F

OMPI

SCCR/10/2 Rev.
ORIGINAL: anglais
DATE: 4 mai 2004

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
GENÈVE

COMITÉ PERMANENT DU DROIT D'AUTEUR ET DES DROITS CONNEXES

Dixième session
Genève, 3 – 5 novembre 2003

TENDANCES RÉCENTES DANS LE DOMAINE
DE LA GESTION NUMÉRIQUE DES DROITS

Étude établie par M. Jeffrey P. Cunard, Debevoise et Plimpton, Washington

M. Keith Hill, conseiller principal, Rightscom Limited, Londres

et

M. Chris Barlas, conseiller principal, Rightscom Limited, Londres

TABLE DES MATIÈRES

Page

Page

Page

Page

Page

Page

RÉSUMÉ[*]

La présente étude consacrée à la gestion des droits dans l'environnement numérique sous l'angle des techniques sur lesquelles elle repose et des instruments juridiques qui régissent les techniques et les processus correspondants en Australie, aux États-Unis d'Amérique, en Europe et au Japon s'adresse à quiconque s'intéresse à la question, et en particulier aux personnes qui ont une connaissance limitée de la gestion numérique des droits.

Bien que l'étude ait été rédigée par des experts, il convient de souligner d'emblée que la gestion des droits dans l'environnement numérique comporte de nombreux aspects sur lesquels on ne peut encore que spéculer. À ce jour, elle n'est pas encore appliquée de manière généralisée, bien que plusieurs types de contenu et de services offrant du contenu fassent déjà appel à certaines techniques de gestion numérique des droits et de protection du contenu. En outre, plusieurs des lois régissant la mise en œuvre et l'utilisation des techniques de gestion numérique des droits sont récentes et la jurisprudence dans ce domaine est peu développée. Il convient donc de souligner que cette étude doit être considérée un instantané et non comme un jugement définitif qui restera valable à l'avenir. Nous espérons néanmoins qu'elle sera utile à quiconque souhaite prendre connaissance de la situation telle qu'elle est à la mi-2003.

L'étude débute par une introduction, qui contient une description fonctionnelle de haut niveau sur les techniques de gestion numérique des droits, articulée autour des diverses fonctions que l'utilisateur – titulaire de droits ou consommateur de contenu – attend d'un tel système. Cette brève description est suivie d'une histoire succincte de l'Internet et des techniques numériques mises au point pour permettre l'utilisation du contenu numérique, y compris celles qui favorisent l'échange illicite de contenu sur les réseaux. Cette partie débouche sur une rapide évaluation de la situation actuelle des titulaires de droits eu égard au progrès technique.

La dernière partie de l'introduction expose de quelle manière les nouveaux modèles d'exploitation du contenu favorisés par les techniques de gestion numérique des droits viendront compléter les modèles traditionnels. Ces nouveaux modèles sont illustrés par quelques scénarios. Cette partie s'achève sur quelques observations relatives à "l'informatique de confiance", qui devrait avoir une incidence non négligeable sur l'avenir des transactions de contenu numérique sécurisé.

La deuxième partie contient une revue de détail des techniques actuelles en matière de gestion numérique des droits. Dans un souci de simplicité, ces techniques sont présentées comme un ensemble de composants et d'instruments pouvant être intégrés dans un système cohérent. Aux fins de l'étude, une distinction est faite entre "la gestion des droits sur le contenu numérique" et "la gestion numérique des droits". La première a trait aux techniques d'identification, aux métadonnées et aux langages de gestion des droits, alors que la seconde se rapporte aux techniques de cryptage, de tatouage, de signatures numériques et de confidentialité et aux systèmes de paiement.

Cette description des techniques qui composent les systèmes de gestion des droits dans l'environnement numérique est suivie d'une brève section consacrée aux normes et à leur importance pour la mise en œuvre de la gestion numérique des droits.

[*] Les points de vue exprimés dans la présente étude sont ceux des auteurs et ne sont pas nécessairement ceux des États membres ou du Secrétariat de l'OMPI.

La troisième partie de l'étude expose le cadre juridique actuel dans lequel les techniques de gestion des droits sur le contenu numérique sont mises en œuvre. Après un examen du Traité de l'OMPI sur le droit d'auteur et du Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes (ci-après dénommés "traités Internet de l'OMPI"), elle décrit les dispositions relatives aux mesures anticontournement et à l'information sur le régime des droits. Passant à l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (Accord sur les ADPIC), l'étude donne une description de la portée de l'accord, suivie d'une brève explication des travaux de l'Organisation mondiale du commerce dans le domaine du commerce électronique. Vient ensuite une analyse de la situation juridique en Australie, dans l'Union européenne, au Japon et aux États-Unis d'Amérique. En ce qui concerne les États-Unis d'Amérique, l'étude passe en revue le Digital Millennium Copyright Act et les autres instruments législatifs pertinents, y compris les lois fédérales et celles des États, ainsi que les instruments réglementaires correspondants. L'examen de la situation à l'intérieur de l'Union européenne est l'occasion de se pencher sur la Directive sur le droit d'auteur, et de récapituler l'état d'avancement de sa mise en œuvre dans les États membres, ainsi que sur d'autres directives, telles que les directives sur les programmes d'ordinateur et sur l'accès conditionnel. Quelques informations sur les ateliers sectoriels de Commission européenne concernant la gestion numérique des droits sont aussi données. Chacune de ces discussions sur les différentes tendances juridictionnelles est suivie, le cas échéant, d'un examen de la jurisprudence la plus appropriée.

La quatrième partie de l'étude débute par un bref examen des parties prenantes à la gestion numérique des droits, des titulaires de droits aux consommateurs, en passant par les sociétés de gestion collective, les intermédiaires et les vendeurs de technologie. On trouvera ensuite différents exemples de services de gestion numérique des droits pour différents types de contenu actuellement sur le marché. Cette partie s'achève sur un bref examen des questions d'interfonctionnement.

La cinquième et dernière partie passe en revue certaines des questions de politique générale soulevées par l'utilisation des techniques de gestion numérique des droits, notamment celles qui touchent directement la propriété intellectuelle. Les autres questions de politique générale recensées et examinées se rapportent à la confidentialité, à la compétence et à la législation applicable, au rôle du gouvernement en matière d'établissement de normes et, pour finir, aux licences de technologie.

L'étude se clôt sur un examen du rôle des institutions internationales et la présentation de quatre recommandations quant aux mesures qui pourraient être prises à l'avenir.

1. INTRODUCTION

Le présent document décrit les tendances commerciales, techniques et juridiques à l'œuvre dans le domaine de la gestion des droits sur le contenu numérique. Il vise en grande partie à faire mieux connaître les techniques qui ont été mises au point pour la gestion des droits et du contenu sous forme numérique, ainsi que la finalité et l'application de ces techniques dans le monde réel. En même temps, il décrit les différents régimes juridiques instaurés au niveau international et dans plusieurs grands ressorts juridiques pour protéger tant les techniques de gestion numérique des droits que le contenu auquel elles s'appliquent. Enfin, il s'achève sur l'énumération des questions actuelles de politique générale qui peuvent justifier un complément d'étude.

Le présent document n'a pas pour vocation d'expliquer en détail les procédés techniques mis en œuvre, bien que ses auteurs espèrent qu'il aidera les néophytes dans leurs rapports avec les spécialistes. Il ne vise pas non plus à favoriser le choix de telle ou telle solution commerciale, qu'elle soit ou non fondée sur des normes.

Compte tenu du vaste spectre commercial et politique balayé, le présent document ne peut décrire toutes les techniques disponibles sur le marché pour chaque type de contenu, ni l'ensemble des instruments législatifs et de la jurisprudence applicables.

1.1 Description technique de la gestion des droits dans l'environnement numérique

D'un point de vue fonctionnel, la gestion des droits dans l'environnement numérique évoque des choses différentes à de nombreuses personnes. Pour certains, il s'agit simplement du procédé technique permettant de sécuriser un contenu sous forme numérique. Pour d'autres, elle recouvre l'ensemble du processus technique permettant d'échanger des droits et du contenu sur des réseaux tels que l'Internet. Par commodité, la gestion des droits dans l'environnement numérique est souvent scindée en deux secteurs d'activité :

– L'identification et la description des droits de propriété intellectuelle sur des œuvres et des parties concernées dans leur création ou leur administration (gestion des droits sur le contenu numérique);

– L'application (technique) des restrictions d'utilisation (gestion numérique des droits).

La gestion des droits dans l'environnement numérique peut donc désigner les techniques ou les procédés qui sont appliqués au contenu numérique pour le décrire et l'identifier ou pour définir, appliquer et imposer des règles d'utilisation de façon sécurisée.

Il est également important de distinguer entre le "contrôle d'accès", la "protection contre la copie" et la "gestion des droits de propriété intellectuelle", en mettant en évidence leurs lignes de démarcation.

Un système de contrôle d'accès est destiné à gérer l'accès des utilisateurs au contenu et fait généralement appel à une protection par mot de passe. Cependant, dès lors que l'accès au contenu a été accordé, aucune protection supplémentaire n'est mise en œuvre. Ainsi, une fois qu'un utilisateur a accès au contenu, il n'est plus possible de contrôler l'utilisation qui est

faite de ce contenu. Ce type de protection est souvent utilisé sur des sites Web où un simple mécanisme de contrôle d'accès est suffisant.

Un système de protection contre la copie est destiné à indiquer dans quelle mesure la copie, et, le cas échéant, la copie en série, est autorisée, mesure définie par l'"information relative à l'utilisation" qui est associée à toute forme de contenu diffusé, et à déclencher la réaction prévue dans le matériel du consommateur. La notion de protection contre la copie peut être élargie au contrôle des mouvements du contenu à l'intérieur et à l'extérieur du domaine de l'utilisateur, y compris sa redistribution sur l'Internet.

Un système complet de gestion des droits de propriété intellectuelle couvre le traitement de toute l'information sur les droits aux fins de la gestion électronique, y compris parfois des informations à caractère contractuel ou personnel, pour permettre la gestion des droits d'un bout à l'autre de la chaîne de valeur. De par sa nature, la gestion numérique des droits peut nécessiter l'accès à des informations commercialement sensibles (par opposition à l'information sur la copie et à la signalétique relative à l'utilisation). L'utilisation d'un tel système autorise un contrôle très précis du contenu, permettant aux titulaires de droits d'appliquer des modèles d'utilisation très élaborés.

Ce processus de gestion des droits de propriété intellectuelle repose nécessairement sur l'utilisation étendue des techniques de gestion numérique des droits. Ces techniques peuvent être incorporées dans de nombreux éléments, allant de ceux qui résident dans un dispositif simple, tel qu'un agenda numérique ("PDA"), à ceux qui se trouvent dans des serveurs Internet commerciaux exploités par de grandes sociétés ou organisations.

Le présent document vise à présenter l'éventail des instruments qui peuvent être utilisés dans le cadre des systèmes de gestion numérique des droits, à montrer de quelle manière ils sont appliqués et à expliquer les principes juridiques applicables ainsi que les diverses questions de politique générale posées par leur utilisation.

1.2 Origines, fondements conceptuels et objet de la gestion des droits dans l'environnement numérique

1.2.1 La naissance de l'Internet

L'Internet et le World Wide Web tirent leur origine des programmes de recherche informatique mis en œuvre par le Gouvernement des États-Unis d'Amérique au milieu des années 50. L'Advanced Research Projects Agency ("ARPA") a été lancée en 1950 et a réalisé la première expérience de mise en réseau d'ordinateurs en 1965. Par la suite, entre 1967 et 1969, l'ARPA a mis au point ARPANET sur commande du Département de la défense, qui effectuait des recherches sur les réseaux. Un réseau de quatre ordinateurs a été établi et, en 1971, ARPANET a été étendu à 15 serveurs. Cette même année, Ray Tomlinson, de chez BBN, a rendu publique la première application de messagerie électronique, qui permettait d'envoyer et de recevoir des messages sur un réseau distribué. En 1972, le signe @ a été choisi pour l'indication des adresses de courrier électronique et intégré dans l'application de BBN.

En 1972, une démonstration d'ARPANET entre 40 machines a été effectuée lors de la Conférence internationale sur les communications informatiques. Cette même année a eu lieu

la première “conversation” d’ordinateur à ordinateur. En 1974, le BBN a lancé Telenet, service public de données par paquets qui était une version commerciale d’ARPANET.

Pendant les années 80, la technologie de l’Internet s’est développée de manière exponentielle. Au début de la décennie, des réseaux parallèles à ARPANET ont été lancés. Ils comprenaient notamment le Bitnet, le CSNET et, en France, le minitel. En même temps, de nombreux organismes ont adopté le protocole de transmission récemment mis au point, TCP/IP, sur lequel est fondé l’Internet tel que nous le connaissons aujourd’hui. En 1983, l’Université du Wisconsin a commencé à développer la technologie des noms de domaine. L’année 1984 a marqué l’adoption du système des noms de domaine (“DNS”). C’est l’une des autres pierres angulaires de l’Internet actuel. Les premiers noms de domaine ont été attribués en 1985.

En 1987, le nombre d’ordinateurs hôtes reliés à l’Internet a atteint 10 000 et, en 1988, l’Internet Assigned Numbers Authority (“IANA”) a été fondée pour administrer le système des noms de domaine. En 1989, les Réseaux IP européens (“RIPE”) ont été constitués par plusieurs prestataires de services européens, alors que le nombre de serveurs Internet dans le monde entier atteignait 100 000. En 1990, “The World comes on-line (world.std.com)” est devenu le premier fournisseur commercial d’accès commuté à l’Internet.

L’étape la plus importante pour le public a peut-être été franchie avec l’invention du World Wide Web (“Web”) en 1991. Cette technologie a été mise au point par Tim Berners-Lee des laboratoires du CERN à Genève, qui a utilisé des hyperliens pour rendre des documents accessibles par l’Internet. Conçue à l’origine pour les besoins internes du CERN, elle a été proposée peu après aux organismes de normalisation internationaux. Cette évolution a conduit aux normes actuelles du World Wide Web, y compris le HTML et le HTTP, qui sont les piliers du Web que nous connaissons aujourd’hui.

En 1992, le nombre de serveurs Internet a atteint un million et, en 1993, le premier navigateur Web commercial, appelé Mosaic, a vu le jour. Cette étape a été considérée comme un progrès particulièrement important, puisqu’elle a permis aux néophytes d’utiliser cette nouvelle technologie sans formation spéciale. La même année, le taux d’utilisation du Web enregistrait un taux de croissance annuel de 341 634%.

La première émission de radio a été diffusée sur l’Internet en 1994. Quelques années plus tard sont apparus les premiers moteurs de recherche et services de téléphonie sur l’Internet, ainsi que des langages de programmation adaptés à l’Internet, tel JAVA, de Sun Microsystems.

La période allant de 1995 à 2003 a vu une croissance phénoménale de l’Internet. Le nombre de domaines a explosé, de même que le nombre d’internautes. Selon l’Internet Software Consortium, on dénombrait, en juillet 2002, 162 128 493 serveurs Internet dans le DNS, contre 147 344 723 en janvier 2002. Selon OCCL, Alexa Internet et IDC, 4400 sites Web sont créés chaque jour.

