositifs comme aux services, il n'est pas simple de fixer les limites qui aboutiront à l'interdiction de tel ou tel système ou service. Les cas extrêmes sont relativement simples. Ainsi les "boîtes noires" ou décodeurs pirates qui servent uniquement, par exemple, à décrypter illégalement les signaux télévisuels (c'est-à-dire qui neutralisent le contrôle d'accès au cryptage) ou à déjouer les mesures de protection contre la copie sont des systèmes qui doivent clairement être illégaux. Les ordinateurs personnels traditionnels, à l'autre extrême, sont parfois utilisés par les pirates informatiques pour déjouer les mesures de protection contre la copie qui sont incluses dans les logiciels. Malgré le fait qu'ils sont parfois utilisés à des fins illicites, les ordinateurs ne doivent pas être interdits en tant que dispositifs de contournement puisque d'une manière générale, ils sont utilisés à des fins et pour des fonctions largement légitimes. Le problème consiste à savoir où passe la frontière entre ces deux extrêmes.

La plupart des gens conviendraient que le fait d'incorporer une horloge à un décodeur pirate ne doit pas rendre l'appareil légitime simplement parce que les fonctions d'horloge d'une partie de cet appareil sont légitimes. Toutefois, nombreux sont ceux qui avanceraient qu'un dispositif permettant la lecture d'un contenu vidéo analogique par ordinateur mais ayant aussi pour résultat d'éliminer de ce contenu les indicateurs de contrôle de copie, doit pouvoir être autorisé. Nous sommes d'avis que la loi sur le droit d'auteur des États-Unis a atteint un équilibre satisfaisant dans ce domaine difficile : en premier lieu, en instaurant

trois tests différents visant à déterminer si un service ou un appareil doit être interdit du fait de ses fonctions de neutralisation; elle prévoit en outre que ce test peut être appliqué aux parties ou composants d'un dispositif ou service, et non seulement à celui-ci dans son intégralité. En conséquence, est interdit tout service ou dispositif, – ou toute partie ou composant de celui-ci – qui entre dans l'une ou l'autre des catégories suivantes :

- il est essentiellement conçu ou produit pour la neutralisation;
- en dehors de la neutralisation, l'intérêt de sa fonction ou de son usage commercial n'est que limité; ou
- il est commercialisé pour être utilisé dans le cadre de la neutralisation.

Un dispositif, un service, une partie ou un composant qui entre dans l'une des trois catégories susmentionnées est interdit et ne peut être ni fabriqué, ni importé, ni vendu, ni distribué d'une autre façon. La seconde composante de l'équilibre atteint par la loi américaine réside dans les dispositions de "non prescription" abordées ci-après. Une telle approche peut utilement servir de modèle à d'autres pays qui s'apprêtent à introduire les dispositions antineutralisation des traités de l'OMPI dans leur législation nationale. Nous sommes d'avis qu'une approche en ce sens de la législation de lutte contre la neutralisation est nécessaire pour apporter le soutien juridique approprié aux mesures de protection techniques.

Réaction à certaines techniques de protection

Les techniques de protection contre la copie entrent actuellement dans deux catégories générales : les mesures qui permettent de contrôler l'accès au contenu, telles que le cryptage, et les mesures qui permettent de contrôler la reproduction du contenu telles que les systèmes SCMS ou Macrovision[4]. Les techniques de contrôle de l'accès, telles que le cryptage, aboutissent généralement à des situations claires pour ce qui est de l'application des lois antineutralisation. Si le contenu est crypté, un dispositif de lecture ou d'enregistrement peut soit ignorer le contenu sous forme cryptée, soit décrypter ce contenu pour qu'il devienne visible ou accessible à l'utilisateur final. Ce décryptage ne peut être le fruit du hasard : il nécessite une action déterminée du dispositif visant à "déverrouiller" les contrôles figurant sur le contenu et à le rendre accessible. Par conséquent, le décryptage sans autorisation constitue un contournement[5].

---

[4] L'annexe A donne une définition du cryptage et une description des systèmes SCMS et Macrovision.

[5] Toutes les structures de protection contre la copie décrites ci-après qui ont été récemment mises en œuvre ou qui sont en cours de négociation au sein du secteur s'appuient sur le cryptage du contenu en tant que principe de base. Et cela précisément parce que le contenu qui est crypté ne peut être décrypté "par hasard". Les fabricants de produits autorisés qui choisissent de participer aux structures de protection contre la copie "s'engagent", obtiennent une licence et conviennent de suivre les règles de protection contre la reproduction pour pouvoir obtenir les clés de décryptage du contenu. Le décryptage du contenu sans autorisation (c'est-à-dire sans posséder une licence) constitue clairement le type d'activité que les lois anti-contournement doivent d'une manière générale interdire.

Les techniques qui permettent de contrôler la reproduction du contenu, telles que les indicateurs de contrôle de copie, posent davantage de questions complexes pour ce qui est de l'application des lois antineutralisation. Cela est dû au fait que le bon fonctionnement de ces techniques est généralement subordonné à une réaction du dispositif de lecture ou d'enregistrement. Dans le cas du cryptage, si le dispositif de lecture ne réagit pas de manière à déverrouiller – décrypter – le contenu, celui-ci reste crypté et protégé. Dans le cas des indicateurs de contrôle de copie par contre, si l'appareil ne recherche pas délibérément les indicateurs et n'y réagit pas, alors le contenu n'est pas protégé et risque de faire l'objet d'une reproduction illicite.

Certaines des techniques de protection contre la copie les plus avancées en usage aujourd'hui, telles que les systèmes SCMS et Macrovision, ne sont pas efficaces pour les ordinateurs personnels. La raison ne tient pas tant au fait que les ordinateurs outrepassent ou suppriment ces protections, mais plutôt au fait qu'ils ne les "recherchent pas" et n'y réagissent pas. Le secteur informatique s'est fortement opposé à l'idée de toute prescription législative selon laquelle les ordinateurs personnels devraient être conçus de façon à rechercher et à réagir à des indicateurs ou à des bits de contrôle de copie particuliers. Le secteur informatique est en particulier hostile au principe selon lequel un ordinateur serait obligé d'examiner tous les flux de données entrants à la recherche de ce type d'indicateur ou de bit. La préoccupation du secteur est accrue par l'éventualité pour les ordinateurs de devoir réagir à toutes les techniques de protection contre la copie, quelles qu'elles soient, qui sont susceptibles d'être adoptées par un propriétaire de contenu donné. Ce type de préoccupation est également partagé par le secteur de l'électronique grand public.

D'où une question clé qui a vu le jour dans le cadre du débat sur la portée et les prescriptions de lois antineutralisation appropriées, à savoir : le fait de ne pas réagir à certaines techniques de protection contre la copie constitue-t-il un acte de neutralisation? Les fabricants de matériel ne veulent pas, ce qui est compréhensible, avoir la responsabilité de garantir que leurs dispositifs sont en mesure de réagir à diverses techniques de protection contre la copie connues (voire inconnues). D'un autre côté, les propriétaires de contenu estiment à juste titre que les fabricants de matériel ne doivent pas être autorisés à concevoir leurs produits de façon à ce qu'ils échappent délibérément aux techniques de protection contre la copie ou les ignorent. Cette question épineuse a été résolue par la loi sur le droit d'auteur des États-Unis moyennant l'adoption de la disposition dite de "non prescription". Cette disposition précise que l'interdiction des dispositifs de neutralisation ne signifie pas que les fabricants d'électronique grand public, de matériel de télécommunication ou d'informatique sont tenus de concevoir leurs produits ou des parties et composants déterminés de ceux-ci dans le but précis de répondre à une mesure technique particulière, quelle qu'elle soit, pour autant que les produits ou parties en question ne rentrent pas par ailleurs dans le cadre des interdictions découlant des trois tests décrits plus haut (c'est-à-dire qu'ils ne soient pas essentiellement conçus ou produits pour la neutralisation; qu'en dehors de la neutralisation, l'intérêt de leur fonction ou de leur usage commercial ne soit pas que limité, et qu'ils ne soient pas commercialisés pour être utilisés dans le cadre de la neutralisation)[6].

---

[6] Le présent débat a uniquement trait aux lois antineutralisation. Dans certains cas, d'autres lois exigeront que le matériel soit conçu de manière à répondre à des techniques de régulation de la copie particulières. La loi sur le droit d'auteur des États-Unis comporte notamment une disposition prévoyant que les magnétoscopes analogiques doivent réagir au système Macrovision.

Exceptions appropriées

Les législations nationales prévoient généralement certaines limitations et exceptions aux droits des auteurs et des titulaires de droits connexes, notamment en cas d'usage loyal ou de bons usages. La Convention de Berne et les deux traités de l'OMPI adoptés en 1996 fixent les grandes lignes de ces exceptions et limitations des droits. D'une manière générale, ces exceptions et limitations ne peuvent être prévues que "dans certains cas spéciaux où il n'est pas porté atteinte à l'exploitation normale de l'œuvre ni causé de préjudice injustifié aux intérêts légitimes de l'auteur" ou des titulaires de droits connexes[7].

Selon une préoccupation fréquemment exprimée, le développement des mesures de protection techniques amènera les propriétaires de contenu à "verrouiller" leurs œuvres et empêchera les utilisateurs de faire valoir à bon droit les exceptions aux droits des propriétaires de contenu. Cette préoccupation est sans doute alarmiste pour plusieurs raisons. En premier lieu, les propriétaires de contenu sont généralement tributaires d'une large consommation publique de leurs œuvres. Ainsi, même si certaines versions ou certains supports de ces œuvres sont sécurisés moyennant des techniques de protection, ces techniques doivent être suffisamment transparentes pour permettre un accès aisé en vue des usages licites. En deuxième lieu, il est possible de garantir aisément la disponibilité des œuvres à des fins publiques, notamment dans les bibliothèques, archives et établissements scolaires, moyennant des accords de licence voire des lois spécifiques. Il n'est pas nécessaire (ni même très efficace) d'imposer des restrictions aux mesures de protection techniques pour répondre à des préoccupations de ce type. En outre, les mesures techniques peuvent fonctionner quel que soit le régime applicable au contenu et à un utilisateur donné. Ainsi, les bibliothèques peuvent obtenir à moindre coût, voire gratuitement, des licences de contenu lorsque des mesures techniques aident effectivement à mettre en place ce type de licences en permettant l'usage dans le cadre de la bibliothèque mais en empêchant la reproduction et la redistribution illicites du contenu. En troisième lieu, il est peu probable que les mesures de protection technique soient appliquées à tous les supports. En dernier lieu, les mesures techniques peuvent effectivement faciliter certaines exceptions et limitations aux droits des propriétaires de contenu, notamment par le biais de la technique de "reproduction unique" qui permet aux consommateurs d'effectuer une seule copie d'une œuvre. Il semblerait prudent de faire preuve de mesure en ce qui concerne l'autorisation d'exceptions en matière de neutralisation des mesures techniques jusqu'à ce que le marché pour les mesures techniques soit davantage développé et sous réserve de l'apparition de problèmes particuliers.

Les traités de l'OMPI ne prévoient pas précisément d'exceptions à l'obligation de fournir une protection juridique appropriée contre la neutralisation. Toute exception éventuelle à la législation antineutralisation doit être élaborée avec circonspection et limitée à des cas spéciaux dans lesquels il n'est pas porté atteinte à l'application et au fonctionnement normaux des techniques de protection ni causé de préjudice injustifié aux intérêts légitimes des propriétaires de contenu à employer ce type de techniques de protection. Parce que les dispositifs et les services, du fait de leur nature même, ne peuvent être limités à des usages particuliers, les exceptions aux lois antineutralisation ne leur semblent pas bien adaptées. Il serait préférable d'envisager ces exceptions conjointement à certains types d'actes individuels et sous réserve d'un ensemble de conditions raisonnables. Les législateurs doivent se montrer

---

[7] Voir les articles 9.2), 10 et 10*bis* de la Convention de Berne, ainsi que l'article 10 du Traité de l'OMPI sur le droit d'auteur et l'article 16 du Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes.

prudents et utiliser des critères tels que : i) la disponibilité générale des œuvres (et non des différents supports), ii) l'incidence que toute exception éventuelle aux règles antineutralisation pourrait avoir sur la valeur des œuvres et l'efficacité des techniques de protection et iii) l'existence de contrats de licence entre les titulaires des droits et les bibliothèques publiques et archives, lorsque des exceptions sont envisagées. En dernier lieu, les législateurs doivent aussi tenir compte des possibilités de reproduction qui dans la pratique sont intégrées aux structures de protection anticopie en cours d'élaboration. Les mesures techniques peuvent s'avérer utiles pour faciliter certaines exceptions et limitations aux droits des propriétaires de contenu. Si cela fonctionne dans la pratique, il y a alors peu d'intérêt à prévoir des exceptions à la règle générale visant à lutter contre le contournement de ces mesures.

La loi sur le droit d'auteur des États-Unis d'Amérique prévoit certaines limitations et exceptions rédigées avec circonspection à l'interdiction générale de neutralisation. En premier lieu, l'interdiction des actes de neutralisation individuels ne s'appliquent qu'aux techniques de protection de l'accès et non aux techniques qui empêchent la copie. D'autres limitations et exceptions sont prévues dans les cas suivants : i) dans le cadre de la sanction des lois et d'autres activités gouvernementales; ii) pour les bibliothèques publiques, les archives et les établissements d'enseignement, uniquement pour déterminer s'ils souhaitent obtenir un accès autorisé aux œuvres; iii) pour la rétroingénierie, uniquement pour parvenir à l'interopérabilité; iv) pour la recherche en matière de cryptage et les tests de sécurité; et v) pour la protection de la vie privée et des mineurs. Les exceptions susmentionnées sont définies avec précision et sont assorties de conditions qui visent à maintenir un certain équilibre et à empêcher les exceptions de rendre inopérante la règle générale visant à lutter contre le contournement.

Chaque pays a ses propres préoccupations spécifiques quant aux exceptions et limitations. Nous estimons que ces préoccupations doivent faire l'objet d'un examen attentif. Les mesures techniques et les dispositifs de contournement sont incapables de déterminer si l'objectif du contournement est licite ou non. Toute exception et limitation éventuelle à la règle de la lutte contre le contournement doit s'appliquer à certains types d'actes individuels bien définis. Les interdictions frappant les dispositifs et services de neutralisation doivent rester fermes et ne peuvent être assouplies. À ce jour, les mesures de protection techniques n'ont pas empêché un usage loyal des œuvres et rien ne prouve que ces mesures auront un tel effet à l'avenir. Nos travaux dans le domaine des protections techniques nous ont conduit à la conclusion que les lois antineutralisation doivent fournir un moyen de dissuasion efficace et des moyens de recours adaptés pour que réparation soit obtenue. Dans ce domaine, des lois fortes et efficaces sont essentielles parce que les mesures techniques ne peuvent qu'être des obstacles à un usage illicite et qu'elles courront toujours le risque d'être contournées.

Les structures de protection contre la copie décrites ci-après reposent sur des accords en matière de techniques et de licences. Des lois antineutralisation efficaces sont indispensables pour garantir que ces structures et accords ne sont pas sapés par ceux qui choisissent soit de n'y pas participer soit de les enfreindre. Les lois doivent encourager la participation et l'adhésion à ces structures et accords et faire en sorte que ceux qui choisissent de n'y pas participer ne puissent agir de manière déloyale en contournant les mesures de protection technique. Parce que les œuvres et les techniques de protection traversent les frontières à un rythme toujours plus soutenu, une mise en œuvre correcte et rapide des dispositions

antineutralisation de l'OMPI par un nombre aussi important que possible de pays est essentielle[8].

TROISIEME VOLET : NEGOCIATIONS ET LICENCES INTERSECTORIELLES : LE DEVELOPPEMENT DES STRUCTURES DE PROTECTION CONTRE LA COPIE

Bien que les mesures de protection techniques constituent le premier volet des structures de protection contre la copie, nous avons exposé comment dans les faits diverses limitations empêchent les mesures techniques d'apporter une solution entièrement satisfaisante. Nous avons ensuite abordé le second volet de la protection contre la copie, à savoir les mesures juridiques et notamment les lois interdisant le contournement. Nous avons expliqué pourquoi des lois antineutralisation fortes et effectivement appliquées sont nécessaires pour conforter l'efficacité des mesures techniques. Nous nous attachons désormais au troisième volet de la protection contre la copie : les accords et structures intersectoriels qui permettent de mettre en œuvre des mesures de protection techniques et d'établir des règles en vue d'un traitement approprié du contenu, moyennant des contrats de licence commerciale.

Premiers efforts

Les premières tentatives visant à mettre en œuvre des mesures de protection contre la copie avaient une portée quelque peu étroite; ainsi en est-il du système SCMS[9] mis au point pour les œuvres musicales numériques, qui permet d'effectuer sans limitation des copies de première génération des enregistrements numériques, mais empêche les copies de deuxième génération ou les copies en chaîne (c'est-à-dire que les copies faites à partir de l'original sont autorisées sans aucune limite, mais qu'il n'est pas possible de faire de nouvelles copies à partir de ces premières copies). L'introduction à l'échelle mondiale du système SCMS a été le résultat de négociations et d'un accord qui a finalement été conclu entre les maisons de disques et les fabricants d'électronique grand public en 1989. Dans certains pays, comme les États Unis, des lois ont finalement été promulguées pour exiger des dispositifs d'électronique grand public qu'ils réagissent au système SCMS. Néanmoins, les accords et lois concernant le système ne sont pas parvenus à inclure le secteur informatique. Ainsi, les ordinateurs personnels qui sont aujourd'hui capables de diffuser et d'enregistrer de la musique numérique ne sont pas tenus de souscrire au système SCMS.

Le cryptage de certaines émissions télévisuelles, notamment les émissions diffusées par câble ou satellite constituent un autre exemple. Le cryptage a été mis au point pour ce type d'émissions afin de garantir que seuls les consommateurs qui y sont autorisés (c'est-à-dire qui acquittent leur abonnement) soient en mesure de décrypter et de regarder les émissions. Telle qu'elle est appliquée actuellement par les entreprises de radiodiffusion par câble et par satellite, la technique de cryptage protège les émissions uniquement jusqu'à ce qu'elles

---

[8] Un exemple récent confirme l'urgence de la question. En Norvège, le système de cryptage permettant de protéger les DVD a récemment été piraté puis placé sur un site Web à partir d'un serveur situé dans le pays. Toutefois la Norvège, comme de nombreux autres pays, n'a pas encore promulgué de législation antineutralisation du type de celle que prescrivent les traités de l'OMPI.

[9] Voir l'annexe A pour la description du système SCMS.

atteignent le décodeur autorisé du consommateur. Une fois que le signal est décrypté, le contenu est à la disposition du consommateur sans aucune autre protection technique contre la reproduction ou redistribution illicite.

Prise de conscience actuelle et principes généraux

Les tentatives actuelles visant à concevoir et à mettre en œuvre des structures de protection contre la copie s'efforcent de pallier certains de ces inconvénients. Les propriétaires de contenu réalisent qu'il est important de fournir un certain degré de protection quel que soit le contexte : supports physiques, radiodiffusion, Internet, etc. Ils comprennent aussi la nécessité de travailler avec les secteurs de l'électronique grand public, de l'informatique, de la radiodiffusion et finalement des télécommunications afin d'élaborer et de mettre en œuvre des techniques de protection et des règles d'usage du contenu. Cette prise de conscience a conduit à la reconnaissance de l'ensemble des objectifs et principes généraux ci-après qui guident les efforts de protection contre la copie déployés actuellement :

Participation volontaire aux structures de protection contre la copie : Les fournisseurs de contenu ne doivent pas être obligés d'utiliser les techniques de protection contre la copie. D'une manière générale, les fabricants de dispositifs doivent être libres de choisir s'ils souhaitent ou non participer à une structure de protection contre la copie. Si, toutefois, ils décident de n'y pas participer, leurs produits ne doivent alors ni neutraliser ni entraver ces techniques de protection.

Le contenu doit être crypté : Le cryptage du contenu est essentiel pour faire clairement la distinction entre les usages autorisés et les usages illicites, notamment dans le domaine informatique. Aucun individu ni dispositif ne peut décrypter un contenu par hasard. En conséquence, le cryptage du contenu est la clé de voûte des efforts déployés actuellement en matière de protection contre la copie.