1.2.2 Développement de l’Internet pour le commerce électronique

En 1986, la première société proposant un service commercial sur l’Internet était une bourse d’échange de timbres appelée “International Stamp Exchange”. La partie “commerce électronique” de la société philatélique était réalisée sur des télex ou des ordinateurs

individuels. Le terme “commerce électronique” est apparu en 1996. Beaucoup considèrent que le commerce électronique a véritablement démarré en 1998, conduisant à l’utilisation généralisée que nous connaissons aujourd’hui. Selon un rapport récent du bureau d’études Jupiter, la valeur du commerce électronique de détail aux États-Unis d’Amérique devrait augmenter de 28% en 2003, pour atteindre 52 milliards de dollars É.-U. Jupiter estime également que ce chiffre pourrait atteindre 105 milliards de dollars É.-U. en 2007 et représenter environ 5% du commerce de détail aux États-Unis d’Amérique. Les achats en ligne connaissent également une explosion en Europe.

Du point de vue technique, les moyens de cryptage finalement mis à la disposition du public par les gouvernements ont permis de sécuriser les transactions électroniques. Le protocole SSL (“Secure Socket Layer”) mis au point par Netscape Communications a marqué la première étape importante pour la sécurisation et la confidentialité des transactions financières sur l’Internet, grâce aux techniques de cryptage. La norme SSL a été mise en service en 1994 avec la version 1 du protocole. La même année a vu la sortie de la version 2, qui était la première application commerciale du protocole. Une version sensiblement révisée est sortie en 1995 (version 3).

1.2.3 Développement des support de stockage numériques

Les supports de stockage numériques (c’est-à-dire tout support à même de stocker des actifs de propriété intellectuelle sous forme numérique) ont aussi joué un rôle fondamental dans la croissance du commerce électronique de contenu numérique. Les supports de stockage numériques comprennent les disques durs, les supports optiques tels que les disques compacts (“CD”) et les disques numériques universels (“DVD”), ainsi que les cartes à mémoire.

Avec le développement des possibilités de stockage de l’information sous forme numérique, les moyens de stockage mécaniques, tels que les bibliothèques physiques de CD audio ou les collections de photos personnelles, sont de plus en plus remplacés par des supports de stockage numériques. Les ordinateurs individuels, qui offrent une très grande souplesse dans le traitement de l’information, ouvrent de vastes possibilités de créer diverses compilations sur leurs disques durs ou leur graveur de CD-ROM. Si ce phénomène ne pose aucun problème tant que ces compilations contiennent seulement des données personnelles ou les créations du propriétaire, il devient un véritable casse-tête pour les titulaires de droits lorsqu’il s’agit de stocker de grandes quantités d’actifs protégés par la propriété intellectuelle. La situation est encore plus complexe quand l’ordinateur individuel est connecté à l’Internet, parce que ces compilations peuvent alors être mises à la disposition de tout un chacun sur un réseau de partage de fichiers.

1.2.4 Développement des techniques d’extraction (“ripping”)

Le terme anglais “ripping” est généralement employé pour décrire le processus consistant à extraire un contenu numérique (audiovisuel, par exemple) d’un CD ou d’un DVD pour l’enregistrer sur son propre support, tel qu’un disque dur.

Le développement de l’extraction est associé à l’avènement du MP3, format audio compressé (norme Mpeg-1, layer 3) qui permet aux utilisateurs de stocker de la musique de haute qualité comprimée sur un disque dur ou tout autre support numérique. Au départ, les

utilisateurs procédaient à l'extraction des pistes audio de leurs CD pour créer des compilations musicales personnelles sur leur ordinateur. Toutefois, comme il a été indiqué précédemment, avec la mise au point d'applications Web telles que Napster, Kazaa et d'autres, qui permettent de partager ces compilations en ligne, le phénomène a explosé, menaçant de plus en plus les titulaires de droits d'auteur.

L'extraction n'est plus limitée au contenu audio. Il est maintenant relativement facile de copier un film DVD sur un disque dur ou sur les graveurs de DVD apparus récemment. Si le DVD original est muni d'un simple dispositif de contrôle d'accès ou de protection contre la copie, on trouve facilement des instruments permettant de supprimer cette protection afin de copier le contenu du disque sur d'autres supports. Le contenu vidéo peut alors être compressé à l'aide d'un logiciel de compression tel que le DiVX (compression vidéo au format MPEG-4), qui réduit considérablement la taille du film sans perte de qualité excessive.

1.2.5 Partage de fichiers point à point

Comme indiqué ci-dessus, l'existence conjuguée d'ordinateurs individuels puissants, des supports de stockage numériques, des applications de réseau (fondées sur le Web, notamment) et des techniques d'extraction favorise le transfert de contenu des supports originaux sur des supports contrôlés par l'utilisateur. Cela fait, le contenu peut être librement diffusé par l'utilisateur, même s'il est juridiquement protégé par le droit d'auteur.

Le premier réseau de partage de fichiers à attirer un grand nombre d'internautes fut Napster, qui est entré en service en mai 1999. Le service offert par la société consistait à donner aux utilisateurs la possibilité de télécharger un logiciel leur permettant d'échanger gratuitement des fichiers musicaux avec d'autres utilisateurs. Il s'agissait d'un des premiers services point à point, dans le cadre duquel les fichiers musicaux étaient indexés sur les serveurs de Napster, qui dirigeaient les utilisateurs vers les fichiers sources. Napster a été considéré comme le pionnier de ces services point à point.

Napster a tout de suite bénéficié d'une popularité exceptionnelle parmi les utilisateurs. Cependant, peu de temps après son lancement, Napster a été confronté à des problèmes judiciaires lorsqu'il est apparu que ses utilisateurs échangeaient des œuvres protégées sans l'autorisation des titulaires des droits d'auteur. Jamais encore l'industrie musicale n'avait été confrontée à un tel phénomène - une vaste communauté d'utilisateurs échangeant des œuvres sur un réseau de partage fichiers.

Napster a été poursuivi en justice par des compagnies d'enregistrement et des éditeurs de musique pour atteinte indirecte au droit d'auteur. Le tribunal a interdit Napster et cette décision a été confirmée par la Cour d'appel. Napster a fait faillite et ses actifs ont été vendus à la société informatique Roxio.

La cession de Napster n'a pas empêché d'autres sociétés de proposer des services et des logiciels de partage de fichiers. D'autres réseaux point à point ont commencé à apparaître, avec des techniques qui ne faisaient pas appel à un serveur central, ce qui rendait les poursuites judiciaires beaucoup plus complexes. Kazaa, Morpheus et StreamCast fournissent ainsi des logiciels ou des services de partage de fichiers point à point, attirant des millions d'utilisateurs désireux d'échanger du contenu sur une base quotidienne et en quantités énormes. On estime actuellement que plus de 2,6 milliards de fichiers musicaux sont

téléchargés illégalement chaque mois, principalement par l'intermédiaire de services point à point[1]. L'IFPI estime en outre que 99% des fichiers musicaux échangés sur l'Internet sont piratés[2]. L'industrie de l'enregistrement a intenté des poursuites systématiques contre ces fournisseurs de services et de logiciels, bien qu'un juge des États-Unis d'Amérique ait, en avril 2003, statué en faveur de Morpheus et de StreamCast, concluant que, hormis la distribution du logiciel, leur responsabilité indirecte ne pouvait être engagée parce qu'ils n'avaient pas contribué activement et matériellement à l'activité illicite des utilisateurs[3]. Au début de 2003, aux États-Unis d'Amérique, l'industrie a poursuivi des utilisateurs ayant configuré leur ordinateur en mini-serveur ("super node") pour permettre la diffusion de vastes quantités de contenu dans les campus universitaires, avant de conclure rapidement un accord à l'amiable. À la fin du mois de juin 2003, elle a annoncé qu'elle recueillait des informations en vue de l'introduction éventuelle de milliers de poursuites contre des personnes se livrant au partage de fichiers point à point[4].

1.2.6 Situation actuelle des titulaires de droits

La conjugaison d'ordinateurs puissants, des techniques d'extraction du contenu, des supports de stockage de très grande capacité et des systèmes de partage de fichiers a rendu la situation extrêmement délicate pour les titulaires de droits. Tout contenu est à présent exposé à la copie et à sa diffusion illicite sur l'Internet, quel que soit le type de support. Ce phénomène qui a commencé par toucher les CD audio s'est à présent étendu aux films, aux livres et à tous les autres types de contenu pouvant être numérisé. La situation est devenue critique pour beaucoup de compagnies, qui voient leurs recettes chuter en raison de la généralisation du piratage.

C'est pour cette raison que les industries de contenu s'intéressent désormais à la gestion numérique des droits. On trouvera à la section 4 du présent document une description générale de ces techniques, ainsi que des informations sur des initiatives spécifiques soutenues par ces industries, axées sur la gestion des droits dans l'environnement numérique et les aspects juridiques et politiques connexes.

1.2.7 Les perspectives juridiques – traités Internet de l'OMPI et autres instruments

Tout au long des années 90, les titulaires de droits ont consacré une attention croissante aux menaces, ainsi qu'aux opportunités, liées aux techniques numériques décrites ci-dessus. La publication de contenu légitimement accessible par l'Internet et d'autres vecteurs de

---

1 Voir *http://news.bbc.co.uk/1/hi/entertainment/music/2283072.stm*.

2 Voir *http://news.bbc.co.uk/1/hi/entertainment/music/2636235.stm*.

3 Voir *Metro-Goldwyn-Mayer-Studios, Inc.* c. *Grokster, Ltd* , CV 01-08541-SVW (25 avril 2003) (décision faisant droit à la demande d'ordonnance en référé des défendeurs (Grokster et StreamCast) et rejetant la demande de pourvoi en référé des plaignants), appel en instance n° 03-55894 (9th Cir. Interjeté le 29 mai 2003).

3 Voir *Recording Industry To Begin Collecting Evidence And Preparing Lawsuits Against File 'Sharers' Who Illegally Offer Music Online* (communiqué de presse du 25 juin 2003), disponible à l'adresse *http://www.riaa.com/news/newsletter/062503.asp*.

diffusion numériques nécessite la mise en œuvre de mesures de sécurisation et de protection du contenu, notamment au moyen des techniques de gestion numérique des droits. En même temps, l'utilisation généralisée des systèmes de partage de fichiers point à point et des techniques d'extraction, ainsi que la facilité avec laquelle il est possible de copier et de diffuser le contenu sous forme de fichiers numériques, ont considérablement avivé les craintes des titulaires de droits, qui hésitent à autoriser la diffusion de contenu sous forme numérique. C'est pourquoi, tout en examinant les mesures techniques possibles, les titulaires de droits et les distributeurs ont accordé une attention accrue aux mécanismes juridiques susceptibles de protéger le contenu légitime contre sa copie et sa diffusion non autorisées.

La démarche juridique le plus couramment utilisée, qui trouve une illustration dans l'affaire Napster décrite ci-dessus, consistait à invoquer la législation relative au droit d'auteur pour poursuivre les personnes qui facilitaient ces pratiques ou y contribuaient. D'une manière générale, les titulaires de droits avaient décidé de ne pas poursuivre directement les utilisateurs qui se livraient à des activités qui, à l'instar du partage de fichiers point à point, portaient directement atteinte au droit d'auteur. Du reste, en ce qui concerne les particuliers, le statut juridique de certaines de leurs activités, telles que l'extraction du contenu de leurs propres CD, était ambigu, du moins aux États-Unis d'Amérique, où la réalisation d'une copie d'une œuvre achetée légalement pouvait entrer dans le cadre de l'usage loyal. Des actions pour atteinte indirecte pouvaient toutefois être intentées contre Napster et d'autres services de partage de fichiers, et les titulaires de droits – en particulier les compagnies d'enregistrement et l'industrie cinématographique – ont poursuivi systématiquement un nombre sans cesse croissant de fournisseurs de tels services.

À partir du début des années 90, les titulaires de droits, en particulier aux États-Unis d'Amérique, ont commencé à s'intéresser à la technologie, au même titre que le droit, pour protéger leurs œuvres. Tout en réfléchissant sur les moyens techniques à mettre au point et à utiliser pour protéger leur contenu, ils ont également pris conscience du fait que ces moyens seraient inefficaces si la loi n'offrait pas une protection renforcée pour ces procédés et systèmes. Comme indiqué ci-dessous, dans la section 3, la protection juridique des mesures techniques n'était pas sans précédent : divers pays prévoyaient déjà une protection juridique à l'égard des systèmes d'accès conditionnel utilisés dans le cadre des services de câble et autres services de télévision à péage[5]. D'ailleurs, aux États-Unis d'Amérique, la loi de 1992 sur l'enregistrement à domicile interdisait déjà le contournement de tout dispositif, programme ou circuit mettant en œuvre un type particulier de mesure technique – le système de contrôle de la copie en série – qui était utilisé pour protéger les œuvres musicales dans les dispositifs d'enregistrement et d'interface numériques, tels que les magnétophones à bande numériques[6].

En septembre 1995, l'Office des brevets et des marques des États-Unis d'Amérique a publié un rapport intitulé *Intellectual Property and the National Information Infrastructure*, qui exposait ces questions en détail[7]. Rédigé par un groupe de travail sur les droits de

---

5 Les États-Unis d'Amérique interdisent la fabrication et la vente des dispositifs qui sont utilisés principalement pour le décryptage illicite de programmes diffusés par satellite puis par câble (article 605.c)4) du titre 47 du Code des États-Unis d'Amérique. On trouve des dispositions similaires à l'article 1707.a) de l'Accord de libre-échange nord-américain ("ALENA").

6 Article 1002.c) du titre 17 du Code des États-Unis d'Amérique.

7 Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights* (Offices des brevets et des marques : 1995).

propriété intellectuelle, le rapport préconisait que le Congrès adopte un amendement à la loi des États-Unis d'Amérique de 1976 sur le droit d'auteur qui interdirait l'importation, la fabrication ou la distribution d'un dispositif, d'un produit ou d'un composant, ou la prestation d'un service, dont "le but ou l'effet premier consiste à … contourner, sans l'aval du titulaire des droits d'auteur ou de la législation, tout processus, traitement, mécanisme ou système qui empêche ou entrave la violation de l'un quelconque des droits exclusifs du titulaire des droits d'auteur"[8].

Il convient de noter que cette procédure aurait seulement interdit la fourniture d'un produit, et non l'acte de contournement proprement dit. Par ailleurs, l'interdiction s'appliquait seulement aux mesures techniques propres à empêcher l'exercice non autorisé des droits d'auteur, et non aux mesures de contrôle d'accès.

En outre, le groupe de travail recommandait que "l'information sur le régime des droits" soit protégée; toute suppression ou modification délibérée, ou toute diffusion délibérée d'informations modifiées, serait interdite. La définition de l'information sur le "régime des droits" englobait "le nom et toute autre information identifiant l'auteur … [et] le titulaire des droits d'auteur, les conditions d'utilisation…"[9].