Les règles de protection contre la copie imposées par les licences de cryptage/décryptage : Le cryptage et le décryptage des contenus nécessitent une licence pour la technique de cryptage pertinente. Cette licence comportera des obligations concernant les règles de protection contre la copie à suivre (par exemple reproduction interdite, reproduction unique autorisée, etc.) pour pouvoir décrypter le contenu et le rendre accessible à l'utilisateur. Les règles de protection contre la copie doivent parvenir à un équilibre entre les droits des propriétaires de contenu, et les attentes légitimes des consommateurs. Une fois que le contenu a été crypté, tout dispositif sous licence décryptant le contenu se conforme aux obligations contractuelles établies par la licence et visant au respect des règles de protection contre la copie. L'idéal serait que le contenu contienne en filigrane ces règles de protection et les conditions d'usage du contenu. Un dispositif qui ne fait pas l'objet d'une licence peut transmettre ou véhiculer un contenu crypté sans restrictions, pourvu que ce dispositif ne décrypte pas ni ne permette d'une autre manière l'accès au contenu. Tout dispositif qui ne fait pas l'objet d'une licence et qui décrypte le contenu enfreint la législation antineutralisation (ainsi que les droits patrimoniaux des propriétaires de la technique de cryptage).

Application aux dispositifs et systèmes : Une protection efficace contre la copie nécessite l'application de techniques et d'obligations en matière de protection contre la copie à tous les dispositifs et services pouvant lire, enregistrer et/ou transmettre le contenu protégé. Étant donné l'existence des réseaux et de l'Internet, tous les dispositifs et "stations intermédiaires" des systèmes de transmission doivent assurer au contenu la même sécurité qu'à la réception et ne doivent ni contourner les protections ni transmettre en clair le contenu aux dispositifs ou composants suivants. Cela signifie que des dispositifs et systèmes de ce type ne peuvent pas véhiculer, par le biais de connexions analogiques ou numériques, un contenu qui a été légitimement décrypté vers d'autres dispositifs et systèmes ne disposant pas de protections appropriées.

Contrôle d'enregistrement et de lecture : Les dispositifs et systèmes ne doivent pas permettre la relecture (ou la rediffusion) à partir d'un support réenregistrable, d'un contenu qui porte le filigrane "reproduction interdite" ("no copy")[10]. Si le filigrane "reproduction interdite" figure sur le support réenregistrable, cela signifie que l'enregistrement était au départ illicite. De la même façon, il ne doit pas y avoir de relecture à partir d'une copie d'un contenu qui porte l'inscription "reproduction unique autorisée" ("copy once") mis à part cette unique copie autorisée. L'idéal serait que les dispositifs d'enregistrement lisent et répondent aux filigranes et refusent de reproduire un contenu portant l'inscription "reproduction interdite".

Disponibilité des techniques à des conditions raisonnables et non discriminatoires : Les mesures de protection techniques doivent être largement disponibles à des conditions équitables et non discriminatoires afin d'être mises en œuvre par toutes les parties pertinentes (les fabricants de matériel, les propriétaires de contenu et les opérateurs de systèmes notamment).

Assurer de façon durable une protection utile : Les systèmes et les techniques de protection contre la copie doivent offrir aux œuvres une protection utile de manière durable. Par conséquent, ces systèmes doivent permettre le rejet de dispositifs qui ont été altérés ou copiés. En outre, les techniques contenues dans ces systèmes doivent être renouvelables de façon à ce qu'une intrusion pirate unique n'en anéantisse pas l'efficacité.

Alors qu'il est relativement simple de définir les objectifs et principes susmentionnés, leur mise en œuvre dans le cadre de structures de protection contre la copie est dans la pratique loin d'être aisée. Nous nous proposons d'examiner à présent de façon plus détaillée la conception et la mise en place de certaines de ces structures, en commençant par le DVD – vidéo ou vidéodisque numérique.

Introduction du disque numérique universel (DVD) vidéo

L'introduction du DVD a été l'occasion d'élaborer certaines techniques visant à limiter la reproduction. Le DVD permet d'obtenir une image de très bonne qualité sur un disque 5 pouces pratique et résistant à l'usure et aux dommages et de proposer des options intéressantes pour le consommateur, telles que les versions multilingues. Le DVD vidéo a été conçu pour pouvoir être utilisé aussi bien sur des appareils électroniques grand public que sur des micro-ordinateurs. L'arrivée de ce nouveau support d'images animées était attendu avec

[10] L'annexe A donne une définition du filigrane.

impatience aussi bien par les fabricants d'appareils électroniques grand public que par les fabricants d'ordinateurs. Pour les fabricants de matériel électronique, le marché des magnétoscopes analogiques était déjà relativement saturé et le vidéodisque permettait de proposer une nouvelle génération d'appareils qui pourraient être très demandés par les consommateurs et occasionner de nombreuses ventes de matériel. Pour les fabricants de matériel informatique, le DVD permettait à l'ordinateur personnel de faire son entrée dans les équipements audio et vidéo des ménages en tant que support d'enregistrement de films. Les producteurs de cinéma, par contre, n'étaient pas prêts à diffuser leurs films sur ce nouveau support numérique sans protection contre la reproduction et la diffusion sauvages, et en particulier la reproduction et la diffusion par des moyens numériques. Le DVD étant un support nouveau, c'était le moment ou jamais de lui intégrer une protection anticopie. En l'absence de parc existant de lecteurs de DVD ou d'unités de lecture de DVD pour les ordinateurs personnels, la protection anticopie pouvait être conçue et intégrée aux nouveaux appareils dès l'origine[11].

Origines du CPTWG et protection anticopie des DVD vidéo

La nécessité de constituer un groupe chargé d'étudier la protection anticopie en concertation entre les trois secteurs mentionnés est devenue évidente au printemps 1996, moment où les groupements professionnels représentant les grandes sociétés de production de cinéma et les groupements professionnels représentant les fabricants de matériel électronique grand public ont présenté aux sociétés informatique une proposition commune de législation. Selon cette proposition, tous les dispositifs permettant l'enregistrement numérique de films devaient rechercher, lire et exécuter des éléments de protection anticopie figurant dans le contenu, qu'il s'agisse de disques DVD ou d'autres supports matériels, ou encore d'émissions radiodiffusées par exemple. Les sociétés informatiques ont immédiatement réagi de façon unanime et vigoureuse en faisant savoir qu'une telle méthode de protection anticopie était contraire à leur conception du rôle des pouvoirs publics (à savoir que ceux-ci n'avaient pas à intervenir dans la conception des produits informatiques), ne pouvait être mise en pratique techniquement sans porter préjudice au fonctionnement des matériels informatiques, et qu'elle était trop incertaine quant à son résultat pour justifier un effort particulier de la part des sociétés informatiques pour s'adapter au système.

Constatant que les fabricants de matériel électronique grand public s'apprêtaient à mettre sur le marché des lecteurs de DVD, qu'ils souhaitaient disposer de disques préenregistrés contenant des films, que les producteurs de cinéma tenaient à ce qu'une protection anticopie suffisante soit prévue pour le contenu de ces DVD, et que la proposition de législation n'avait pas abouti, les trois secteurs ont constitué deux groupes de travail. Le premier de ces groupes était chargé d'étudier les questions de politique générale et le deuxième, dénommé *Copy Protection Technical Working Group* (CPTWG), les questions techniques. Le groupe de travail chargé des questions de politique générale s'est réuni à

[11] Même à ce moment très favorable d'introduction d'un nouveau support, certaines limites demeurent. Par exemple, pour être bien accueillis par les consommateurs, les lecteurs de DVD doivent être compatibles avec le parc de téléviseurs existant. Par conséquent, les techniques de protection anticopie adoptées devaient être telles que les DVD passés sur des lecteurs dans des conditions légales puissent être regardées sur des téléviseurs plus anciens.

plusieurs reprises sans arriver à avancer sur la question des dispositions législatives qui pourraient être acceptables pour le secteur informatique tout en constituant un dispositif satisfaisant du point de vue des objectifs de protection anticopie du secteur du cinéma. C'est pourquoi l'essentiel des activités s'est concentré sur le groupe technique.

À partir de la première semaine de mai et jusqu'à la mi-juillet 1996, le CPTWG et sa section DVD se sont réunis presque chaque semaine, avec généralement des participants venant des États-Unis, du Japon et de l'Europe. Les représentants du secteur informatique considéraient que le cryptage du contenu était le point de départ de tout système de protection anticopie. Les représentants du secteur du matériel électronique grand public ont commencé par s'opposer à cette idée, craignant que le cryptage ne constitue une lourde charge pour les appareils, en accroissant leur complexité et leur coût. Après un certain nombre de réunions, deux sociétés, Matsushita Electric Industrial Co., Ltd. ("MEI", fabricant et distributeur de produits sous les marques Panasonic, Quasar et National) et Toshiba Corporation ont proposé un procédé anticopie réunissant les caractéristiques suivantes : i) le procédé était conçu spécifiquement pour le support DVD; ii) il tenait compte des contraintes de conception du matériel électronique grand public; iii) reposant sur le cryptage du contenu à protéger, il répondait aux vœux des sociétés informatiques; iv) il permettait d'imposer des règles assorties de sanctions légales contre la reproduction et la diffusion illicites dans des conditions acceptables pour les producteurs de cinéma grâce à un système de licence commerciale.

Les critères de conception fondamentaux auxquels devaient correspondre les techniques de protection anticopie et le système de licence étaient les suivants :

– une protection technique et juridique suffisante pour compliquer la tâche aux moins scrupuleux, c'est-à-dire pour que le consommateur ordinaire ne puisse réaliser facilement une copie du contenu protégé au moyen des outils dont il dispose normalement;

– une protection technique et juridique suffisante pour empêcher la mise au point d'un moyen utilisable et accessible à tous de contourner les obstacles imposés par les dispositifs techniques et le système de licence;

– une mise en œuvre dans les produits informatiques et dans les appareils électroniques telle que la complexité et le coût supplémentaires soient minimes;

– des licences qui soient à la fois suffisantes pour assurer la protection juridique nécessaire et peu onéreuse pour les fabricants et des distributeurs d'appareils;

– un fonctionnement transparent pour le consommateur, sauf lorsque celui-ci s'efforce de réaliser des copies illicites de contenus protégés.

Enfin, il était posé dès le départ que les sociétés de production et les fabricants d'appareils ne seraient pas tenus de recourir aux techniques en question et de prendre les licences correspondantes. D'autres dispositifs de protection anticopie pour les DVD pouvaient être mis au point et lancés sur le marché, ce qui a d'ailleurs été le cas[12].

---

[12] La plus connue des autres solutions proposées est le système DIVX lancé par Circuit City et un groupe d'investisseurs privés.