Ces dispositions se sont révélées controversées. Bien qu'elles aient été incorporées dans un projet de loi, elles n'ont été promulguées. Néanmoins, le rapport et ces propositions de loi ont constitué le point de départ de la position de négociation et de la proposition sous forme de projet de traité défendues par les États-Unis d'Amérique lors des préparatifs de la Conférence diplomatique sur certaines questions de droit d'auteur et de droits connexes (Conférence diplomatique de 1996 de l'OMPI). Cette conférence diplomatique a abouti à l'adoption du Traité de l'OMPI sur le droit d'auteur ("WCT") et du Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes ("WPPT") (dénommés collectivement "traités de l'OMPI"), qui ont été signés à Genève en décembre 1996. Les WCT et le WPPT, ainsi que leur mise en œuvre, sont examinés à la section 3 ci-après.

1.3 La gestion des droits en tant que moyen de favoriser l'accès au contenu en ligne

La présente section porte sur les incidences du réseau mondial sur les modes traditionnels d'accès à la propriété intellectuelle et, partant, les modes de fonctionnement des "industries du contenu". Il s'ensuivra une étude des moyens par lesquels les techniques de gestion numérique des droits pourraient favoriser de nouveaux modèles d'activité améliorant l'accès d'une manière profitable à la fois aux titulaires de droits et aux utilisateurs.

1.3.1 Modèles traditionnels de distribution commerciale

Les chaînes de distribution traditionnelles créent de la valeur aux points de rareté. Cela vaut autant pour les industries de contenu que pour n'importe quel autre producteur. Les droits de propriété intellectuelle créent un de ces points rareté pour leurs titulaires : les créateurs (ou leurs ayants cause) jouissent, pendant une période limitée, du droit de contrôler l'accès à leur contenu, créant un point de rareté dans la mesure où ce contenu (pour quelque

[8] *Id.* à l'appendice 1, 6.
[9] *Id.* à l'appendice 1, 6-7.

raison que ce soit) ne peut être remplacé par un autre. Si le consommateur veut accéder à un contenu particulier, ce n'est possible que dans la mesure où le titulaire des droits a autorisé la création de points d'accès.

Les atteintes au droit d'auteur sont aussi anciennes que la législation elle-même et l'existence des lois sur le droit d'auteur n'a jamais complètement contrarié les visées de ceux qui entendent profiter de manière illicite des actifs de propriété intellectuelle d'autrui. Le droit d'auteur existe depuis longtemps pour conférer à des titulaires de droits la faculté d'interdire les utilisations non autorisées de leur contenu. Toute seule, la loi ne peut pas et n'a jamais pu empêcher complètement ces utilisations, qu'elles soient à des fins illicites ou légitimes. Il faut pour cela disposer du savoir-faire et des capitaux nécessaires pour créer les supports physiques et accéder à la chaîne d'approvisionnement (ce qui constitue un obstacle important, par exemple au piratage du livre dans les pays où le secteur du livre est bien développé).

1.3.2 Nouveaux modèles de gestion pour la distribution en réseau

Comme indiqué ci-dessus, le développement de l'Internet remet en cause tous les modes de distribution fondés sur la rareté. Bien que les statistiques puissent se prêter à de nombreuses interprétations, on dénombrait vers la fin de 2002 quelque 9 millions de sites sur le World Wide Web. On estime également que plus de 4000 sites sont créés chaque jour. Les réseaux point à point ont rendu le processus de diffusion du contenu encore plus simple, même pour les néophytes. Il est clair que les obstacles à l'entrée dans l'édition (au sens le plus large du terme) et la distribution ont été considérablement abaissés. Les obstacles financiers et ceux liés aux compétences nécessaires pour diffuser du contenu à l'échelle mondiale sont quant à eux tout simplement tombés.

Malheureusement pour les titulaires de droits, ces mécanismes facilitent la tâche non seulement des éditeurs et des utilisateurs légitimes, mais aussi de ceux qui diffusent du contenu, que se soit de manière occasionnelle ou de manière systématique, sans être expressément autorisés à le faire et sans s'inquiéter de savoir si la redistribution est interdite par loi. Par conséquent, alors qu'un volume croissant de contenu devient accessible aux utilisateurs sans aucune taxe, en concurrence directe avec les sources légitimes payantes, les modèles de gestion fondés sur la rareté commencent à être défaillants.

Bien qu'il soit possible d'arguer que l'économie d'effet de réseau valorise l'ubiquité par rapport à la rareté (ce qui, d'un point de vue abstrait, ne fait aucun doute), il peut se révéler très complexe de la chiffrer, c'est-à-dire de la matérialiser dans la chaîne de valeur. Si le contenu est largement disponible gratuitement, cela peut effectivement augmenter la valeur potentielle liée au moment de la création et ainsi au créateur du contenu – mais comment réaliser cette valeur?

Pour être efficace, l'application de la technologie à ce problème doit donc rétablir d'une manière ou d'une autre un point de rareté pour le titulaire des droits. Cependant, cela soulève un paradoxe fondamental, qui n'a pas échappé à ceux qui ont essayé de mettre en œuvre la gestion des droits dans l'environnement numérique, à savoir que le métier d'éditeur (au sens le plus large possible, incluant toutes les entreprises qui mettent toutes sortes de contenu sur toutes sortes de supports à la disposition du public) consiste à faciliter l'accès et non à l'interdire.

L'objectif ultime de la mise en œuvre de "mesures techniques" pour contrôler la diffusion de la propriété intellectuelle doit concilier le souhait des titulaires de droits de contrôler et de protéger la diffusion de leur contenu et l'intérêt des consommateurs, qui est d'avoir accès à ce contenu. Naturellement, les consommateurs préféreraient avoir accès au contenu pour rien – pourquoi payer quelque chose qu'on peut obtenir gratuitement? Bien entendu, il faut aussi persuader les consommateurs de la "valeur" objective d'actifs intangibles, ce qui ne va pas de soi. Néanmoins, à moins d'abandonner complètement le droit d'auteur comme mécanisme de commerce d'actifs de propriété intellectuelle, il faudra absolument trouver une solution à ce paradoxe.

1.3.3 Quelques scénarios de gestion numérique des droits

Pour assurer l'efficacité de la gestion des droits dans l'environnement numérique et surmonter le paradoxe ubiquité/rareté, quels types d'applications susceptibles d'attirer les consommateurs faut-il mettre en œuvre? Voici quelques scénarios potentiels :

– Une consommatrice télécharge depuis chez elle de la musique sur un service de réseau et obtient l'autorisation d'écouter ces morceaux musique (aussi souvent qu'elle souhaite) sur n'importe quel dispositif en sa possession pendant une période de 12 mois à compter de la date du téléchargement; elle peut également transmettre une copie de ces morceaux à 10 de ses amis au maximum sans frais, mais ceux-ci ne pourront les écouter qu'une seule fois dès lors qu'ils n'achètent pas leur propre licence. Toutefois, pour la récompenser en tant que distributeur des fichiers protégés, elle obtiendra une contrepartie, financière ou en nature, du titulaire des droits qui bénéficie de la diffusion du contenu auprès de ses amis.

– Une consommatrice télécharge un film récent. Elle est autorisée à regarder ce film trois fois seulement pendant un délai d'un mois. Après ce délai, le fichier devient inaccessible à moins qu'une nouvelle redevance soit payée. Toutefois, la licence lui donne également droit à une séance gratuite dans son cinéma local le mois qui suit l'expiration de l'autorisation.

– Un étudiant "visite" depuis chez lui sa bibliothèque universitaire, qui se trouve à l'extérieur du campus, et trouve les cinq articles de presse et chapitres des livres dont il a besoin pour rédiger son devoir. Il les télécharge sur son ordinateur portable. Ces fichiers ne sont disponibles qu'en prêt "à court terme", de sorte qu'après cinq jours, les fichiers téléchargés sur son ordinateur portable deviennent inaccessibles. Toutefois, la bibliothèque a également un accord avec un vendeur de livres électroniques, qui offre des rabais sur un éventail de livres électroniques en rapport avec les articles de presse. Cette procédure met en œuvre des correspondances de métadonnées complexes dans le cadre du système de gestion numérique des droits.

1.3.4 L'avenir de la gestion numérique des droits : l'informatique de confiance

Aujourd'hui, la gestion numérique des droits est encore une industrie naissante. Si les différentes techniques nécessaires pour mettre en œuvre la protection des droits et du contenu sous une forme numérique sont de plus en plus sophistiquées (ainsi qu'il sera démontré plus tard dans le présent document), elles ne sont toujours pas largement adoptées. Cette question est liée en partie à la méfiance des titulaires de droits et en partie à la résistance des

consommateurs. Elle est également liée très étroitement à la grande quantité de contenu disponible gratuitement, mais illégalement, sur l'Internet.

Si ce problème est actuellement traité par une combinaison de poursuite judiciaires contre les pirates et de l'offre de services de contenu à valeur ajoutée tels que ceux qui sont décrits ci-dessus, des mesures plus radicales, faisant appel à certaines des techniques déjà mises au point, seront nécessaires à l'avenir. C'est ce qui explique le développement de systèmes connus sous le nom générique d'informatique "de confiance" ou "sécurisée".

L'informatique de confiance repose essentiellement sur la mise au point de dispositifs faisant appel à des microprocesseurs (tels que PC, PDA, téléphones mobiles, téléviseurs, chaînes hi-fi ou tout autre dispositif de restitution commandé par microprocesseur) qui comprennent à la fois le matériel et le logiciel nécessaires à la protection du contenu. Et le contenu désigne ici n'importe quel type d'élément restitué par le dispositif, qu'il s'agisse d'actifs protégés par des droits de propriété intellectuelle ou de contenu non protégé que les fournisseurs souhaitent néanmoins voir consulté et utilisé selon des conditions prédéfinies.

Plusieurs initiatives, certaines fondées sur des normes (par exemple, la Trusted Computing Platform Alliance), d'autres exclusives (par exemple, la Next-Generation Secure Computing Base de Microsoft) sont en cours. Elles visent à créer un environnement de réseau protégé, fondé sur l'identification sécurisée des utilisateurs, des dispositifs et modules logiciels pour s'assurer que le contenu ne pourra être exploité que dans le respect des règles fixées par les propriétaires du matériel. Si ces initiatives soulèvent un grand nombre de questions, concernant notamment le respect de la vie privée de l'utilisateur, la combinaison de mesures de sécurité logicielles et matérielles est généralement considérée comme le meilleur moyen d'assurer un environnement sûr et protégé. Dans un tel environnement, la distinction entre les méthodes de traitement du contenu protégé par le droit d'auteur et du contenu régi par d'autres formes de protection juridique (telles que la législation relative au secret commercial ou à la protection des données) disparaîtra en grande partie. Toutefois, cette technologie est une perspective encore lointaine (certains doutent même qu'elle parvienne jamais à s'imposer). Pour le moment, il convient donc de se concentrer sur les techniques qui visent à assurer uniquement la protection des droits de propriété intellectuelle.

2. DESCRIPTION DES TECHNIQUES ACTUELLES DE GESTION NUMÉRIQUE DES DROITS

2.1 Introduction

Cette section décrit, en termes généraux, les techniques qui peuvent être combinées pour mettre en œuvre les fonctions nécessaires aux fins de la gestion numérique des droits. Si toutes les techniques décrites ici ont des applications commerciales, l'étude qui en est faite repose sur la conviction que toute technologie protégée par la propriété industrielle est en réalité une réponse à un besoin technique. Ces besoins peuvent être exprimées en termes de fonctions. Cette étude s'apparente donc à une analyse des besoins, mais elle est fondée sur l'hypothèse que les techniques disponibles dans le commerce répondent déjà aux besoins recensés.

2.2 La gestion numérique des droits en tant qu'ensemble d'instruments et de composants

On pense souvent que la gestion numérique des droits est mise en œuvre par un logiciel unique, qu'il suffit d'installer pour protéger le contenu en ligne. En fait, la gestion numérique des droits fait appel à une grande variété de techniques et de services, dont certains peuvent résider sur le dispositif de l'utilisateur, d'autres sur le serveur de réseau d'un vendeur et d'autres enfin sur le réseau lui-même.

D'une manière générale, ces techniques peuvent être classées comme suit :

– Techniques d'identification;
– Techniques reposant sur les métadonnées;
– Techniques relatives aux langages de gestion des droits;
– Techniques de cryptage;
– Techniques d'association rémanente;
– Techniques de confidentialité;
– Techniques de paiement.

Ces dernières années, de nombreuses études et activités ont été lancées sur la façon de combiner ces divers composants afin d'assurer un environnement sécurisé pour le contenu protégé. Ces activités sont le fait de sociétés informatiques privées, d'organismes de normalisation et des milieux universitaires. Le consensus qui a émergé est que l'avenir de la gestion des droits dans l'environnement numérique réside dans une hybridation des services commerciaux, de composants logiciels et d'éléments normalisés. L'objectif est d'instaurer un marché concurrentiel pour ces techniques, tout en veillant à ce que le consommateur ait la faculté d'accéder au contenu par l'intermédiaire des systèmes de gestion numérique des droits sans se heurter à des obstacles techniques tels que des incompatibilités entre les systèmes. Alors que de nouvelles solutions continuent d'apparaître et que l'interfonctionnement (voir ci-dessous) demeure un sujet de vif débat, les perspectives d'avenir se précisent de plus en plus.

2.3 Gestion des droits sur le contenu numérique

L'élément infrastructurel d'un système intégré pour la gestion de l'accès à la propriété intellectuelle dans l'environnement de réseau passe par l'élaboration de normes infrastructurelles imbriquées pour l'identification et la description formelles des actifs de propriété intellectuelle, y compris les droits et les autorisations qui s'y rattachent.

L'étude la plus détaillée sur les critères d'identification et de description pour les échanges d'actifs de propriété intellectuelle sur le réseau est sans doute celle entreprise dans le cadre du projet <indecs>[10]. Dans le cadre de ce projet, un modèle générique de commerce très simple a été mis au point et la nécessité absolue d'identifier chacun des éléments essentiels du modèle, à savoir le "contenu" proprement dit, les transactions sur ce contenu et les parties à ces arrangements (particuliers ou organismes) a été mise en évidence.

[10] Voir *www.indecs.org*. Les parties prenantes au projet, qui était financé par la Commission européenne dans le cadre du programme Info2000, représentaient un large éventail d'organismes intéressés par la gestion des droits de propriété intellectuelle.

Les participants du projet <indecs> ont considéré qu'un système d'identification et de description unique, monolithique et global couvrant tout le spectre de la propriété intellectuelle serait une ambition irréalisable et qu'il convenait plutôt de mettre au point des mécanismes pour faciliter l'interfonctionnement entre les solutions locales et sectorielles. La clé de l'interfonctionnement réside dans la conception des systèmes d'identification et de description eux-mêmes, qui doivent adhérer à certains principes logiques pour participer à une solution globale de gestion de la propriété intellectuelle.

2.3.1 Les fondements de l'identification

Par "identification" on entend l'attribution d'une étiquette à un élément afin qu'il puisse être formellement identifié par un tiers. L'identification formelle est un élément central dans tout processus commercial automatisé; c'est d'autant plus vrai des processus qui impliquent des communications au-delà des frontières de l'organisation, lorsque les identificateurs "locaux" ont peu de chances d'être reconnus par les autres parties prenantes à la chaîne d'approvisionnement.