La proposition technique mise au point par MEI et Toshiba a été étudiée en étroite coordination avec d'autres participants du CPTWG; elle a été présentée au départ au "Consortium DVD" afin que les responsables du développement du DVD apportent leur appui au système de protection, reconnu comme convivial par rapport à ce nouveau support. MEI et Toshiba ont alors présenté cette proposition au CPTWG plénier à la mi-juillet. Un travail intensif a été accompli au cours des trois mois suivants pour mieux définir la technique et étudier les règles de son utilisation, afin d'être sûr que la protection était à la fois adéquate du point de vue des producteurs de cinéma et raisonnable du point de vue des sociétés chargées de sa mise en œuvre dans leurs appareils.

Les études techniques ont comporté une évaluation précise du dispositif par les sociétés du secteur informatique, afin de s'assurer que la mise en œuvre des fonctions de décryptage dans le logiciel n'exigeait pas une puissance de traitement déraisonnable. Étant donné que MEI et Toshiba avaient des activités de production de circuits intégrés et d'autres éléments de matériel pour l'élaboration des produits, le système avait été prévu à l'origine pour être mis en œuvre dans le matériel. Les grandes sociétés informatiques ont compris très rapidement que cette façon de procéder n'était pas la meilleure du point de vue du décryptage et qu'un micro-ordinateur considéré comme standard jusqu'à présent ne pourrait pas réaliser le décryptage sans épuiser la totalité ou la presque totalité de ses capacités de traitement. Plusieurs sociétés informatiques, ayant obtenu dans le cadre d'accords de confidentialité et de non-divulgation la description, très confidentielle, de la technique utilisée, se sont mises au travail pour trouver un moyen d'adapter la technique en question en vue d'une mise en œuvre dans les ordinateurs dans des conditions acceptables. Ces dispositifs révisés ont été soumis pour étude au CPTWG. Il a été convenu par consensus que la version révisée contenait une protection suffisante contre la reproduction par le consommateur. Cette version révisée du système, appelée Content Scramble System ("CSS"), est alors devenue la technique de base de la protection des DVD. On trouvera en annexe B une description plus détaillée de la technique CSS et de son fonctionnement.

Ayant décidé d'utiliser le système CSS pour crypter l'image vidéo des DVD, les représentants des différents secteurs ont dû ensuite négocier les conditions dans lesquelles le contenu des disques serait décrypté et regardé. Il ne faut pas oublier que le but de la diffusion d'images par disque DVD est de permettre aux consommateurs de regarder un film. Le procédé n'aurait aucun intérêt ni pour les consommateurs ni pour les producteurs ou fabricants si le contenu restait crypté et inaccessible. C'est pourquoi les négociations ont porté essentiellement sur la façon dont le contenu des disques DVD devait être traité par les dispositifs de lecture (soit appareil électronique, soit unité informatique) une fois décryptés. Les représentants des différents secteurs ont convenu en principe que le contenu vidéo du disque DVD ne devait pas faire l'objet de copies ni de transmissions non autorisées, y compris par Internet.

Le débat sur ces principes, ainsi que sur les règles d'utilisation du CSS, a eu lieu dans le cadre du CPTWG. Il en est résulté un consensus sur un ensemble de points. Le CPTWG lui-même n'était pas habilité à "adopter" des principes ou à les imposer à quiconque, mais leur formulation avait une fonction très importante. En effet, le dialogue mené entre tous les participants a permis à MEI de dégager un schéma général pour élaborer la licence d'utilisation de la technique CSS[13].

---

[13] MEI a joué le rôle de mandataire pour l'octroi de licences concernant la technique CSS à la fois pour elle-même et pour Toshiba.

Avant de décrire les obligations contractuelles spécifiques à la licence, il est important de comprendre tout d'abord pourquoi cette licence était nécessaire. Le système CSS élaboré par MEI et Toshiba est un système exclusif; ces deux sociétés ont mis au point un procédé technique sur lequel elles possèdent des droits de propriété intellectuelle. C'est pourquoi toute personne souhaitant utiliser la technique CSS, que ce soit pour crypter ou pour décrypter, doit obtenir une licence. Cette licence, outre qu'elle confère un droit d'utilisation, est assortie de "serrures" et de "clés" techniques nécessaires au fonctionnement. Dans la mesure où l'utilisateur doit prendre une licence, il est possible de lui imposer des obligations sur les modes d'utilisation et le traitement du contenu après décryptage. Pour que la technique soit effectivement utilisée par les diffuseurs de contenu, les fabricants de matériel électronique et les fabricants d'ordinateurs, il était essentiel que ces trois secteurs aboutissent à un accord sur les obligations imposées par la licence.

Du fait du consensus qui s'est dégagé sur certains principes au sein du CPTWG, MEI pouvait considérer comme très vraisemblable qu'une licence d'utilisation de cette technique reprenant les principes en question serait acceptée par les participants sur le nouveau marché du DVD vidéo. Dans un délai de quelques jours après la réunion du CPTWG au cours de laquelle le consensus a été atteint, quelques jours après l'accord définitif sur l'utilisation de la technique de décryptage révisée, MEI a proposé un document de licence provisoire, et les partenaires ont pu produire à la fois des DVD contenant des films cryptés et des appareils capables de lire ces films pour les consommateurs tout en les protégeant contre une éventuelle reproduction illicite par le consommateur[14].

La licence d'utilisation de la technique CSS

La licence d'utilisation de cette technique possède deux caractéristiques très particulières : tout d'abord, elle est proposée à titre gratuit, mis à part une somme modique prélevée pour compenser le coût réel d'administration du système de licences; et ensuite, la licence à long terme sera confiée à un organisme dont les propriétaires et les administrateurs seront les preneurs de licences eux-mêmes, c'est-à-dire ceux qui proposent les contenus des disques, les sociétés du secteur informatique et les fabricants de matériel électronique. Il a fallu beaucoup de temps et de négociations pour définir les procédures d'administration et de fonctionnement de cet organisme multipartite et les conditions dans lesquelles seront proposées les licences définitives, mais les documents relatifs aux licences ont désormais une forme presque définitive et la licence à long terme, accordée par l'organisme multipartite appartenant aux preneurs de licences, devrait commencer à fonctionner prochainement.

Contraintes fonctionnelles de la protection anticopie. La licence d'utilisation du CSS accordée par MEI impose au preneur de licence une série d'obligations relativement à la protection des images cryptées par CSS une fois qu'elles ont été décryptées. Les sociétés produisant des appareils de lecture sous licence doivent, en vertu du contrat de licence et de ses spécifications, employer certaines techniques définies pour maintenir la protection des images :

---

[14] Bien que la licence provisoire initiale ait été élaborée très rapidement, la licence provisoire à long terme a demandé des mois de négociation pour que les parties intéressées arrivent à un accord définitif sur un ensemble de règles d'utilisation et de protection anticopie.

La première de ces obligations est d'empêcher les consommateurs d'accéder au contenu décrypté au cours du processus de lecture.

Dans le cas de la lecture sur poste informatique, le contenu décrypté ne peut pas être placé sur des barres bus accessibles à l'utilisateur lorsqu'il est sous forme codée en MPEG. Une règle qui sera appliquée ultérieurement est que le contenu ne pourra figurer sur des bus accessibles à l'utilisateur même après décodage MPEG, étant donné que les codeurs MPEG sont très répandus pour des applications grand public. À court terme, on estime qu'un train de données protégées codées en MPEG pourrait être traité par l'ordinateur du consommateur de telle façon qu'il serait possible de réaliser une copie du contenu : c'est pourquoi la règle prévoit que le contenu codé en MPEG ne sera pas accessible sur des bus dont l'accès est normalement ouvert au consommateur. Les flux de données décodées en MPEG sont suffisamment volumineux et compliqués à manier pour un consommateur ordinaire, pour qu'il n'ait pas paru nécessaire au moment de la négociation de lui interdire l'accès à ces données. Lorsque les codeurs MPEG seront largement répandus et d'utilisation facile pour les consommateurs, ce qui sera bientôt le cas, et qu'il sera simple de maintenir le contenu décodé à l'écart des bus accessibles aux consommateurs, les spécifications imposent que les fabricants d'unités informatiques s'assurent que le contenu ne figure pas sur ces bus.

À l'origine, il n'y avait pas de spécification équivalente dans le cas du matériel électronique, compte tenu du fait que, dans des conditions normales, les consommateurs ne modifient pas le fonctionnement de leurs appareils par rapport aux paramètres fixés par le fabricant. Pour éviter d'éventuelles modifications, toutefois, les règles seront bientôt modifiées pour imposer même aux appareils électroniques l'impossibilité de faire figurer un contenu décrypté codé en MPEG sur des bus accessibles aux consommateurs, et interdisant la fabrication de configurations telles que le contenu décrypté codé en MPEG soit accessible par les consommateurs au moyen d'outils d'usage courant.

Les connexions entre les dispositifs de lecture et les autres produits sont étroitement limitées par la licence. Seules certaines connexions spécifiques sont permises, à savoir :

– les connexions standard des appareils électroniques doivent comporter des dispositifs spécifiques de protection contre la reproduction analogique : systèmes Macrovision si possible, et la version analogique des indicateurs de protection anticopie du système Copy Generation Management System pour certaines connexions;

– les connexions numériques ont été totalement proscrites, étant donné l'absence de consensus sur les systèmes de protection anticopie. Cette règle pourrait évoluer prochainement, avec l'acceptation généralisée du dispositif dénommé Digital Transmission Copy Protection et des contrats de licence correspondants.

– étant donné que les connexions pour écrans informatiques étaient déjà répandues sur le marché (dispositif RGB), le contrat de licence les autorise, malgré l'absence d'une protection anticopie reconnue.

Spécifications connexes sur les fonctions :

– Codes régionaux. Un consensus a été atteint sur le fait que des codes régionaux peuvent être mis en place dans un contexte DVD vidéo et que la licence d'utilisation du CSS est le moyen de mise en œuvre de cette spécification. On trouvera à l'annexe C des précisions complémentaires sur les codes régionaux.

– Restriction relative aux supports réenregistrables. Pour compléter les règles relatives à l'interdiction de l'accès du consommateur à des flux de données dans des conditions permettant de la reproduction de celles-ci, la licence CSS interdit d'exécuter des fonctions de lecture CSS (décryptage, etc.) pour tout contenu figurant sur un support réenregistrable. En d'autres termes, la technique CSS ne doit être utilisée que pour un contenu préenregistré sur un support produit en série et non effaçable (DVD-ROM).