En l'absence d'un cadre d'identification monolithique, ces identificateurs ne peuvent être réellement uniques que s'ils s'inscrivent dans un système de nommage déterminé, généralement désigné sous l'expression "espace de nom".

Les identificateurs uniques sont généralement, mais pas toujours, des nombres. L'exemple ci-après, tiré du système appliqué par une industrie de contenu, est aisément reconnaissable :

ISBN 0 85021 294 4.

Ici, les lettres "ISBN" identifient l'espace de nom. Cet identificateur s'inscrit dans l'espace de nom du numéro international normalisé des livres; si cet espace de nom est correctement administré (ce qui est le cas de l'ISBN), la combinaison de l'espace de nom et de l'identificateur doit permettre d'identifier un élément de manière unique. En l'occurrence, il s'agit d'un produit qu'un éditeur souhaite vendre.

Dans un système bien organisé de commerce d'actifs de propriété intellectuelle, les identificateurs de produits (parfois désignés sous le nom d'identificateurs d'articles du commerce) ne sont pas suffisants. Des systèmes d'identification sont nécessaires pour assurer l'identification formelle d'un certain nombre d'autres aspects de propriété intellectuelle, comme en témoigne la description de la "famille" croissante des identificateurs normalisés mis au point pour la gestion des œuvres musicales. Le tableau suivant décrit les normes d'identification déjà appliquées (ou en passe de l'être). À cet égard, l'industrie musicale est considérablement mieux développée que d'autres secteurs; on peut supposer que la gestion collective des droits de reproduction mécanique et d'autres droits, ainsi que la nécessité d'établir des communications entre des sociétés de perception établies dans différents territoires, ont considérablement accéléré les choses.

Nom et sigle de l'identificateur	Statut de l'identificateur	Objet de l'identification
International Standard Musical Work Code (ISWC)	Norme internationale ISO 15707	L'ISWC identifie les œuvres musicales – c'est-à-dire, l'"abstraction" fondamentale d'un morceau de musique. Par exemple, la "cinquième de Beethoven" est une notion qui existe et doit être identifiée indépendamment de telle ou telle exécution, de tel ou tel enregistrement ou de telle ou telle partition (mais qui relie tous ces éléments entre eux). L'ISWC joue un rôle central dans la gestion des droits sur les œuvres musicales.
International Standard Recording Code (ISRC)	Norme internationale ISO 3901	L'ISRC identifie l'enregistrement spécifique d'une œuvre musicale, indépendamment de la forme sous laquelle il est fixé (sur un CD, par exemple, ou dans un fichier en ligne). Il identifie l'"exécution" enregistrée d'une œuvre musicale. Il n'identifie pas le support de fixation particulier.
International Standard Music Code (ISMN)	Norme internationale ISO 10957	Cet identificateur (étroitement lié au code ISBN mais géré de manière indépendante) est utilisé pour identifier des partitions musicales dans la chaîne d'approvisionnement.
Numérotation européenne des articles /Universal Product Code (NEA/UPC)	Norme de fait utilisée dans le monde entier	Ces identificateurs sont ceux qui sont le plus souvent utilisés pour identifier des articles du commerce (CD ou cassettes audio) dans la chaîne de distribution physique. Ils sont souvent, mais pas nécessairement, apposés sur le produit sous forme de code à barres.
Global Release Identifier (GRID)	Norme commerciale en cours d'élaboration	Cet identificateur a été mis au point par l'industrie de l'enregistrement pour identifier les œuvres musicales sous forme électronique; il a été décrit comme l'équivalent numérique du code à barres NEA, c'est-à-dire un identificateur d'articles marchands sous forme numérique.
Interested Party Number (IPN)	Norme commerciale appliquée collectivement par les sociétés de gestion des droits d'auteurs d'œuvres musicales	Cet identificateur est le successeur récent du code "CAE" (Compositeur, Auteur, Éditeur). Ces deux systèmes de numérotation ont été mis au point – et sont exclusivement utilisés – par les sociétés de gestion des droits d'auteurs d'œuvres musicales aux fins de l'administration collective des droits de leurs membres.

Nom et sigle de l'identificateur	Statut de l'identificateur	Objet de l'identification
International Performers Database Number (IPDN)	Norme commerciale appliquée par les sociétés de gestion des droits des artistes interprètes ou exécutants	Cet identificateur, mis au point en marge du code IPN par un consortium des sociétés de gestion des droits des artistes interprètes ou exécutants, est utilisé pour l'administration collective des droits des artistes concernés.

Identificateurs de l'industrie musicale

La musique a été choisie comme exemple parce qu'elle illustre bien la complexité de l'identification, même dans une architecture relativement bien développée. D'autres secteurs adoptent à présent des perspectives similaires. L'industrie du livre, par exemple, travaille à l'élaboration d'une norme d'identification des œuvres écrites (l'International Standard Textual Work Code - ISTC - qui devrait devenir une norme internationale dans le courant de 2003).

L'un des aspects les plus marquants du système d'identification dans le domaine musical concerne sans doute la prise de conscience de la nécessité d'identifier les parties. L'identification formelle des titulaires de droits est essentielle pour l'exactitude et l'efficacité de la répartition des redevances collectées en leur nom. Or, ces identificateurs n'ont pas encore été mis en œuvre dans tous les secteurs de l'industrie musicale; les maisons de disques, par exemple, n'identifient pas toujours leurs artistes de manière uniforme dans leurs propres systèmes internes. La plupart des autres secteurs de l'industrie du contenu ne disposent pas de mécanismes efficaces pour l'identification formelle des parties[11].

À la nécessité d'identification des titulaires de droits correspond une nécessité similaire d'identifier les utilisateurs de ces droits. Cette question devient particulièrement sensible lorsqu'il s'agit d'identifier personnellement les consommateurs. L'identification individuelle et les menaces qu'elle fait peser sur le respect de la vie privée comportent bien entendu un risque potentiel. On y reviendra dans la section 5.2.1).

2.3.2 Identificateurs de réseau

La plupart des identificateurs dont il est question ici sont antérieurs à la création de l'Internet et peuvent sembler peu pertinents dans le monde de communication en réseau d'aujourd'hui. Le localisateur universel de ressources ("URL") a l'avantage non négligeable de pouvoir être converti dans l'environnement de réseau : le fait de "cliquer" sur un URL déclenche une action prévisible, à savoir que votre navigateur est dirigé vers une ressource déterminée du World Wide Web.

---

[11] Dans ce contexte, l'utilisation d'autorités chargée des noms par les bibliothèques doit être soulignée. Le projet InterParty (voir *www.interparty.org*) recherche actuellement des mécanismes susceptibles de faciliter l'interfonctionnement des "identificateurs de personnes" entre différents secteurs.

Une action prévisible peut-être, mais un résultat qui ne l'est pas forcément. Le résultat de la "conversion" d'un URL en adresse est souvent insatisfaisant, soit qu'il n'y ait plus rien, soit que le contenu ait changé. L'URL n'est après tout que ce qui il est censé être, c'est-à-dire l'identificateur d'un lieu et non du contenu qui s'y trouve. À cet égard, on peut le comparer aux panneaux figurant sur les rayonnages des bibliothèques : ils vous conduisent à un endroit spécifique où vous trouverez ou non ce que vous cherchez.

Les acteurs du réseau, représentés par leurs deux organismes de normalisation (le World Wide Web Consortium ("W3C"), et l'Internet Engineering Task Force ("IETF")), se heurtent à ces questions depuis une décennie. Le cadre conceptuel de l'identification rémanente sur le réseau – le nom universel de ressource ("URN") - est en place depuis plusieurs années. Cependant, la conversion des URN (et donc leur utilité) s'est révélée plus difficile à mettre en œuvre.

L'industrie de l'édition, principalement sous l'impulsion des éditeurs de revues scientifiques, dont les publications étaient rapidement mises en ligne, a pris conscience de la nécessité de disposer d'identificateurs rémanents convertibles du contenu sur le réseau et a créé en 1998 l'International DOI Foundation, chargée d'élaborer et de mettre en œuvre l'identificateur d'objet numérique ("DOI"), un identificateur de réseau convertible qui fait appel à la technique de "conversion" Handle mise au point par la Corporation for National Research Initiatives (CNRI). Selon la CNRI, il s'agissait de la première mise en œuvre de l'URN.

L'un des avantages potentiels du DOI sur d'autres solutions réside dans la capacité de "résolutions multiples" du système Handle – en d'autres termes, l'"action" initiée par un DOI peut être différente selon le contexte dans lequel il est employé. Cependant, les incidences réelles de ces possibilités commencent seulement à être comprises et démontrées. En attendant, des applications plus générales de l'URN sont proposées, et des noms de domaine URN "de premier niveau" sont attribués à des systèmes d'identification existants, l'idée étant qu'un identificateur tel que "URN:ISBN:0850212944" devrait devenir convertible sur le réseau.

Cependant, une telle fonction en mode "natif" n'existe pas encore sur le réseau.

2.3.3 Gestion des identificateurs

Le vrai défi concernant les systèmes d'identification réside dans la manière dont ils sont administrés. Comme l'a souligné Tim Berners-Lee, le "père du World Wide Web", la difficulté que présente l'utilisation de l'URL comme identificateur rémanent est d'ordre plus social que technique. Même des identificateurs bien établis comme l'ISBN sont détournés par des utilisateurs qui les appliquent à des articles "hors-sujet" (l'exemple le plus connu concerne l'application du code ISBN à des jouets en peluche qui se trouvent être distribués par l'intermédiaire de la filière de distribution du secteur du livre).

Si la clarté des directives d'utilisation est essentielle, il y a en définitive peu de moyens de s'assurer que les utilisateurs appliqueront réellement les identificateurs de la manière prévue (voire de s'assurer qu'ils les appliqueront tout court!). L'une des solutions de plus en plus adoptée consiste à faire en sorte que les identificateurs ne puissent être appliqués qu'à des objets susceptibles d'être décrits dans le cadre des structures minimales de métadonnées associées à l'identificateur en question.

En fin de compte, la gestion des identificateurs est affaire de consentement : les utilisateurs doivent considérer qu'il est dans leur intérêt de "respecter les règles du jeu". Ce problème n'est pas trop grave tant qu'il s'agit d'identificateurs dont le coût d'application est relativement faible. Cependant, les difficultés sont beaucoup plus importantes lorsque le coût de jonction du système d'identification est relativement élevé (comme dans le cas des identificateurs d'objets numériques). Dans ce cas, les organisations peuvent se méfier de systèmes de gestion qu'il leur semble difficile d'influencer directement.

2.3.4 Récapitulatif des questions liées à l'identification

La mise en place d'une infrastructure d'identification formelle pour la gestion des droits sur le contenu numérique sera complexe et difficile. Les industries de contenu ne sont pas (encore?) uniformément convaincues de sa nécessité. Toutefois, le secteur où l'infrastructure de gestion des droits est la plus développée (celui de la musique) a pris conscience des enjeux dans ce domaine.

Cela étant, les identificateurs ont peu de valeur en eux-mêmes. Ils favorisent simplement la liaison entre les systèmes en s'assurant que tous parlent de "la même chose". C'est la capacité d'utiliser un identificateur pour relier des informations sur "la même chose" dans différents systèmes informatiques qui confère de la valeur à l'identificateur.

2.3.5 Métadonnées

Le terme "métadonnées" est employé dans de nombreux sens. Il illustre parfaitement le problème de l'ambiguïté sémantique qui sera examiné en plus détail dans la présente section. Il est donc important de définir ce terme tel qu'il est utilisé dans le présent rapport : on entend par "métadonnées" l'information qui décrit le "contenu" (c'est-à-dire les "données"). Cette définition légèrement excentrique est celle qui est généralement admise dans les industries de contenu.

La notion de "description" est, bien entendu, très large. Dans le projet <indecs>, les métadonnées étaient définies en termes d'expression de relations, ce qui peut être utile pour prendre en considération toutes les façons potentielles de décrire une chose (voire une personne).

Le présent document traite avant tout des métadonnées expressément associées aux identificateurs, puisque ce sont celles qui trouvent l'application la plus directe dans la "gestion des droits sur le contenu numérique". Les normes relatives aux métadonnées sont beaucoup moins développées que les normes relatives aux identificateurs, parce que l'importance de l'interfonctionnement des métadonnées commence seulement à être comprise.

Il convient de noter dans ce contexte qu'une énorme quantité de métadonnées est traditionnellement compilée et recompilée à de nombreux points de la chaîne de diffusion de l'information. Concrètement, la "même" information est enregistrée par de nombreuses personnes. Le manque d'efficacité des pratiques de collecte et de traitement des données – en termes de coût et de qualité – a conduit à l'élaboration de normes relatives au partage des données (et, par conséquent, du travail).

2.3.6 Identificateurs et métadonnées minimales

L'importance du lien entre les systèmes d'identification et les métadonnées est devenue de plus en plus évidente pour les organismes chargés de l'élaboration des normes relatives aux identificateurs. ISO TC46/SC 9, le comité de l'ISO chargé des normes d'identification et de description dans le domaine de l'information et de la documentation (qui est chargé de toutes les normes ISO relatives aux identificateurs mentionnées dans le présent document) a décidé qu'aucune nouvelle norme relative aux identificateurs ne serait publiée sans un minimum de spécifications en matière de métadonnées.

Par exemple, la révision actuelle de la norme ISBN prévoit une série minimale de métadonnées à intégrer à l'ISBN.

Ces "séries minimales de métadonnées" ont pour objectif premier de lever les ambiguïtés – les données doivent être suffisantes pour permettre la distinction entre deux éléments différents mais superficiellement semblables (en d'autres termes, pour distinguer des entités qui partagent certains attributs, mais pas la totalité d'entre eux).

En ce qui concerne le secteur de l'édition du livre, des mesures sont prises afin de s'assurer que les normes ISO applicables aux métadonnées d'identificateurs sont conformes à la norme commerciale ONIX. Il s'agit d'assurer l'interfonctionnement transparent de différentes séries de métadonnées dans le même secteur.

2.3.7 Interfonctionnement des métadonnées

Même si un secteur, comme celui de l'édition du livre, parvient à définir des normes commerciales qui sont largement appliquées dans ce secteur, il est fort peu probable que ces normes puissent traverser les frontières sectorielles, territoriales et linguistiques historiquement établies.

Avec la mondialisation, et le caractère inéluctable de la convergence des supports découlant du fait que tous les types de contenu sont distribués sur une filière de réseau commune, l'interfonctionnement à travers ces frontières devient essentiel.

Comme indiqué ci-dessus (voir la section 2.3), le projet <indecs> définissait les conditions applicables à l'interfonctionnement des métadonnées. L'une des conditions essentielles est que la terminologie relative aux métadonnées doit être *bien conçue,* ce qui signifie avant tout qu'elle doit être *correctement et clairement définie*. Une grande partie des efforts déployés pour résoudre le problème de l'interfonctionnement a traditionnellement porté sur la syntaxe. Or, la véritable difficulté réside peut-être dans la *sémantique*.

2.3.8 Sémantique

Cette nécessité d'une sémantique bien définie accroît sensiblement l'importance de dictionnaires correctement structurés – des dictionnaires qui définissent les termes utilisés dans une série de métadonnées selon un modèle de données correctement structuré (essentiellement, une "vue" des relations entre les différentes entités de la série de métadonnées). On trouvera davantage d'informations sur cette question ci-dessous.

2.3.9 Langages et dictionnaires d'expression des droits

2.3.9.1 Fonctions requises

Une fois que le contenu a été identifié et décrit, les titulaires de droits souhaiteront établir les règles relatives à la consultation de ce contenu par les utilisateurs. Ces règles leur permettront de créer des modèles de gestion, connus ou nouveaux, dont quelques exemples ont été décrits dans la section 1.3. Les règles de cette nature doivent répondre à un certain nombre de critères. Elles doivent être :

– pleinement expressives – c'est-à-dire qu'elles doivent permettre aux titulaires de droits et à leurs mandataires d'exprimer leurs droits et leurs intérêts sur le contenu, ainsi que les accords contractuels y relatifs, selon divers modèles d'utilisation et de gestion;

– non ambiguës – c'est-à-dire qu'elles doivent être absolument précises, afin qu'elles ne puissent être interprétées d'aucune autre manière que celle voulue par le titulaire des droits;

– déchiffrables par machine – c'est-à-dire que les licences doivent être déchiffrables par des ordinateurs et d'autres dispositifs à microprocesseur;

– sécurisés – c'est-à-dire qu'elles doivent permettre de détecter toute altération.

Il ne s'agit là que d'une liste minimale des conditions applicables à un langage d'expression des droits. Ce langage est la clé de la gestion numérique des droits, parce qu'il permet de prendre en charge les modèles de gestion actuels et d'en créer de nouveaux.

2.3.9.2 Description technique des langages d'expression des droits

La façon la plus simple de faire comprendre le fonctionnement de l'expression des droits consiste sans doute à l'expliquer en termes de langage susceptible de donner des instructions à un ordinateur. Dans ce cas, les instructions concernent ce qu'un utilisateur peut faire avec un contenu. Le titulaire des droits convertit son autorisation humaine (*Vous pouvez copier ce fichier sur votre disque dur et l'exécuter dix fois*) en langage logique pouvant être interprété par programme d'ordinateur. Le programme d'ordinateur en question est le système de cryptage qui protège le contenu auquel l'utilisateur souhaite accéder.

La technologie du langage d'expression des droits a été élaborée au début des années 90 au Xerox Parc Research Center, à Palo Alto (Californie). Depuis lors, elle n'a cessé d'être perfectionnée. Elle est essentiellement fondée sur la notion d'autorisation accordée à un utilisateur pour accomplir un acte déterminé à l'égard d'un contenu protégé par des droits de propriété intellectuelle. Par exemple, si un titulaire de droits souhaitait accorder à un utilisateur le droit de copier un certain contenu, afin de l'exécuter à partir du disque dur de son ordinateur, il serait possible d'accorder ce droit sous certaines conditions. Le titulaire des droits pourrait souhaiter interdire la transmission du contenu à un tiers (c'est-à-dire, interdire toute nouvelle copie) ou toute altération de ce contenu. Il s'agit d'une autorisation simple qu'une expression des droits pourrait formuler dans une expression déchiffrable par machine.

Le langage d'expression des droits lui-même est écrit dans un certain langage de programmation, probablement le XML. Il s'agit d'un langage de programmation dit de haut niveau qui peut aussi être lu (avec une certaine difficulté) par les êtres humains. Le XML, parfois appelé langage du Web, est largement répandu, ce qui explique son intérêt pour l'expression des droits et l'interfonctionnement (section 2.5.3.2).

2.3.9.3 Description des dictionnaires de données sur les droits

Un langage d'expression des droits exige des termes extrêmement précis (sémantique) afin de créer des expressions précises et dénuées d'ambiguïté. Or, on sait depuis longtemps que le langage naturel et le langage informatique sont deux choses différentes. La langue quotidienne est loin d'être précise pour un ordinateur et la société elle-même repose sur l'idée que l'interprétation des nuances de la langue est essentielle. Par exemple, toute loi est conçue sur le principe qu'elle ne saurait être précise au point d'exclure l'interprétation.

Les ordinateurs, d'autre part, ne peuvent pas traiter l'imprécision. En présence d'une expression ambiguë, ils ne fonctionneront pas ou fonctionneront d'une façon imprévisible. C'est pourquoi il est nécessaire d'élaborer une série de termes (mots) destinés à être spécifiquement employés dans un langage d'expression des droits. Ces termes forment la base d'un dictionnaire de données relatives aux droits.

Le terme "copie" illustre bien à quel point le langage naturel peut être problématique une fois appliqué dans un langage d'expression des droits. Il est largement utilisé dans la législation relative au droit d'auteur (il est même à la base du terme "copyright"), mais il est complètement déplacé dans le langage informatique. Si le verbe copier signifie théoriquement faire de quelque chose une reproduction exacte, en tous points semblables, l'être humain sait qu'une interprétation est nécessaire. Nous "savons" en fait ce que signifie "copier". Toutefois, ce concept n'a aucun sens pour un ordinateur. Comment une chose pourrait-elle être exactement identique à une autre? Il s'agirait en fait d'une seule et même chose (le même objet au même endroit et au même moment), de sorte que, d'un point de vue théorique, il n'y aurait aucune copie. Ainsi, lorsqu'on utilise le verbe *copier* aux fins d'un langage d'expression des droits qui doit être interprété par des ordinateurs, il est essentiel de supprimer toute imprécision liée à ce terme. En outre, s'il fallait invoquer le sens du verbe *copier* devant un tribunal, il ne serait pas possible de le définir avec précision, ce qui rendrait hasardeuse l'utilisation d'une expression des droits contenant le terme *copie* (section 2.5.3.3).

2.3.9.4 Intégration de la technologie et des mesures techniques de protection

Comme indiqué précédemment, une expression des droits (rédigée au moyen de termes figurant dans un dictionnaire de données relatives aux droits) est une instruction donnée à un dispositif à microprocesseur. Cette instruction est introduite dans un programme, qui constitue l'un des principaux éléments de tout système de gestion des droits utilisé pour protéger le contenu numérique. Comme nous le verrons ultérieurement, l'instruction indique au programme les conditions sous lesquelles le contenu, actuellement inaccessible à l'utilisateur, peut être exploité. Pour être intéressante, une expression des droits doit pouvoir fonctionner sans heurt avec le programme de protection afin que les instructions qu'elle comporte puissent être avec comprises avec précision et mises en œuvre au moment voulu.

On peut donc en déduire qu'un langage d'expression des droits doit pouvoir fonctionner avec de nombreux programmes de gestion numérique des droits, sans quoi il restera associé à un seul système de gestion des droits et n'aura qu'une utilité limitée. L'intégration d'une expression des droits dans différents systèmes commerciaux de gestion numérique est donc l'un des moyens de favoriser l'interfonctionnement pour les utilisateurs de ces systèmes. En effet, si le même contenu, régi par une seule expression des droits, peut être exploité par différents systèmes de gestion numérique des droits, cela réduit à la fois le travail de préparation des titulaires de droits (qui devraient sinon élaborer de nombreuses expressions des droits dans différents langages adaptés aux différents systèmes de gestion numérique des droits) et les inconvénients pour les consommateurs, puisqu'une seule expression des droits pourra fonctionner avec la technologie du fournisseur de gestion des droits de leur choix.

2.4 Gestion numérique des droits

À ce stade, il devrait être clair que la gestion des droits sur le contenu numérique exige une identification rémanente, une description claire et des règles d'utilisation suffisamment précises et fiables pour fournir des instructions dénuées d'ambiguïté à un programme d'ordinateur utilisé pour protéger le contenu.

La section suivante décrit les techniques de protection du contenu contre les utilisations non autorisées, à savoir les verrous et clés numériques.

2.4.1 Fonctions requises en matière de cryptage

La protection du contenu contre l'accès non autorisé exige une forme de cryptage. Le cryptage, ou processus de brouillage de l'information, est développé depuis des milliers d'années. Il a trouvé de multiples applications diplomatiques et militaires, en particulier en temps de guerre, s'agissant de dissimuler des informations à l'ennemi. Son utilisation commerciale est plus récente. Elle est particulièrement répandue dans les opérations bancaires et d'autres secteurs financiers sensibles, où la sécurité des transactions et de l'échange d'information est une considération primordiale.

Le processus de cryptage utilisé sur les dispositifs à microprocesseur pour la gestion numérique des droits fait appel à des algorithmes (systèmes mathématiques) pour brouiller l'information numérique afin d'empêcher sa restitution sous une forme intelligible. Cette méthode permet de protéger efficacement les actifs de propriété intellectuelle contre tout accès non autorisé.

La gestion numérique des droits repose sur plusieurs conditions essentielles en matière de cryptage si l'on veut que le système soit suffisamment fiable et sûr pour protéger le contenu contre tout accès ou toute altération non autorisés.

– Sécurité suffisante : les systèmes de cryptage doivent être adaptés au type de contenu à protéger. Ainsi, un ouvrage mis dans le commerce nécessite un degré de sécurité moindre qu'un document du gouvernement traitant d'armements nucléaires secrets. Il y a un arbitrage à faire entre le niveau de cryptage et les inconvénients pour l'utilisateur.

– Facilité d'utilisation : les systèmes de cryptage ne doivent pas compliquer excessivement la tâche de l'utilisateur. Par exemple, un système de cryptage qui imposerait à l'utilisateur un délai d'attente excessif pendant le déroulement de la procédure de vérification ne serait pas acceptable.

– Vulnérabilité : même les meilleurs systèmes de cryptage finissent par être déjoués. Cependant, un système de cryptage devrait être aussi élaboré que possible afin qu'une faille ne remette pas en cause la sécurité de l'ensemble du système, mais uniquement celle du dispositif ou de l'identité considéré.

– Aptitude au renouvellement : à la suite d'une défaillance majeure du dispositif de sécurité, il doit être possible de rétablir la sécurité dans l'ensemble du système au moyen d'une mise à niveau logicielle rapide[12].

– Révocabilité : il doit être possible d'empêcher un utilisateur d'accéder à un système sécurisé. Par exemple, si on sait que l'identité d'un utilisateur a été dérobée, il doit être possible d'empêcher une personne non autorisée d'employer cette identité pour accéder au système en retirant les privilèges associés à l'identité volée.

Si le cryptage est principalement utilisé pour ce que l'on appelle généralement "l'habillage du contenu", il peut trouver plusieurs autres applications. Par exemple, le cryptage fait partie intégrante de la signature numérique, qui permet de s'assurer de l'origine et de l'intégrité du contenu et des identités (afin de protéger le droit moral).

2.4.2 Description des techniques de cryptage

Le cryptage numérique est utilisé pour verrouiller l'accès au contenu. Et, comme dans le monde physique, où il existe des serrures et des clés, l'un des aspects les plus importants du cryptage pour la gestion des droits dans l'environnement numérique touche à la gestion des clés donnant accès au contenu crypté. C'est de toute évidence la sécurité et la commodité de ces processus de gestion des clés qui font la différence entre les "bons" systèmes de gestion des droits et les "mauvais".

Le cryptage numérique utilisé dans la gestion numérique des droits met en œuvre deux grands types de processus. L'un est le cryptage à simple clé, l'autre est le cryptage à clé privée et clé publique. Le premier est relativement simple. Le contenu est sécurisé par la partie A (Ted) et envoyé à la partie B (Alice). Pour déverrouiller le contenu, Alice doit disposer de la clé utilisée par Ted pour le sécuriser.

Le moyen le plus simple d'expliquer ce processus est de procéder par analogie. Supposons que la personne A (Ted) souhaite envoyer un coffret verrouillé à la personne B (Alice). Pour qu'Alice puisse ouvrir le coffret fermé à clé par Ted, elle doit avoir sa clé (ou un double de celle-ci). Cela signifie que Ted doit lui avoir donné sa clé ou un double. Il faudrait pour ce faire qu'ils se rencontrent ou que Ted envoie la clé à Alice par la poste.

---

[12] Voir la section 3.3.2 concernant l'examen, dans le cadre de l'atelier de la Commission européenne sur la gestion numérique des droits, des vues des titulaires de droits sur l'importance de l'aptitude au renouvellement.

Ce processus d'échange de clé semble tout à fait satisfaisant, jusqu'à ce que certains points faibles apparaissent. Tout d'abord, il est évident que Ted ne peut pas envoyer la clé dans le même colis que le coffret (ce qui serait trop risqué). Il faudra donc procéder à une transaction distincte. Ensuite, que se passera-t-il si Ted veut laisser le coffret à l'intention d'Alice dans un lieu public, mais ne connaît pas son adresse pour lui envoyer la clé? Dans ce cas, Alice pourrait récupérer le coffret verrouillé mais n'aurait pas accès à la clé.

À première vue, cela semble impossible, mais supposons que Ted a un coffret avec une serrure d'un type particulier, qu'il pourrait fermer avec sa propre clé, mais qu'il ne peut pas ouvrir, parce que seule Alice a une clé qui permet de le faire. Cela peut sembler étrange, mais c'est précisément la technique sur laquelle repose le cryptage utilisé dans la gestion moderne des droits sur le contenu numérique. Ce processus s'appelle cryptage à clé publique et clé privée.