Restriction de lecture applicable aux contenus non cryptés. Les diffuseurs de contenu sont libres de présenter leurs produits sous forme non crypté sur des disques DVD de tout type, mais la licence CSS interdit de placer un contenu crypté à l'origine par CSS sur un disque quel qu'il soit sous forme non cryptée. Ainsi, si un consommateur arrive à accéder aux données après décryptage et à enregistrer le contenu sur un disque DVD, la licence impose que le système de lecture reconnaisse le fait que le contenu était à l'origine crypté par CSS et ne peut être présenté sous forme non cryptée, quel que soit le support en cause. La technique d'abord employée pour arriver à ce résultat repose sur l'insertion d'un seul bit dans les données DVD, et on la considère comme très peu fiable. Le système utilisé à l'avenir pour interdire la lecture dans ce cas reposera sur une technique de filigrane que les diffuseurs de contenu pourront utiliser pour marquer le contenu, et que les appareils produits sous licence auront l'obligation de rechercher pour tout contenu présenté sous forme non cryptée.

Résistance aux attaques. Pour que les mesures mises en œuvre ne soient pas facilement contournées par les consommateurs, soit par leurs propres outils et procédés, soit au moyen de programmes ou de produits créés dans le but d'enfreindre l'interdiction de copier, la licence CSS impose aussi que les fonctions de décryptage et de protection anticopie soient difficiles à mettre en échec. La définition précise de cette obligation a donné lieu à des controverses, et certains preneurs de licence ne l'ont pas respectée dans la pratique. La faiblesse de certains systèmes de codes régionaux intégrés dans des lecteurs DVD a rendu ce dispositif inopérant dans bien des cas en 1998 et début 1999. Le rappel de cette obligation auprès des preneurs de licence, et la production d'un plus grand nombre de disques vidéo préenregistrés ou destinés à des marchés extérieurs à la région nord-américaine ont conduit à faire mieux respecter cette règle. Plus récemment, une mise en œuvre dans de mauvaises conditions de sécurité des fonctions de décryptage d'un programme de lecture a permis un piratage très médiatisé de la technique de cryptage elle-même; ce problème devra être résolu pour cette technique particulière au cours des mois à venir.

Sanctions et autres conditions de la licence. Comme nous l'avons dit, la technique CSS fait actuellement l'objet de licences accordées par MEI à titre provisoire et sera bientôt confiée à un organisme intersectoriel dénommé DVD Copy Control Administration (DVC CCA), administré par les preneurs de licences. En tant que donneur de licences, MEI a le droit de faire appliquer les conditions de la licence et les règles de spécification connexes, droit qui reviendra ultérieurement à DVD CCA. Pour tenir compte du fait que le but de la licence est de protéger le contenu, que les moyens techniques sont proposés gratuitement (sans redevance), et que la technique utilisée ajoute de la valeur aux produits uniquement dans

la mesure où elle permet l'existence de contenus qui, dans d'autres conditions, n'auraient pas été disponibles sur ce support, les diffuseurs de contenu sous licence se sont vu attribuer un droit spécial de faire appliquer la licence en tant que "tiers bénéficiaire". Ce droit a été limité à des mesures d'injonction et à d'autres mesures non pécuniaires (visant essentiellement à écarter du marché les appareils ne respectant pas les spécifications), mais le risque de s'exposer à une action en justice de la part des sociétés en question peut constituer un élément de dissuasion crédible pour les preneurs de licences qui ne respecteraient pas les règles.

Autres questions traitées par le CPTWG

Après les travaux réalisés sur la technique CSS concernant les disques DVD, le CPTWG s'est penché sur d'autres problèmes. L'un d'entre eux concerne la protection des contenus transférés par connexion numérique entre différents appareils installés chez le même consommateur. Un deuxième problème concerne le marquage du contenu par des informations de protection anticopie selon un procédé qui résisterait aux transformations normales du contenu selon les différentes procédures standard (par exemple, conversion du numérique en analogique et vice-versa).

À l'heure actuelle, le CPTWG est un lieu de débat où peuvent être présentées les techniques de protection du contenu audio et vidéo numérique contre la reproduction illicites par les consommateurs. Le groupe se réunit chaque mois à Burbank en Californie et ces réunions mensuelles rassemblent environ 125 à 150 participants. Le groupe suit régulièrement certaines questions traitées dans d'autres enceintes mais n'a pas d'ordre du jour fixé; toute personne souhaitant intervenir peut se présenter et prendre la parole. Par sa nature même, le CPTWG n'est pas un organe de décision, mais plutôt un lieu de communication et de débat. Le CPTWG a constitué, à la demande de ses membres, des groupes spéciaux de travail et de discussion consacrés à des sujets particuliers, ce qu'il continuera vraisemblablement à faire à l'avenir. La régularité des réunions du CPTWG facilite l'organisation d'autres réunions sur la protection anticopie au cours de la semaine pendant laquelle il se réunit. Les participants viennent de toutes les régions du monde et peuvent être aussi bien des représentants de petites entreprises ou des inventeurs que des représentants de grandes sociétés du secteur du cinéma, de la musique, de l'informatique et du matériel électronique[15].

L'objectif défini par l'ensemble des industriels était de trouver les moyens juridiques et techniques de rendre la fraude difficile. Les efforts déployés, cela a été bien précisé, ne prétendaient pas empêcher les pirates professionnels d'accéder au contenu protégé par le droit d'auteur ou de produire des copies illégales des œuvres. Le but était simplement d'élaborer des moyens de compliquer la tâche du consommateur ordinaire qui souhaiterait réaliser des copies ou des transmissions sauvages d'œuvres protégées.

Concernant les deux questions relatives à i) la protection du contenu sur les connexions numériques et ii) le marquage du contenu par des informations de protection anticopie résistant aux différentes conversions, le CPTWG a constitué deux groupes de travail : un Groupe de discussion sur la transmission numérique ("DTDG") et un Sous-groupe sur

---

[15] Le secteur de la musique a moins participé que les autres et, comme nous l'expliquons par ailleurs, a préféré élaborer son propre projet, dénommé Secure Digital Music Initiative, pour traiter des questions relatives à la protection anticopie concernant spécifiquement la musique.

l'occultation des données ("DHSG") – chargés de rechercher des solutions techniques pour les différents secteurs et d'étudier et analyser les propositions reçues. Les deux groupes ont débattu des méthodes qu'ils utiliseraient pour évaluer les propositions, ont élaboré des projets et invité les intéressés à leur en soumettre et ont étudié et analysé les propositions reçues. Aucun des groupes n'avait mandat pour effectuer une "sélection" quelle qu'elle soit des techniques proposées, mais leur prestige et les compétences techniques qu'ils représentaient étaient suffisants pour que l'étude, l'analyse et l'évaluation retiennent l'attention des différents secteurs industriels et partenaires.

Protection anticopie des transmissions numériques – système DTCP

Issu de la fusion de deux procédés techniques proposés à l'origine au Groupe de discussion sur la transmission numérique du CPTWG, le système DTCP (protection anticopie des transmissions numériques) est conçu pour protéger le contenu au cours de la transmission numérique entre deux appareils grand public. Le système repose sur une combinaison d'un processus d'identification – communication d'appareil à appareil sur interface numérique bidirectionnelle pour vérifier que chaque dispositif est bien un "partenaire" acceptable de la "famille" DTCP – et cryptage du contenu pour le protéger contre l'interception illicite lors de son parcours sur l'interface.

La licence de ce système est gérée par une société à responsabilité limitée constituée par les cinq sociétés ayant mis au point la technique, à savoir Hitachi, Intel, Matsushita, Sony et Toshiba. La licence ressemble en bien des points à la licence CSS, c'est-à-dire que la licence de base autorise l'utilisation de procédés exclusifs de LLC dans l'algorithme, les clés et les autres techniques. Le niveau des redevances et des taxes correspond pour l'essentiel au coût de fonctionnement du système. Enfin la protection de base anticopie prévue par les spécifications impose que le contenu soit protégé de façon sûre pendant tout le processus de transmission.

Le système de licence applicable à cette technique présente cependant deux caractéristiques nouvelles qui ont été très discutées : les règles d'usage applicables aux propriétaires de contenu souhaitant recourir à cette technique pour protéger le contenu qu'ils diffusent; et le dispositif de sécurité qui doit être utilisé pour protéger les éventuelles copies autorisées du contenu protégé au moyen du système DTCP.

En ce qui concerne les règles d'usage, le DTLA a proposé un ensemble de règles visant à permettre au consommateur de continuer à réaliser des copies de certains types d'émissions, par exemple des programmes de télévision gratuits et des programmes par câble. Les propriétaires de contenu qui sont d'éventuels preneurs de licence sur cette technique sont actuellement en négociation avec le DTLA pour résoudre certains points relatifs au nombre de copies qui doit être admis et aux règles qui doivent s'appliquer aux émissions à accès payant ou conditionnel. Le DTLA et les propriétaires de contenu sont d'accord sur le fait que le DTCP peut être utilisé pour empêcher la copie par le consommateur sur un support matériel (tel qu'un DVD vidéo) d'émissions payantes et de films vidéo sur commande. Une décision définitive devrait être prise à brève échéance sur la question des règles d'usage.

Dans la mesure où le système du DTCP autorise un certain nombre de copies, il est reconnu que toute copie autorisée doit être elle-même munie d'une protection anticopie. Dans le cas contraire, il n'y aurait guère d'intérêt à protéger le contenu jusqu'au moment où une copie autorisée est réalisée. C'est pourquoi les règles du DTCP imposent que toute copie

autorisée soit cryptée ou fasse partie d'un "système fermé", de sorte que toute reproduction ultérieure soit limitée par des spécifications supplémentaires de la licence applicables à la lecture de la copie en question.

Même si certains points demeurent en suspens, notamment la question de savoir dans quelle mesure le DTCP peut être utilisé pour empêcher le téléchargement non autorisé du contenu sur l'Internet, il semble vraisemblable que les sociétés concernées aboutiront à un accord. Le système DTCP fait l'objet d'une licence depuis plus d'un mois et a été intégré dans un nombre croissant d'appareils. Il a aussi été accepté en tant que norme UIT (Union internationale des télécommunications) et est actuellement intégré à la norme Open Cable pour les décodeurs. L'adoption définitive de cette technique et des conditions de licence dont elle est assortie aura un effet très positif du point de vue de son utilisation effective sur le marché.

Inclusion d'informations de protection anticopie – Information numérique sécurisée et techniques de "filigrane"

Étant donné que certains contenus peuvent être copiés licitement, il est très important que les informations de protection anticopie des contenus protégés figurent de façon exacte, sécurisée et pratiques à utiliser.