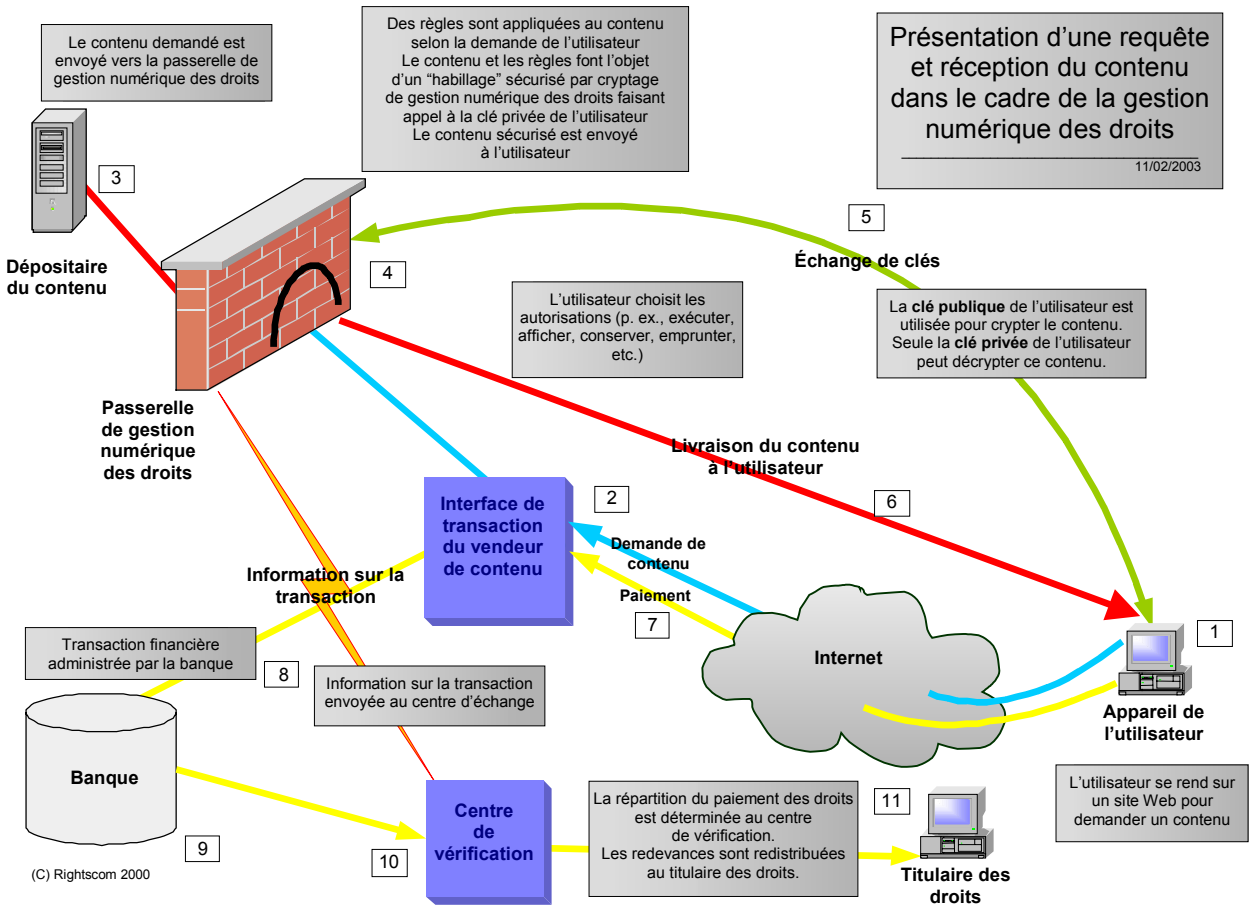
Ce système de cryptage exploite une branche des mathématiques appelée arithmétique modulaire, dans laquelle des fonctions univoques permettent d'effectuer un calcul dans une seule direction qui rend pratiquement impossible tout retour en arrière. Fondamentalement, le processus permet de générer deux clés mathématiques (numériques), une clé de verrouillage et une clé de déverrouillage. Le processus de cryptage à clé publique et clé privée fonctionne parce la clé de verrouillage peut être donnée à n'importe qui tout en maintenant privée la clé de déverrouillage. De cette façon, seule la personne ayant accès à la clé de déverrouillage (qui doit naturellement rester privée) pourra accéder au contenu une fois crypté. Ce processus permet à un vendeur de verrouiller le contenu avant de le diffuser, sur l'Internet public, à un particulier qui seul sera en mesure de le déverrouiller.

Pour la gestion des droits dans l'environnement numérique, la technique de la clé publique et de la clé privée présente l'avantage sans équivalent de s'assurer que le contenu est verrouillé pour un utilisateur ou un appareil particulier. Théoriquement, il sera impossible pour un utilisateur A (Ted) de transférer un contenu à l'utilisateur B (Alice) sans qu'Alice puisse transmettre le contenu à Mike, parce que cela donnerait accès à la clé d'Alice. Allant encore plus loin, certaines applications de gestion numérique des droits font en sorte que la clé d'Alice soit inaccessible, afin qu'elle ne puisse pas la transmettre, mais seulement l'utiliser localement sur son appareil pour ouvrir le contenu qu'elle a reçu.

Cependant, tout a un prix. En l'occurrence, il s'agit d'un prix technique. Dans ce cas, cela signifie que créer et traiter du contenu sécurisé au moyen du cryptage à clé publique et à clé privée exige beaucoup de puissance de calcul, ce qui ralentit le processus de restitution du contenu. Pour y remédier, le cryptage à clé publique et à clé privée est utilisé seulement pour verrouiller une clé ordinaire, fournie par le système de gestion numérique des droits. Étant donné que cette clé ordinaire, qui permet à la fois de verrouiller et de déverrouiller le contenu, est sécurisée par la clé privée du destinataire, elle n'est pas accessible aux utilisateurs non autorisés. Ces clés ordinaires qui sont sécurisées par cryptage à clé publique et à clé privée sont utilisables pour un seul contenu et peuvent parfois être utilisées une seule fois, d'où leur nom de "clés de session".

2.4.3 Une transaction sécurisée de contenu protégé

Le diagramme ci-après montre les différentes étapes d'une transaction simple et sécurisée entre un propriétaire et un acheteur de contenu. Ces étapes sont indiquées par des chiffres.


Présentation d'une requête et réception du contenu dans le cadre de la gestion numérique des droits
11/02/2003
Le contenu demandé est envoyé vers la passerelle de gestion numérique des droits
Des règles sont appliquées au contenu selon la demande de l'utilisateur
Le contenu et les règles font l'objet d'un "habillage" sécurisé par cryptage de gestion numérique des droits faisant appel à la clé privée de l'utilisateur
Le contenu sécurisé est envoyé à l'utilisateur
3
Dépositaire du contenu
4
5
Échange de clés
L'utilisateur choisit les autorisations (p. ex., exécuter, afficher, conserver, emprunter, etc.)
La clé publique de l'utilisateur est utilisée pour crypter le contenu. Seule la clé privée de l'utilisateur peut décrypter ce contenu.
Passerelle de gestion numérique des droits
Livraison du contenu à l'utilisateur
6
Interface de transaction du vendeur de contenu
2
Demande de contenu
Paiement
7
Information sur la transaction
Internet
1
Appareil de l'utilisateur
Transaction financière administrée par la banque
8
Information sur la transaction envoyée au centre d'échange
Banque
9
(C) Rightscom 2000
10
Centre de vérification
La répartition du paiement des droits est déterminée au centre de vérification.
Les redevances sont redistribuées au titulaire des droits.
11
Titulaire des droits
L'utilisateur se rend sur un site Web pour demander un contenu

Une transaction sécurisée de contenu protégé (© Rightscom 2003)

Un utilisateur (Alice) [1] se met en rapport avec un service de téléchargement [2] pour parcourir l'offre à la vente. Une fois qu'un choix a été fait, le service de téléchargement [2] accède à un dépositaire [3] où le contenu est censé être disponible. Le contenu est alors sécurisé lors de son passage par la passerelle de gestion numérique des droits [4] à l'aide d'une clé de session sécurisée par la clé publique d'Alice [5]. Peu importe que la passerelle de gestion numérique des droits obtienne la clé publique d'Alice, puisqu'il s'agit uniquement de la clé de verrouillage. Le contenu, sécurisé par sa clé publique, est alors envoyé à Alice [1]. Alice [1] déverrouille ensuite le contenu à l'aide de la clé privée qui n'appartient qu'à elle. Bien entendu, en contrepartie du contenu téléchargé, Alice [1] a effectué au profit service de téléchargement [7] un paiement qui est transféré au service bancaire du service de téléchargement. En même temps, le service de gestion numérique des droits peut se connecter à un centre de vérification [10] où le téléchargement est comparé avec les redevances prélevées par le serveur de téléchargement, qui sont finalement transmises au titulaire des droits (Ted).

Il s'agit, bien entendu, d'une vue très générale de l'activité, mais elle décrit avec une certaine exactitude les diverses étapes qui doivent avoir lieu. Le modèle de transaction point à point décrit plus haut pourrait aisément être mis en œuvre dans un système de cette nature. Dans ce cas, au lieu que le contenu soit envoyé à Mike par Ted, c'est Alice qui l'envoie. Mais, étant donné que ce contenu est sécurisé et qu'il ne peut pas être déverrouillé sans la clé d'Alice (soit qu'elle ne souhaite pas l'envoyer, soit qu'elle n'y ait pas accès en dehors de son propre appareil), Mike doit demander à Ted une nouvelle clé de session. Ted sécurise donc une nouvelle clé de session avec la clé publique de Mike et l'envoie à celui-ci, afin qu'il puisse déverrouiller le contenu envoyé par Alice. Ce modèle de diffusion de contenu sécurisé, dans le cadre duquel un consommateur peut transférer le contenu à un autre consommateur, devrait trouver une très large application à l'avenir.

2.4.2 Description des techniques d'association rémanente

Cette section donne une vue d'ensemble de plusieurs techniques qui peuvent être mises en œuvre pour répondre à la nécessité impérieuse d'associer de manière permanente l'information au contenu. Ces techniques sont celles de l'empreinte numérique, du tatouage et de la signature numérique.

2.4.5 Fonctions requises des techniques d'association rémanente

Pour administrer et protéger la propriété intellectuelle, il est essentiel de disposer d'une identification et d'une description (métadonnées) appropriées du contenu disponible. Ces "métadonnées" doivent toutefois être *associées en permanence* au contenu lui-même afin que les diverses applications – y compris les services antipiratage – puissent y avoir accès[13]. Dans le monde analogique, une telle association entre le contenu et ses métadonnées peut être réalisée en imprimant un identificateur sur le *support* de données contenant le contenu (par exemple, en imprimant un code à barres sur une pochette de CD ou un numéro ISBN dans un

---

13 L'identificateur dénommé "broadcast flag", dont il est question à la section 3.2.1.3.b), est un exemple d'association rémanente des métadonnées avec le contenu.

livre). Cette méthode n'est toutefois pas applicable dans le monde numérique, parce qu'il n'y a aucun support physique où imprimer les identificateurs. Il faut donc mettre en œuvre des techniques permettant d'accéder aux métadonnées *à partir du contenu lui-même*. Les principales caractéristiques requises de ces techniques sont les suivantes :[14]

– elles doivent être en mesure d'établir le lien entre le contenu et les métadonnées avec un degré d'exactitude élevé;

– la qualité du contenu ne doit pas être altérée au point que des "artefacts" deviennent perceptibles;[15]

– bonne résistance aux altérations du contenu, allant des opérations "normales" (par exemple, redimensionnement ou recadrage d'une image) aux tentatives "malveillantes" de rompre le lien entre le contenu et ses métadonnées;

– résistance dans le domaine analogique (c'est-à-dire que lorsque le contenu est a) décodé, b) restitué, par exemple sur un haut-parleur analogique, et c) renumérisé, l'identification est encore possible);

– la détection, la prise en considération et le traitement des métadonnées sont autant d'opérations qui requièrent de la puissance, et la consommation de mémoire matérielle et logicielle devrait être réduite le plus possible; et

– la préservation de la compatibilité en amont du nouveau contenu avec les appareils anciens, ainsi que de la possibilité d'exploiter le contenu ancien sur du matériel nouveau, est essentielle.

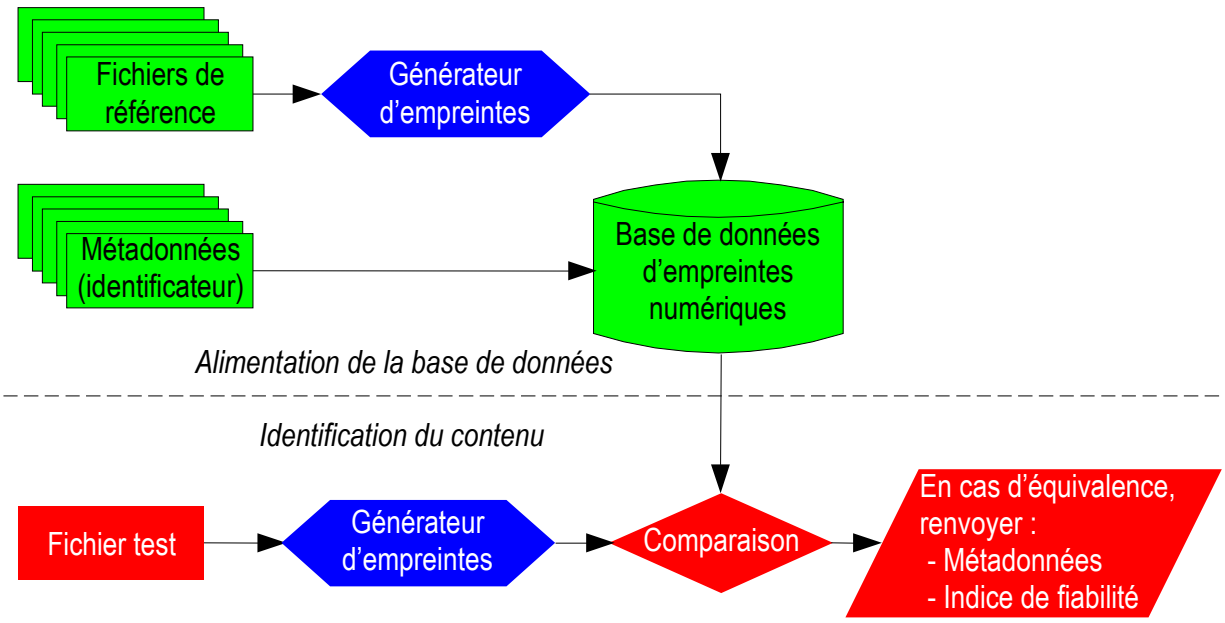
2.4.6 Empreintes numériques

Des empreintes numériques peuvent être employées pour identifier le contenu selon le processus représenté dans le diagramme ci-dessous. Les empreintes numériques, ou "techniques d'identification fondées sur le contenu" fonctionnent sur le principe de l'extraction des caractéristiques d'un fichier et de leur stockage dans une base de données. En présence d'un fichier inconnu, les caractéristiques de celui-ci sont calculées et comparées avec celles conservées dans la base de données, afin de rechercher une équivalence. Si une équivalence est trouvée, le système extraira les métadonnées appropriées de la base de données d'empreintes numériques.

---

14 Il convient noter que toutes les conditions ne s'appliquent pas à tous les scénarios d'application.

15 À l'exception des "tatouages visibles" utilisés, par exemple, par des chaînes de télévision pour intégrer leur logo dans leurs émissions.



Système d'empreintes numériques

L'utilisation des empreintes numériques passe par trois étapes :

– tout d'abord, une base de données contenant des "empreintes numériques de référence" et les métadonnées appropriées doit être constituée. Cette étape, dépeinte dans le diagramme ci-dessus, est un préalable à toute tentative d'identification de contenu inconnu;

– ensuite, pour trouver des informations sur n'importe quel fichier (appelé "fichier test"), le système génère une "empreinte test" à partir du fichier test. Cette empreinte test est alors comparée à toutes les "empreintes numériques de référence" stockées dans la base de données;[16]

[16] Il convient noter que cette comparaison peut représenter une lourde tâche lorsque la base de données est vaste. Cependant, des stratégies bien conçues de gestion de bases de données peuvent ramener les ressources nécessaires à des niveaux acceptables.

- enfin, lorsqu'une empreinte numérique équivalente a été trouvée, les métadonnées correspondantes sont extraites de la base de données. Ces métadonnées sont l'aboutissement du processus.

Des logiciels et des services utilisant des techniques d'empreintes numériques existent pour différents types de supports tels que des fichiers audio et vidéo. Les meilleurs de ces systèmes permettent – dans certains domaines – d'identifier correctement plus de 95 fichiers sur 100, même lorsque des fichiers ont été altérés par mégarde ou par malveillance pour neutraliser l'empreinte numérique. Certaines techniques peuvent même atteindre des taux de correspondance élevés alors que le fichier test a été créé en présence d'un fort bruit de fond, comme dans un club.

Si elles sont très efficaces avec certains types de contenu, les empreintes numériques sont moins utiles pour faciliter l'identification formelle d'autres types de contenu, selon leur niveau de "détail". Ainsi, les empreintes numériques sont adaptées au contenu audio, vidéo et audiovisuel, de même qu'aux photographies, mais moins à l'infographie[17] ou au texte.