Les propositions initiales prévoyaient l'inclusion d'informations de protection anticopie sous la forme d'"informations accessoires" (c'est-à-dire, d'informations associées à un contenu donné mais n'en faisant pas partie et qui ne sont pas indispensables au visionnage ou à l'audition); ce procédé me garantit pas que les modifications illicites sont impossibles; les informations peuvent donc être inexactes en un point quelconque et sont parfois difficiles à rechercher pour certains appareils. C'est pourquoi cette façon d'inclure les informations de protection anticopie s'est heurtée à une vive opposition, en particulier de la part des sociétés informatiques.

Deux méthodes permettant d'inclure les informations de protection anticopie ont été mises au point pour répondre à ce problème.

Données numériques sécurisées. L'un des éléments de la technique DTCP est que l'information protection anticopie pour tout contenu envoyé au moyen d'une interface protégée en DTCP est transporté en tant qu'élément du système de cryptage lui-même. De la sorte, lorsqu'on essaie de manipuler les informations de protection anticopie, les clés relatives au contenu sont modifiées, si bien que le contenu lui-même ne peut plus être lu par les dispositifs récepteurs. Ce procédé apporte une solution aux trois problèmes à la fois : l'information est protégée contre les attaques de toute personne souhaitant la modifier, l'information est fiable lorsqu'elle arrive (à condition qu'il n'y ait pas eu d'intervention indue) et l'information est facile d'utilisation dans la mesure où elle fait partie du système de sécurité lui-même. Le contenu n'utilisant pas le système DTCP, quant à lui, ne comporte pas cette information de protection anticopie, et l'ordinateur dans ce cas ne recherche pas les informations de protection. Les ordinateurs doivent de toute façon traiter spécifiquement le matériau protégé en DTCP, étant donné la nécessité de le décrypter, et l'information de protection anticopie n'est pas plus onéreuse pour le logiciel que le système de protection lui-même.

Filigrane. La deuxième méthode employée pour inclure des informations de protection anticopie apporte une réponse aux problèmes de sécurité et de fiabilité mais ne peut en elle-même résoudre le problème de la facilité d'utilisation. En effet, les techniques de filigrane font figurer les informations en dissimulant certains codes dans le contenu lui-même. Pour ceux qui savent où chercher ces codes et comment les interpréter, l'information peut être extraite et la réponse adéquate peut être donnée. Toutefois, il est également essentiel que cette information ne perturbe pas la vision ou l'écoute du consommateur. Elle doit donc être invisible, sauf pour un détecteur spécialement conçu à cet effet. Cela signifie que la détection de l'information constitue une charge, puisque l'appareil dans lequel passe le contenu ou qui sert à la vision ou à l'audition doit savoir rechercher le filigrane dans ce contenu. Comme de nombreux dispositifs ne distinguent pas les différents types de contenu, le système ne constitue pas une protection dans les systèmes non équipés.

Jusqu'à présent, nous avons surtout évoqué la protection des contenus vidéo (c'est-à-dire des œuvres audiovisuelles). Nous allons maintenant nous pencher sur la musique enregistrée. Dans ce domaine, il faut signaler deux initiatives importantes : la protection anticopie des DVD audio et le projet SDMI.

Protection anticopie des DVD audio

Alors que les DVD vidéo et les appareils de lecture correspondants se trouvent sur le marché depuis près de trois ans, le support DVD audio n'est pas encore commercialisé. La protection anticopie pour ce support est proposée par le groupe 4C Entity, LLC, société à responsabilité limitée constituée pour proposer et gérer des licences portant sur des techniques de protection anticopie mises au point par quatre sociétés, à savoir IBM, Intel, Matshushita et Toshiba. Au départ, une variante du système CSS destiné aux DVD vidéo avait été proposée comme cryptage de base pour le contenu enregistré sur les DVD audio, mais à la suite du piratage récent de la technique pour les contenus vidéo, cette proposition a été écartée. Il est désormais vraisemblable que le système de cryptage utilisé pour les DVD audio sera fondé sur une technique entièrement nouvelle, ne donnant pas lieu au même piratage ou au même type de piratage que celui qui a été employé pour les DVD vidéo protégés par CSS.

Les règles de protection anticopie seront quelque peu différentes dans le cas des DVD audio. Pour tenir compte du fait que les consommateurs ne manient pas les contenus audio de la même façon que les contenus vidéo, il sera possible de réaliser certaines copies. La nature et le nombre des reproductions autorisées ont fait l'objet d'un débat approfondi entre le groupe 4C et les cinq grandes sociétés d'enregistrement. La solution retenue a été annoncée en février 1999 à l'occasion de la réunion du CPTWG; elle repose sur les principes fondamentaux suivants :

Trois types de sortie seront autorisés à partir des appareils de lecture audio DVD : deux sorties traditionnelles (analogique et IEC 958) et des sorties numériques protégées (qui seront vraisemblablement configurées en sortie IEEE 1395).

En ce qui concerne les sorties traditionnelles, la protection sera assurée par un ensemble de filigranes contenant des informations de protection anticopie et pour les sorties IEC 958, par le système Serial Copy Management (système de gestion de la reproduction en série) imposé aux États-Unis d'Amérique par la loi de 1992 sur l'enregistrement à domicile des produits audio et intégré dans la norme de la Commission électrotechnique internationale observée en Union européenne, au Japon et dans d'autres pays. Dans de telles sorties, le

contenu est livré généralement en temps réel (c'est-à- dire qu'il doit être transporté à la vitesse normale d'écoute).

S'agissant des autres sorties numériques, une protection anticopie sera requise, et la technique DTCP constituera une des formes possibles de protection. Quelle que soit la technique utilisée, celle-ci devra 1) limiter le contenu à une "qualité CD" au maximum ou diminuer les fréquences d'échantillonnage et longueurs en bits du contenu; 2) transporter la totalité des informations de protection anticopie nécessaire pour avoir toute la gamme des options du fournisseur de contenu (voir ci-dessous); et 3) assurer la protection adéquate du contenu à la fois au moment de la transmission et dans la copie autorisée réalisée. L'interface numérique protégée peut transporter le contenu à une vitesse quelconque suivant ses capacités (c'est-à-dire, la vitesse peut être supérieure au temps réel et, par conséquent, le système autorise des capacités d'enregistrement à très grande vitesse).

Lorsqu'il lit un disque non crypté, l'appareil de lecture doit chercher le filigrane pour déterminer si la copie réalisée est une copie illégale. S'il découvre un filigrane qui indique que le contenu était à l'origine crypté au moyen du système 4C, l'appareil de lecture doit refuser de lire le disque.

Les dispositifs d'enregistrement utiliseront un système d'enregistrement sous licence avec un système de cryptage déterminé afin de protéger le contenu figurant sur une copie autorisée. Pour respecter les conditions de la licence, l'appareil d'enregistrement devra :

– lire les informations de protection anticopie et y donner la réponse adéquate, ces informations prenant la forme du filigrane dans l'interface traditionnelle ou d'informations numériques dans l'interface numérique protégée contre la copie. Afin de donner la réponse appropriée, l'enregistreur doit déterminer si le signal d'entrée lui-même correspond à l'original de l'enregistrement ou à une copie du contenu réalisée au moyen du système de protection anticopie (auquel cas l'information de protection anticopie le précisera);

– refuser de réaliser une copie d'un contenu lorsque le signal d'entrée ou l'information d'entrée provient d'une source qui était elle-même une copie;

– refuser de réaliser une copie d'un contenu quelconque reçu au moyen d'une interface numérique munie d'une protection anticopie lorsque l'enregistreur a lui-même déjà réalisé une copie du contenu (autrement dit, il sera possible de réaliser une seule copie par appareil d'enregistrement lorsque le contenu est envoyé par interface numérique avec protection anticopie);

– enfin, dans toutes les circonstances où il est permis de réaliser une copie du contenu à l'entrée, mettre à jour les informations de protection anticopie à la fois sous forme numérique (le cas échéant) et sous forme de filigrane, afin d'indiquer que la copie qui est réalisée est bien une copie et non l'enregistrement original.

En permettant aux consommateurs de réaliser des copies dans les conditions décrites, le groupe 4C veut adapter les restrictions imposée aux attentes normales du consommateur et aux habitudes prises dans d'autres environnements audio. Le groupe reconnaît, tout comme les maisons de disques ayant donné leur avis, que les consommateurs sont habitués à réaliser au moins une copie de confort des enregistrements audio pour leurs déplacements, par exemple, pour disposer d'un exemplaire supplémentaire dans la voiture, pour le baladeur,

pour d'autres pièces de la maison ou d'autres endroits où ils souhaitent écouter de la musique. Tout système qui ne permettrait pas de réaliser ce genre de copies se heurterait à un rejet de la part du consommateur sur le plan commercial et s'exposerait à toutes sortes de procédés de contournement. Plutôt que d'avoir à rencontrer ces problèmes, le groupe, de même que les maisons de disques ayant donné leur avis, ont accepté de permettre ce type de copie de confort mais de recourir à différentes techniques pour empêcher toute reproduction supplémentaire.

De plus, le groupe a compris qu'il fallait rester compatible avec les produits et systèmes existants afin de rendre les appareils intéressants pour les consommateurs. Ainsi, ceux-ci seraient amenés plus rapidement à acquérir des appareils "conformes" assurant la protection anticopie dans le cadre des règles décrites ci-dessus, plutôt qu'à continuer à utiliser des systèmes existants non conformes, qui n'assurent aucune protection.

Projet SDMI (Secure Digital Music Initiative)

Le projet SDMI est l'œuvre de grandes associations professionnelles du secteur de l'enregistrement et de grandes maisons de disques. Il a fait suite à l'arrivée du MP3, qui s'est répandu partout dans le monde en 1998. MP3 est une technique de compression permettant de faire tenir un contenu audio dans des fichiers informatiques suffisamment restreints pour pouvoir être transmis facilement par Internet, ce qui donne aux consommateurs les moyens de devenir leur propre distributeur de musique enregistrée. En l'absence totale de protection, liée soit à l'accès soit à la reproduction, cette technique donnait corps au pire cauchemar des maisons de disques : vendre un unique album, lequel serait ensuite redistribué par des particuliers à toute personne intéressée, de sorte que les maisons de disques ne vendraient jamais aucun autre exemplaire que cet unique album initial.