Le domaine d'application traditionnel des techniques d'empreinte numérique est la surveillance des stations de radio pour a) établir les hits parades radio et, depuis l'avènement de MTV, vidéo, et b) favoriser la répartition des redevances aux titulaires de droits par les sociétés de perception. Les empreintes numériques sont de plus en plus utilisées pour détecter les atteintes au droit d'auteur dans les systèmes de distribution de contenu point à point. Le scénario suivant illustre aussi les applications des empreintes numériques. Un utilisateur qui se trouve dans un pub ou un restaurant entend soudain une chanson qui lui plaît, active son appareil à empreintes numériques (par exemple, son téléphone portable), qui identifie la chanson et transmet certaines informations à un fournisseur de services. Arrivé chez lui, l'utilisateur trouve dans sa boîte aux lettres électronique la même chanson sous forme de dossier audio protégé par un système de gestion numérique des droits. Ce fichier lui a été envoyé par un système automatisé mettant en œuvre l'empreinte numérique envoyée du téléphone portable pour identifier la chanson appréciée par l'utilisateur.

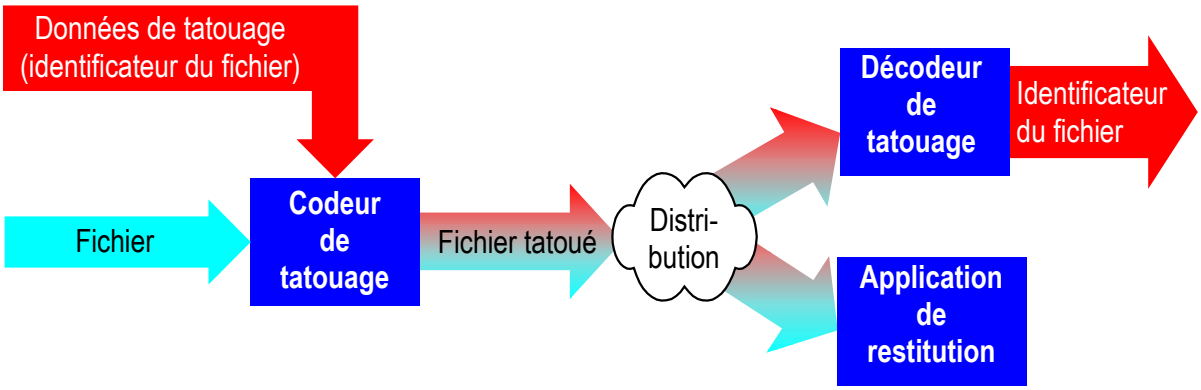
2.4.7 Tatouage

Le tatouage est aussi fréquemment cité parmi les techniques de protection du droit d'auteur. Un tatouage est "une information (imperceptiblement) incorporée". Cette information (souvent un fichier ou un identificateur de propriété intellectuelle) peut, bien qu'imperceptible[18] aux yeux des consommateurs ordinaires, être extraite au moyen d'un logiciel spécial. Ce "détecteur de tatouage" peut, une fois appliqué à un contenu susceptible d'être piraté, vérifier si le contenu comporte le tatouage et, de ce fait, confirmer ou infirmer les soupçons. D'une manière générale, tous les fichiers qui doivent être distribués sont tatoués avant d'intégrer le circuit de distribution. C'est ce que montre le diagramme ci-dessous.

---

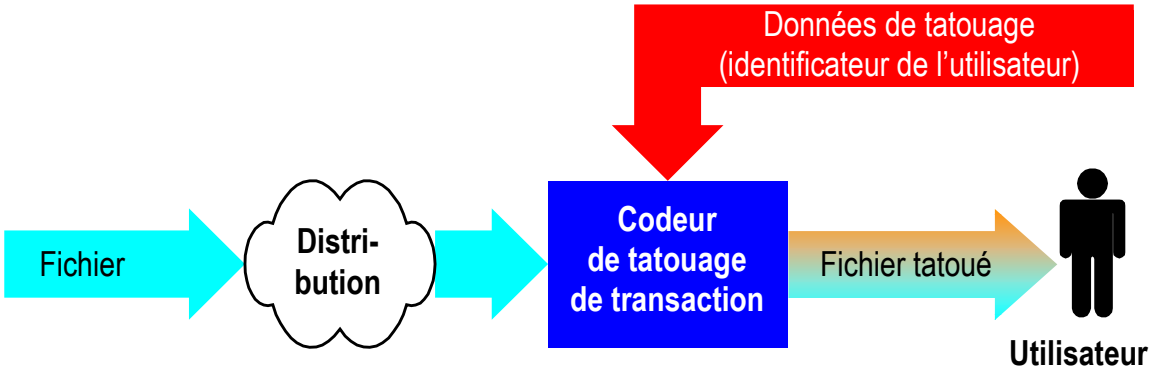
17 Bien entendu, des photographies comportant très peu de détails (par exemple, la photographie d'un ciel bleu) peuvent être moins adaptées aux empreintes numériques qu'un graphique d'ordinateur avec beaucoup de détails.

18 Comme indiqué ci-dessus, tous les tatouages ne sont pas nécessairement imperceptibles, voir la note 15.



Système de tatouage

Une deuxième application de la même technologie consiste à incorporer un "tatouage de transaction", comme l'illustre le diagramme ci-dessous. Les tatouages de transaction permettent d'établir un lien entre un utilisateur hypothétique dans la chaîne de distribution du contenu et le contenu qu'il a "touché". Dans les cas où des identificateurs sont nécessaires *à la fois* pour le contenu et pour l'utilisateur, les deux types de tatouage peuvent être combinés.



Système de tatouage de transaction

La "charge utile"[19] du tatouage (qu'il s'agisse d'un tatouage a priori ou d'un tatouage de transaction) peut varier et dépend du type de contenu, principalement en raison de la quantité de données qui peut être transportée de manière fiable et pratique dans le tatouage. D'une manière générale, plus le fichier est volumineux, plus il peut dissimuler de données.

Les tatouages présentent toutefois quelques inconvénients. Comme dans le cas de l'empreinte numérique, le tatouage ne peut pas être employé avec tous les types de contenu. Les petits éléments graphiques tels que les logos ou du texte ne peuvent pas transporter des tatouages en raison de la limitation générale de la quantité de données qui peuvent être incorporées dans le contenu. La charge utile de tatouage dépend de trois facteurs principaux :

– le type de contenu (audio, vidéo, images fixes, graphiques, texte);

---

19 La charge utile du tatouage désigne le volume de données qui peuvent être "dissimulées" (par exemple, l'identificateur utilisé pour identifier de manière unique le fichier ou l'élément de propriété intellectuelle qu'il contient).

- la taille du contenu :

    - vidéo : fréquence de trame, taille de l'image, taux de compression, durée;
    - audio : taux d'échantillonnage, taux de compression, durée;
    - images fixes : taille de l'image, taux de compression.

- la fiabilité :

    - à quel type d'"attaques" le tatouage doit-il résister?;
    - faut-il le protéger contre des opérations ordinaires de traitement du signal, telles que recadrage, rééchantillonnage ou changement de vitesse, ou faut-il viser également des activités plus sophistiquées, telles que faire pivoter une image de quelques degrés?

D'un autre côté, on peut aussi arguer que la fiabilité du tatouage peut dépendre du volume des informations à incorporer dans tel ou tel type de contenu. Ces limitations étant assez strictes avec des algorithmes de tatouage d'aujourd'hui, il est largement admis que les tatouages devraient transporter seulement une faible quantité d'informations, généralement un identificateur de contenu. Une deuxième limitation des techniques de tatouage tient au fait que, lorsqu'on incorpore un tatouage, on modifie le contenu original. Si cette modification est dans la majorité des cas sans incidence sur la qualité du matériel d'un point de vue humain, il peut s'avérer difficile d'incorporer à plusieurs reprises des tatouages au même contenu sans qu'ils finissent par devenir perceptibles. Par conséquent, des tatouages ne peuvent pas, par exemple, être incorporés au cours du processus itératif d'élaboration d'une publicité.

Troisièmement, tous les systèmes de tatouage connus aujourd'hui peuvent être supprimés sans incidence notable sur la qualité du contenu lui-même, de sorte que, lorsqu'un système de tatouage a été cassé, le contenu protégé à l'origine peut devenir incontrôlable.

Un dernier inconvénient réside dans le fait que la détection du tatouage ne peut pas fonctionner avec du contenu ancien si aucun tatouage n'a été inséré à l'origine.

Le tatouage est principalement utilisé dans la sphère audiovisuelle pour faciliter le contrôle de l'utilisation du matériel protégé par le droit d'auteur. Certains CD audio, par exemple, contiennent des tatouages. Des tatouages sous forme de logos sont aussi incrustés par des chaînes de télévision à leur signal de radiodiffusion. Ces tatouages sont clairement visibles et servent à dissuader d'autres chaînes d'utiliser ces émissions de manière illicite. Toutefois, ils restent faciles à supprimer.

La frontière entre le tatouage et l'empreinte numérique étant souvent confuse, le tableau ci-après énumère les principales différences entre ces deux techniques.

Empreinte numérique	Tatouage
Fonctionne sur tous les types de supports (bien que d'application limitée pour certains d'entre eux).	Fonctionne seulement sur certains types de supports.

Empreinte numérique	Tatouage
Aucune modification des fichiers n'est nécessaire. Par conséquent les utilisateurs n'auront jamais en leur possession qu'un fichier "original" ou non modifié.	Les fichiers doivent être tatoués avant qu'on puisse détecter le tatouage, ce qui peut, dans certaines circonstances, compromettre leur bonne utilisation.
Vulnérable aux attaques malveillantes, bien que le taux de reconnaissance de certains types de contenu par certains systèmes soit nettement supérieur à 95%.	Vulnérable aux attaques malveillantes.
Peut identifier le contenu "ancien".	Ne peut pas identifier le contenu "ancien".
L'empreinte ne contient aucune donnée. Elle fournit seulement un lien vers une base de données qui contient une quantité illimitée de métadonnées.	La quantité de données pouvant être incorporée dans un tatouage est très limitée. Lorsque le tatouage contient un identificateur, un lien vers une base de données – qui peut comporter une quantité illimitée de métadonnées – peut être effectué.
Nécessite une infrastructure faisant appel à une base de données d'empreintes numériques.	L'infrastructure est seulement nécessaire pour les vérifications juridiques. L'efficacité des systèmes de tatouage peut diminuer à mesure qu'apparaissent de nouvelles techniques de compression du contenu plus efficaces, malgré les améliorations apportées aux techniques de tatouage.

Tatouage contre empreinte numérique

2.4.8 Signatures numériques

Il est important que l'information associée au contenu (par exemple, les identificateurs et les expressions des droits) soit fiable. C'est possible lorsque la partie qui ajoute les métadonnées a) signe numériquement ces métadonnées et b) est réputée avoir l'autorisation d'ajouter les métadonnées. Une signature numérique, qui s'apparente à une signature manuscrite[20], donne des renseignements sur l'origine d'une information et sur l'existence éventuelle de modifications de cette information. Pour s'assurer que les métadonnées associées à un fichier n'ont pas été modifiées, il convient de procéder de la manière suivante :

– le signataire calcule une valeur de hachage pour le contenu et les métadonnées;

– le signataire code la valeur de hachage au moyen d'une clé à laquelle lui seul a accès;

[20] De plus en plus de pays confèrent aux signatures numériques le même statut juridique qu'aux signatures physiques (ou manuelles).

– la valeur de hachage chiffrée (“signature”) est ajoutée au fichier (qui contient maintenant trois éléments : le contenu original, les métadonnées et la signature); et

– la personne qui souhaite vérifier la signature peut utiliser le même outil que celui employé par le signataire pour signer l’algorithme avec une clé correspondante dont on sait qu’elle provient du signataire.

Le processus en quatre étapes décrit ci-dessus permet à un utilisateur de vérifier que le contenu n’a pas été modifié, mais la personne qui vérifie ne sait toujours pas si le signataire avait le droit d’ajouter des informations ou d’habiller le contenu. Pour ce faire, le signataire doit ajouter un certificat à sa signature. Ce certificat, délivré par un organisme de certification, identifie formellement le signataire et permet de l’identifier (et de lui demander des comptes) lorsque des erreurs sont relevées dans les données qu’il communique.

2.4.9 Gestion de la confidentialité

L’une des difficultés s’agissant d’établir une infrastructure efficace de gestion des droits dans l’environnement numérique concerne le respect de la vie privée, de la confidentialité et des données personnelles. La mesure dans laquelle toute infrastructure de gestion des droits dans l’environnement numérique qui fait la preuve de son efficacité aux fins de la protection de la propriété intellectuelle peut se traduire en même temps par des intrusions absolument inacceptables dans la vie privée des individus ou leurs activités commerciales soulève des préoccupations très réelles et parfaitement compréhensibles[21]. Cette question est examinée dans la section 5.2.1.

Les modèles de gestion numérique des droits reposent sur une infrastructure d’identification fiable du contenu, des autorisations relatives à ce contenu et des parties aux transactions découlant de ces autorisations. Cette question devient particulièrement sensible lorsque les parties concernées sont des consommateurs privés. Une grande partie du débat sur la gestion de la confidentialité semble se concentrer sur la valeur marchande des données personnelles et sur les préoccupations relatives à l’usurpation d’identités et de cartes de crédit. Aussi importantes soient-elles, ces questions ne doivent pas banaliser la question fondamentale du respect de la vie privée.

La mise en œuvre appropriée de techniques de renforcement de la confidentialité dans l’infrastructure de gestion des droits sur le contenu numérique sera sans aucun doute essentielle pour que le consommateur accepte à long terme les systèmes de gestion numérique des droits dans. Cela passe par l’utilisation de techniques de garantie de l’anonymat, qui permettent l’authentification des identités par des “tiers de confiance” (en d’autres termes, un organisme qui a la confiance du consommateur et du distributeur), sans que l’identité réelle du consommateur soit divulguée. Si ces niveaux intermédiaires peuvent sembler ajouter une complexité inutile, une infrastructure de gestion numérique des droits qui ne tiendrait pas

---

[21] Pour une conception spectaculairement dystopique de la gestion numérique des droits, voir l’article de Richard Stallman, *The Right to Read*, publié à l’origine édité dans C*ommunications of the ACM*, février 1997, 40 n° 2; disponible, avec une note de l’auteur mise à jour en 2002, à l’adresse *http://www.gnu.org/philosophy/right-to-read.html*. Bien que cet article puisse être critiqué pour sa tonalité tendant à l’exagération, quiconque participe à l’élaboration ou à la mise en œuvre de solutions de gestion numérique des droits devrait le lire attentivement.

compte des préoccupations légitimes en matière de respect de la vie privée et de la confidentialité serait vouée à l'échec.

2.4.10 Systèmes de paiement

Il existe plusieurs de modèles de paiement pouvant fonctionner dans les systèmes de gestion numérique des droits.