Les sociétés concernées ont réagi en entamant une action en justice, qui n'a pas été couronnée de succès, contre la diffusion du premier appareil portatif qui permettait aux consommateurs de stocker des fichiers MP3. Alors même que cette action était en cours, les maisons de disques se sont efforcées de faire participer les fabricants d'appareils électroniques et les sociétés informatiques à une action volontaire visant à mettre au point des normes et des techniques permettant de limiter la distribution illicite de musique sur l'Internet, tout en permettant la distribution licite. Les sociétés étaient invitées à adhérer à SDMI pour la somme de 10 000 dollars des États Unis d'Amérique, ce qui leur permettait de participer à l'élaboration des normes et au choix des techniques appropriées. À la fin de 1999, environ 150 sociétés avaient adhéré à SDMI, et beaucoup d'autres envoyaient des représentants à la plupart des réunions.

Alors que l'assemblée plénière, organe regroupant tous les membres de SDMI, est ouverte à toutes les sociétés disposées à payer la cotisation et à signer l'accord relatif aux conditions de participation, l'organisme est administré par la Fondation SDMI, constituée d'un conseil d'administration rassemblant des représentants de sociétés d'enregistrement (pour la plupart, mais pas uniquement, les grandes maisons de disques). Le pouvoir de la fondation est toutefois limité, et ne lui permet pas de passer outre aux décisions prises en assemblée plénière quant à la teneur de la norme ou aux conditions des licences proposées par SDMI.

Le premier souci du groupe était de mettre au point une norme provisoire pour entamer le processus de régulation du transfert dans les appareils portatifs de contenu audio. Pour ce

faire, SDMI a constitué le Groupe de travail sur les appareils portatifs (PDWG) aux fins de formuler une norme initiale d'ici au 30 juin 1999. Le PDWG s'est réuni en moyenne deux fois par mois de février à juillet, et en juillet 1999, il a publié la version 1.0 de sa norme sur les appareils portatifs pour la phase I du projet.

La norme prévoit trois formes de protection. Tout d'abord, elle impose aux systèmes conformes d'être équipés d'outils permettant de détecter trois types de signaux inscrits en filigrane :

– le signal indiquant que la phase I est terminé et qu'une mise à niveau de phase II est nécessaire pour que le système puisse recevoir le contenu marqué pour la phase II. La mise à niveau du système ne sera pas indispensable à condition que le consommateur accepte de ne pas pouvoir recevoir les contenus adaptés à la phase II;

– les informations de protection anticopie indiquant qu'aucune reproduction du contenu marqué n'est autorisée;

– enfin, l'indication selon laquelle le contenu est adapté à la phase II, et ne peut être lu par le système que si celui-ci a fait l'objet d'une mise à niveau phase II.

En deuxième lieu, même si tous les types de contenus (par exemple les fichiers MP3) y compris les copies illégales d'œuvres, peuvent entrer dans un système conforme SDMI au cours de la phase I, certaines protections doivent obligatoirement être maintenues une fois que le contenu a été admis. Le consommateur ayant choisi de stocker le contenu dans un environnement SDMI, toute reproduction doit se faire de façon protégée (cryptée selon un procédé sûr quelconque) et la lecture du contenu ne peut se faire qu'à certaines sorties autorisées, ce qui empêche le consommateur de télécharger l'œuvre sur l'Internet ou de l'envoyer à d'autres appareils au moyen d'une connexion numérique. La troisième forme de protection prévue est un système plus élaboré qui sera mis en place en phase II.

SDMI fonctionne comme un organisme de normalisation industrielle, sur le modèle des procédures utilisées pour élaborer des normes telles que MPEG, sans toutefois suivre complètement les procédures de normalisation habituelles. Les décisions sont prises lorsqu'il existe un consensus suffisant de tous les groupes industriels concernés à l'appui de la décision en question. L'existence d'un tel consensus est déterminée par le directeur exécutif de SDMI, lequel est désigné par la Fondation SDMI.

En général, la norme SDMI est comparable à de nombreuses autres normes utilisées par différents secteurs pour promouvoir le développement de certains produits ou systèmes. La seule partie de la norme SDMI qui suppose une licence technique spécifique est le filigrane. La raison pour laquelle il est préférable de ne disposer que d'une seule technique de filigrane, ce qui implique une licence d'utilisation de la technique correspondant à la norme, est que le fait d'insérer des filigranes multiples dans le contenu conduirait vraisemblablement à une dégradation sensible de la qualité de la musique et que détecter plus d'un filigrane serait trop onéreux pour les appareils. Ainsi, les producteurs de contenus comme les fabricants d'appareils sont fortement incités à se limiter à une seule technique de filigrane utilisée uniformément par les producteurs de contenus et détectée par les appareils de réception. C'est pourquoi le PDWG a été amené à choisir une technique unique de filigrane pour transmettre les informations de protection anticopie pour la phase I et insérer le signal indiquant que la phase I est terminée et que l'appareil doit être mis à niveau phase II pour pouvoir recevoir le

contenu adapté à la phase II. Cette sélection est l'aboutissement d'un appel d'offres d'une évaluation initiale des techniques proposées ainsi que des conditions de licence et de développement et enfin de la mise en œuvre d'essais visant à déterminer quels filigranes étaient les plus facilement et les plus sûrement détectés et quels filigranes avaient le moins d'incidence sur la qualité de l'audition pour le consommateur.

Ce processus s'est avéré nettement plus long que prévu. Malgré tout, après la sélection du filigrane et l'élaboration d'une norme définitive, des produits aux normes SDMI seront présents sur les marchés mondiaux peu après le début de l'an 2000. Les maisons de disques espèrent que les appareils aux normes se multiplieront et élimineront les autres.

Le groupe SDMI est maintenant passée à une action à plus long terme visant à définir une norme pour la phase II (désignant tout ce qui vient après la fin de la phase I). Le projet devrait être mené à bien d'ici à avril 2000, quoique l'expérience du projet sur la phase I laisse penser que la fixation de cette date est peut-être optimiste. L'objectif principal de la phase II est de sélectionner un moyen de déterminer à long terme quel contenu est aux normes SDMI, et ce selon un procédé fiable, sûr et raisonnable à mettre en œuvre. La technique de filigrane utilisée en phase I ne sera pas automatiquement reprise en phase II, bien qu'il semble nécessaire de continuer à appliquer cette technique pendant un certain temps, ne serait-ce qu'en raison du signal indiquant aux consommateurs qu'ils doivent passer à la phase II.

La technique de filigrane utilisée en phase I est une technique exclusive mise au point par une entreprise particulière et fait l'objet de licences accordées par celle-ci, par l'intermédiaire du groupe 4C, LLC jouant le rôle de mandataire. Les paiements liés à cette licence correspondent à la somme des frais d'administration, comme pour les autres systèmes de protection anticopie cités, et des redevances commerciales normales résultant de l'exploitation commerciale d'une technique. La licence elle-même impose certaines restrictions d'usage, essentiellement pour permettre aux consommateurs de continuer à réaliser les copies de confort que nous avons évoquées lors de l'analyse des techniques de protection anticopie des DVD audio. D'un point de vue pratique, cela signifie que la musique préenregistrée destinée à être vendue aux consommateurs ne peut être codée de façon à interdire toute reproduction, et qu'elle doit au contraire être aménagée pour permettre aux consommateurs de réaliser au moins une copie.

Conclusions

Comme le présent document s'est efforcé de le montrer, l'élaboration et la mise en œuvre de mesures techniques de protection anticopie sont complexes. L'innovation en matière de techniques de protection est un processus continu qui suppose un investissement important de recherche et développement. La mise en œuvre des mesures techniques nécessite une coopération entre les secteurs industriels. Les licences relatives aux mesures de protection technique destinées aux titulaires de droits et aux fabricants de matériel sont le fruit de négociations détaillées qui ont permis d'arriver à un consensus sur la protection approprié et les règles d'usage correspondantes. Nous avons montré par la description des structures de protection anticopie existantes que des mesures techniques peuvent être mises en œuvre de façon à répondre aux attentes raisonnables du consommateur et à autoriser à réaliser certaines copies. Loin d'exclure toutes les possibilités d'exception légitime aux droits exclusifs sur l'œuvre, les mesures techniques peuvent même faciliter la mise en pratique de ces exceptions dans des conditions correctes. Le développement de mesures de protection techniques et leur mise en œuvre par des dispositifs de licence commerciale, toutefois, ne répondent que

partiellement au problème de la protection contre la reproduction. Des protections juridiques fortes – par la législation sur le droit d'auteur et les droits voisins ou sur la neutralisation des mesures de protection techniques – sont indispensables.

En l'absence de protection juridique appropriée contre la neutralisation des mesures de protection anticopie, ceux qui respectent la règle du jeu subissent un désavantage concurrentiel. Ainsi, les fabricants de lecteurs DVD qui veulent que leurs appareils puissent être en mesure de lire des disques DVD cryptés au moyen de CSS doivent conclure un contrat de licence pour le décryptage. Comme nous l'avons dit, ce contrat impose des obligations sur la façon dont les dispositifs doivent fonctionner de façon à protéger le contenu une fois décrypté. Or si certains ont le droit de manipuler et de contourner le système CSS, les fabricants pourront produire des appareils sans licence de décryptage CSS et sans se conformer aux obligations de protection anticopie. Si ce type de contournement n'est pas explicitement rendu illégal, les fabricants de matériel ne seront guère incités à prendre la licence au départ et toute l'édifice de la protection anticopie s'effondre. L'importance de législations fortes et efficaces en la matière met en évidence la nécessité pour tous les pays de mettre en œuvre les deux traités de l'OMPI et de prévoir dans leurs législations nationales des dispositions efficaces contre la neutralisation des mesures techniques de protection.

[Les annexes suivent]

ANNEXE A

BRÈVE DESCRIPTION DE QUELQUES TECHNIQUES ET PROCÉDÉS DE PROTECTION

Indicateurs de contrôle de copie : bits numériques insérés juste avant le contenu ou dans celui-ci et indiquant si la reproduction est autorisée. Ces indicateurs peuvent être plus élaborés, définissant le nombre de copies possibles ou la durée du temps de vision, etc. Pour que ces indicateurs soient efficaces, les fabricants de matériel doivent faire en sorte que les appareils recherchent les indicateurs et donnent la réponse appropriée. Les indicateurs peuvent être facilement identifiés par les pirates et ils sont faciles à effacer ou à neutraliser. À ce jour, le secteur de l'informatique (du moins aux États Unis) n'a aucune obligation d'intégrer une recherche d'indicateurs et se refuse à le faire.

SCMS (système de gestion des reproductions en série) : méthode spécifique d'utilisation des indicateurs de contrôle de copie qui permet de réaliser des copies numériques à partir de la matrice, mais non à partir d'une copie de cette matrice. Le système interdit de réaliser des copies de deuxième génération et au-delà. Pour cela, il existe un ensemble d'indicateurs sur la matrice qui sont modifiés par le dispositif de reproduction au cours de la procédure. Si l'on essaye de réaliser une nouvelle copie à partir de la première copie, les indicateurs sont faux et le dispositif de reproduction refuse de considérer l'objet comme une matrice à copier. Le système SCMS est utilisé essentiellement sur les CD musicaux. Les systèmes informatiques n'ont pas l'obligation d'être conformes au système SCMS. De plus, l'expérience montre que les indicateurs de contrôle sont faciles à neutraliser.

Macrovision : signal inclus dans un signal vidéo analogique qui empêche les magnétoscopes d'enregistrer. Le système Macrovision type I perturbe les circuits d'enregistrement des magnétoscopes analogiques. Ce Macrovision type I est compatible avec les signaux vidéos NTSC et PAL. Pour les DVD, les systèmes Macrovision types II et III (salve de synchronisation couleur deux lignes et quatre lignes respectivement) ont été introduits. Ces signaux entraînent des dégradations supplémentaires du signal vidéo. Les systèmes Macrovision types II et III sont compatibles uniquement avec la norme NTSC.

Cryptage : brouillage numérique des bits qui constituent le contenu, de façon à éviter que ce contenu puisse être vu en clair jusqu'à ce que le brouillage soit défait (c'est-à-dire jusqu'au décryptage). Les clés nécessaires au décryptage ne sont accessibles qu'aux utilisateurs autorisés et au matériel autorisé. Cette technique est utilisée très largement pour la radiodiffusion par satellite, y compris par les chaînes à accès conditionnel. Les premiers systèmes reposaient sur une seule méthode de cryptage réitérée, qui lorsqu'elle avait été contournée, ne servait plus à rien. Les systèmes ultérieurs ont employé des clés comportant des procédés de cryptage renouvelables et évolutifs. Des cartes à puce ont été remises aux consommateurs pour vérifier le paiement du service en question. Le cryptage protège le contenu jusqu'à son décryptage (généralement au niveau d'un décodeur); il peut ensuite être copié sur un autre support numérique (par exemple disque informatique) ou analogique (par exemple, cassette vidéo) qui peut être raccordé au décodeur soit directement soit indirectement par l'intermédiaire d'un autre dispositif, par exemple un téléviseur.

Identification : moyen distinctif d'identifier les dispositifs et les classes de dispositifs en vue de faciliter l'authentification et la révocation.

Authentification : procédure consistant à vérifier un dispositif pour déterminer si celui-ci est conforme à une structure ou technique particulière de protection anticopie et est habilité à recevoir un contenu protégé. Si le dispositif est bien conforme, l'authentification permet le transfert de données (contenu) entre le dispositif d'envoi et le dispositif de réception authentifié par un canal sécurisé, généralement par différentes techniques cryptographiques.

Autorisation : droit d'accès donné à un dispositif une fois qu'il a été identifié et authentifié.

Révocation : lorsqu'une manipulation ou un clonage illicite a eu lieu dans un dispositif ou une classe de dispositifs, la révocation numérique interdit tout nouvel accès à ce dispositif dans le respect des normes. Pour cela, il fournit une liste de tous les dispositifs révoqués aux dispositifs en conformité. Les dispositifs en conformité refusent alors d'authentifier et d'autoriser les dispositifs révoqués. La liste est mise à jour électroniquement au moyen de réseaux et de supports matériels à l'intention des dispositifs reconnus; aucune modification matérielle n'est nécessaire.

Filigrane : bits intégrés dans le contenu indétectables à l'œil ou l'oreille, mais qui peuvent être lus par un dispositif de détection qui reçoit ainsi l'information sur l'authenticité et la source du contenu. Cette information peut intégrer des données sur l'auteur, les droits, la distribution, etc. Elle peut aussi comporter des informations et des instructions de contrôle de copie. Un filigrane ne peut être efficace que si les détecteurs aux normes qui lisent et donnent la réponse appropriée sont intégrés aux dispositifs de lecture et d'enregistrement; dans le cas contraire, il n'est pas détecté. L'une des difficultés de la technique est que le filigrane doit résister aux méthodes de compression sans devenir visible ou audible à la décompression.

[L'annexe B suit]

ANNEXE B

DESCRIPTION DE LA TECHNIQUE CSS ET DE SON APPLICATION AUX DVD VIDÉO

La technique CSS elle-même est une combinaison d'un algorithme privé et d'une série de clés associées à l'œuvre individuelle qu'on souhaite protéger, au disque sur lequel l'œuvre est placée, et au fabricant d'un appareil de décryptage. Dans l'application informatique, la relation entre le lecteur de DVD et le système de décryptage de l'ordinateur hôte est gouvernée par un protocole d'authentification et par un cryptage supplémentaire des clés au moment où elles sont reportées du disque sur le module de décryptage du lecteur. L'information de protection anticopie est placée dans les données à des emplacements définis par la configuration du DVD, avant d'être utilisée par le programme de décryptage.

Pour le décryptage, lorsqu'une société de production de films souhaite protéger une œuvre au moyen de ce système, elle demande à l'une des sociétés chargée de préparer le contenu pour le support DVD de crypter l'œuvre. Lorsque la compagnie de production elle-même est intégrée, de sorte qu'un service de cette société s'occupe de la mise en forme du contenu et du cryptage, la société de production elle-même doit prendre une licence, alors que si elle sous-traite le cryptage à un tiers, elle n'a pas besoin de licence. La société de production ou la personne qu'elle désigne peut choisir une clé disque et une clé titre exclusives, en les modifiant aussi souvent ou aussi peu souvent qu'elle le souhaite. La clé titre est utilisée pour crypter le contenu, et la clé disque est utilisée pour crypter la clé titre. MEI conserve le module qui permet de crypter la clé disque. Le propriétaire du contenu ou la personne qu'il désigne envoie la clé disque et la clé titre à MEI, qui est chargé de crypter l'ensemble des clés au moyen du module. Les échanges se font par des moyens sécurisés, et l'information qui en résulte est placée sur le disque dans une zone qui n'est pas normalement accessible à un lecteur non muni d'une licence pour ce système.

S'agissant de l'appareil de lecture, toute société ayant accès à l'information confidentielle ou ultraconfidentielle pour réaliser son appareil doit avoir une licence et doit prendre une licence pour chaque catégorie de spécification CSS. Les sociétés qui fabriquent le produit de décryptage lui-même se voient attribuer des clés correspondant à ce produit. Ce sont les clés utilisées par MEI dans le processus de cryptage de l'ensemble de clés.

[L'annexe C suit]

ANNEXE C

CODES REGIONAUX DESSY STEMES DVD VIDEO

L'arrivée des DVD vidéo était très attendue, mais elle risquait de perturber gravement les systèmes de distribution des sociétés de production de cinéma. La technique DVD est véritablement mondiale, se présentant sur un support immuable quelles que soient les différences locales de normes de télévision, et permettant de visionner facilement des films sur des téléviseurs et des postes informatiques dans la langue de son choix du consommateur. C'est pourquoi un disque DVD contenant un film diffusé en un lieu serait utilisable immédiatement, et de façon conviviale, dans toutes les régions du monde. Les problèmes soulevés par cette possibilité étaient de deux ordres : tout d'abord, les droits de distribution d'un film dans différents pays appartiennent souvent à des sociétés différentes; et en deuxième lieu, les sociétés de production fixent souvent des dates de sortie différentes pour le même film dans différentes régions du monde. Ainsi, un film conçu comme "film d'été" est diffusé dans l'hémisphère nord en juillet, mais sa diffusion dans l'hémisphère sud est différée jusqu'en janvier de l'année suivante. Or au moment où le film aurait été en salle dans l'hémisphère sud, il était vraisemblable qu'il aurait déjà été diffusé sur disque DVD à l'intention des consommateurs de l'hémisphère nord. Les sociétés de production étaient très préoccupées par l'effet de la diffusion dans l'hémisphère sud des disques prévus pour l'hémisphère nord, considérant que les résultats en salle dans l'hémisphère sud seraient compromis par l'afflux de disques DVD que le consommateur pourrait passer à son domicile.

Pour ces deux raisons, la question juridique des droits de distribution et les créneaux de diffusion des sociétés de production, celles-ci tenaient à ce que la technique DVD soit assortie d'un système de codes régionaux, c'est-à-dire qu'un disque diffusé dans une région ne puisse être accepté par des systèmes de lecture utilisés dans d'autres régions. Ce dispositif, là encore, aurait pour but de rendre la fraude difficile, et non de mettre au point un régime parfait empêchant toute personne de lire un disque codé pour une région sur des appareils vendus dans d'autres régions. La situation était encore compliquée par les structures de distribution d'appareils, qui font qu'un fabricant d'un lecteur de DVD pour ordinateur ou d'une unité centrale informatique ne sait pas au moment de la fabrication dans quel pays le lecteur ou l'unité centrale va être vendu. Beaucoup de sociétés informatiques ont des réseaux de distribution mondiaux et expédient leurs produits d'un marché à l'autre en fonction de la demande. Ces sociétés ont estimé qu'elles ne pouvaient pas être obligées de concevoir de façon inaltérable un lecteur ou une unité centrale pour une région donnée au moment de la fabrication. Le système devrait par conséquent être suffisamment souple pour s'adapter à ce problème. Là encore, le CPTWG s'est réuni pendant des semaines pour étudier différents moyens de satisfaire à la fois les producteurs des films et les sociétés informatiques.

Le résultat final a été un compromis qui a ensuite été recommandé en vue de l'élaboration du régime légal imposant la conformité à certaines règles. Ce compromis consistait en ce que les ordinateurs pouvaient être réglés à nouveau par les consommateurs, jusqu'à une limite de 25 fois par le même consommateur. Le dispositif étant un peu complexe à concevoir et à mettre en œuvre, une autre technique a été autorisée pour la première phase des systèmes de lecture informatique des DVD. Au cours de la première phase, les ordinateurs pourront être adaptés à une région donnée par un outil logiciel qui pourra être réglé au moment de l'installation de l'ordinateur par le consommateur, s'adaptant ainsi aux besoins des sociétés informatiques en matière de distribution. Là encore, le CPTWG ne

disposait pas de moyens de faire appliquer ou d'imposer cette façon de procéder. Les règles de restriction régionale ont donc été mises en œuvre dans le cadre de la licence CSS. Les fabricants de matériels prenant une licence pour que leurs appareils soient en mesure de lire les disques DVD cryptés par CSS sont obligés par cette licence d'inclure dans leurs produits des codes régionaux.

[Fin de l'annexe C et du document]