Généralement, on règle l'achat de contenu en saisissant un numéro de carte de crédit sur une page Web sécurisée, cryptée à l'aide du protocole SSL. La carte de crédit est le mode de règlement le plus répandu pour le contenu (et les produits) achetés en ligne. Selon une évaluation récente de la société Visa, les clients européens ont dépensé 2,57 milliards d'euros en ligne à l'aide de cartes Visa au cours du quatrième trimestre de 2002, soit 136% de plus qu'au cours de la même période en 2001. Visa estime également à 31,1 millions le nombre de transactions en ligne effectuées au quatrième trimestre de 2002, contre 14,5 millions au quatrième trimestre de 2001. Toutefois, nombreux sont encore les utilisateurs qui sont réticents à utiliser leur carte de crédit directement sur le site Web d'un vendeur en ligne, en raison de préoccupations liées à la confidentialité et à la sécurité, alors que les vendeurs en ligne, quant à eux, voient parfois leur responsabilité engagée.

Bien que la plupart des paiements en ligne soient effectués au moyen de cartes de crédit, d'autres modes de paiement ont été mis au point ou sont en voie de l'être. Par exemple, le portail musical Popfile.de, en Allemagne, a élaboré, en association avec Deutsche Telekom, un système qui permet aux utilisateurs d'écouter en continu et de télécharger des morceaux de musique protégés, les coûts correspondants étant répercutés sur la facture de leur téléphone fixe. Divers systèmes de micropaiement se développent également et deviendront peut-être des méthode de paiement généralisées pour l'achat de contenu protégé, non seulement en ligne mais également sur des dispositifs mobiles.

Plusieurs entreprises ont également mis au point des systèmes qui permettent à des utilisateurs de saisir leur numéro de carte de crédit sur un serveur central. Une fois enregistré, le consommateur a accès à un porte-monnaie électronique, qui peut ensuite être utilisé pour acheter du contenu sur des portails en ligne, qui sont partenaires du service. Le système est censé garantir l'anonymat et la confidentialité, tout en réduisant les risques de poursuites à l'encontre des cybercommerçants. D'autres sociétés ont élaboré des systèmes de micropaiement, qui sont généralement traités par l'intermédiaire des téléphones portables, pour des transactions de faible montant, telles que l'achat d'un morceau de musique parmi un catalogue en ligne, d'un livre électronique ou d'un article dans la partie réservée (payante) du site Web d'un journal.

2.5 Normes concernant la gestion numérique des droits

L'élaboration de normes est l'un des aspects cruciaux pour l'avenir de la gestion numérique des droits. De nombreuses applications destinées à administrer et à mettre en œuvre la protection du contenu font appel à des normes. Les normes sont une composante essentielle des applications de gestion numérique des droits et interviennent à différentes étapes de la diffusion du contenu électronique. La mise en œuvre des normes dans les applications de gestion numérique des droits est tout aussi importante pour permettre à des appareils, des applications et des services de différents fournisseurs d'échanger du contenu

que pour les prestataires de services, qui possèdent et contrôlent l'infrastructure de gestion numérique des droits, les titulaires de droits qui sont intéressés par la diffusion maximale de leur contenu et les consommateurs qui écoutent, regardent et lisent du contenu sur des appareils et des applications généralement désignés sous le nom de "lecteurs". L'objectif principal de l'utilisation des normes dans les applications de gestion numérique des droits consiste à favoriser l'interfonctionnement des appareils, des applications et des services, condition essentielle à la réussite de toute entreprise utilisant la gestion numérique des droits.

2.5.1 Normes officielles et normes informelles

Les normes peuvent être officielles ou non. Les normes officielles sont celles régies par des organismes de normalisation internationalement agréés, tels que l'Organisation internationale de normalisation (ISO) ou l'Union internationale des télécommunications ("UIT"). Toutefois, leurs procédures sont généralement lentes, de sorte que certains estiment qu'elles ne sont pas adaptées au rythme du changement à l'ère informatique. Outre les organismes de normalisation officiels, il en existe d'autres, tels que l'Internet Engineering Task Force ("IETF") et le World Wide Web Consortium ("W3C"). Sans être des organismes de normalisation officiels, l'IETF et le W3C jouent un rôle fondamental dans l'élaboration des normes pour l'Internet et leurs recommandations sont largement adoptées.

Les normes informelles vont de celles appliquées au niveau international par un pan entier de l'industrie, telles que le projet Digital Video Broadcasting ("DVB") ou l'Organization for the Advancement of Structured Information Standards ("OASIS"). Ces deux organismes ont des adhérents dans l'industrie et travaillent à des solutions permettant à des fabricants de créer des produits et des services à l'intention des titulaires de droits et des consommateurs. Ils sont reconnus sur le plan international, et les normes qu'ils mettent au point sont appliquées et apportent une contribution importante à l'infrastructure technique et réglementaire de la gestion numérique des droits.

2.5.2 Normes de gestion des droits sur le contenu numérique

Comme indiqué dans le tableau figurant à la section 2.3.1, de nombreux systèmes d'identification sont normalisés et administrés par l'ISO. Ces normes officielles sont une garantie de stabilité des systèmes d'identification et devraient assurer leur longévité, deux facteurs essentiels pour une large application. Il existe toutefois des systèmes d'identification qui ne sont pas administrés par l'ISO, telle la norme DOI (section 2.3.2).

La première norme importante relative aux métadonnées a été mise au point par les milieux de bibliothéconomie pour permettre le partage des fiches catalographiques. Cette norme, dénommée MARC, est toujours largement utilisée. Toutefois, les métadonnées documentaires ont été conçues pour un seul type d'utilisation – la "recherche" – afin de donner aux utilisateurs des points d'accès au fonds bibliothécaire (tout comme les métadonnées mises au point ultérieurement dans ce domaine). Comment un utilisateur (humain) souhaite-t-il effectuer ses recherches : en fonction du nom de la publication (quelles éditions de l'ouvrage sont archivées?), de l'auteur (quels ouvrages de cet auteur sont archivés?) ou du thème traité (quels ouvrages sur ce sujet sont archivés?).

La tradition des métadonnées de recherche a été adaptée en ligne dans le cadre du projet "Dublin Core"[22], qui a aboutit à une norme de bibliothéconomie conçue initialement comme le "plus petit dénominateur commun" pour la recherche tous supports et tous secteurs sur l'Internet. Des tentatives ont été faites en vue de perfectionner la norme Dublin Core moyennant l'adjonction de "qualificatifs" aux 15 éléments originaux; malheureusement, ils n'ont fait que confirmer à quel point cette norme est fondamentalement inextensible (elle ne repose sur aucun principe susceptible d'être exprimé par un modèle de données cohérent).

La nécessité de disposer de "données sur les produits" pour favoriser la distribution est reconnue depuis longtemps. Le secteur du livre en particulier, avec ses nombreuses lignes de produits et ses multiples lancements de nouveaux produits, a pris conscience depuis longtemps de la nécessité de distribuer des données sur les "ouvrages imprimés", tout d'abord sous forme de volumes imprimés, puis sous forme de publications électroniques, que les destinataires (grossistes et détaillants) peuvent charger dans leurs systèmes informatiques locaux.

Généralement, ces informations sur les produits sont agrégées par un nombre restreint "d'organismes bibliographiques" sur chaque territoire; alors que le commerce du livre se fait de plus en plus en ligne, les organismes bibliographiques ont augmenté leur offre en y incluant des informations de plus en plus sophistiquées sur les produits (images de couverture, par exemple), qui peuvent s'avérer nécessaires pour inciter les consommateurs à acheter en l'absence de possibilité de parcourir les ouvrages. L'industrie de l'enregistrement, où les enjeux ne sont toutefois pas les mêmes en ce qui concerne le nombre de produits, a également vu la création d'un certain nombre d'organismes d'agrégation des données pour fournir aux détaillants des informations synthétiques sur les produits.

La demande en faveur de possibilités accrues en matière de transfert d'informations sur les produits dans le secteur du livre s'illustre dans la mise au point la norme ONIX (échange d'information en ligne). Cette norme fondée sur le XML, qui est désormais largement appliquée, permet la diffusion d'informations complètes sur le produit à partir du point de création, chez l'éditeur, et dans toute la filière de distribution (soit directement, soit via des intermédiaires, qui peuvent assurer un contrôle de la qualité et améliorer les données et, bien entendu, les compléter, ce qui peut être un atout particulièrement important). Des normes semblables pour les données sur les produits devraient apparaître dans les industries musicales et audiovisuelles.

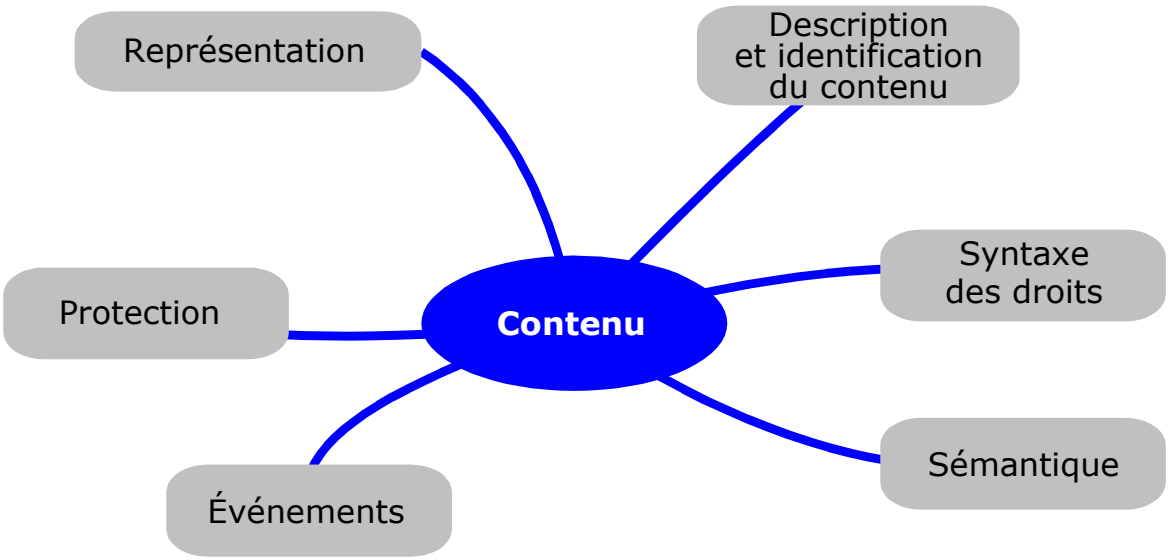
2.5.3 Normes pour la gestion numérique des droits

Plusieurs éléments sont nécessaires pour établir une infrastructure normative logique et fonctionnelle pour les applications de gestion numérique des droits. La figure ci-dessous montre les divers secteurs qui qualifient les éléments de contenu (tels que des fichiers musicaux, des clips vidéo ou des livres électroniques) dans une application de gestion numérique des droits.

---

[22] Voir *www.dublincore.org*.

Les sous-sections suivantes contiennent une brève description de ces qualificatifs :



Éléments de contenu et qualificatifs liés à la gestion numérique des droits

2.5.3.1 Représentation du contenu

La représentation du contenu est employée pour habiller le contenu. Les normes généralement utilisées sont les formats MP3 ou Mpeg-4. Dans le contexte de la gestion numérique des droits, il importe de pouvoir représenter également les métadonnées et la structure des éléments de contenu complexes. Parmi les exemples typiques de normes de représentation du contenu pouvant être employées dans un tel contexte, on citera les formats XML et Mpeg-21 DID :

– Le XML (Extensible Markup Language) est un langage courant du Web, utilisé à de nombreuses fins. Le XML peut représenter un contenu en ligne structuré tel que du texte,

mais également les métadonnées associées à n'importe quel contenu. Il est moins approprié pour représenter d'autres types de contenu tels que les fichiers audio et vidéo.

– La déclaration d'objet numérique (DID) fait partie du cadre Mpeg-21[23]. Cette norme de représentation du contenu permet de déclarer la structure et les métadonnées des éléments de contenu complexes. Par exemple, une œuvre musicale numérique comportant plusieurs enregistrements sonores, la photographie de la pochette, l'insert avec les paroles, etc.

2.5.3.2 Syntaxe des droits

Faisant aussi techniquement partie de la description du contenu, la syntaxe des droits est une série de termes définissant des règles à l'égard de ce contenu. Les syntaxes de droits normalisées sont généralement appelées langages d'expression des droits ("REL", pour "Rights Expression Language"), comme indiqué dans la section 2.3.9. Le langage d'expression des droits Mpeg-21 ("Mpeg-21 REL") en est un exemple.

La norme Mpeg-21 REL décrit la syntaxe et la sémantique de l'expression des droits. Ce langage utilise un modèle de données fondamental et extensible pour ses principaux concepts et éléments. Le modèle de données comprend quatre entités fondamentales et les relations entre ces entités. Ces relations sont définies par l'affirmation REL "octroi". La relation d'octroi dans le cadre de la norme MPEG REL comprend généralement les éléments suivants :

– le bénéficiaire principal;

– le droit conféré;

– la ressource à laquelle le droit conféré s'applique; et

– les conditions préalables à l'exercice du droit.

Le modèle de données central sera enrichi d'un certain nombre d'"extensions" qui ajouteront des fonctions. Par exemple, une telle extension peut viser à élargir la gamme des conditions qui peuvent être appliquées aux droits octroyés. Le Mpeg-21 REL devrait devenir une norme internationale d'ici l'automne 2003.

---

[23] Voir *www.telecomitalialab.com*.

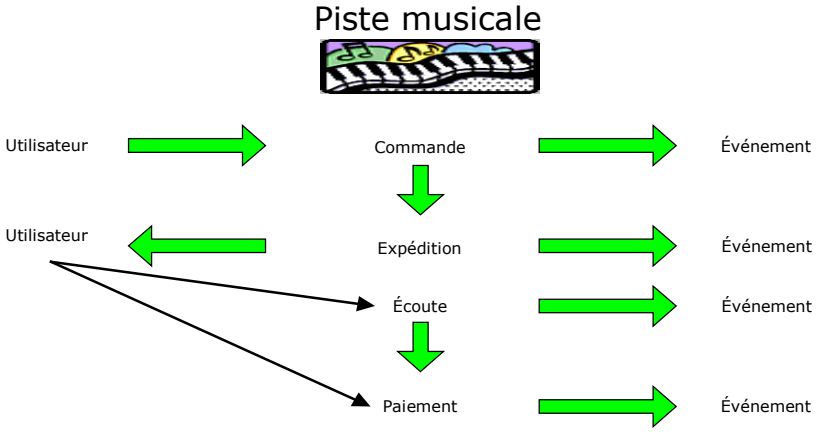
2.5.3.3 Sémantique

Les syntaxes de droits ne peuvent être utilisées que lorsque leurs termes sont bien définis par la sémantique fondamentale. La sémantique donne la signification exacte des verbes et des termes utilisés dans tout langage ou, en fait, toute syntaxe des droits. Le but des normes sémantiques dans ce domaine est de permettre l'échange de contenu faisant appel à des normes et à des schémas de langages de droits différents. Ainsi, les normes sémantiques pourraient bientôt devenir un élément important pour l'interfonctionnement entre les applications de gestion numérique des droits. La norme de sémantique la plus importante en cours d'élaboration est le dictionnaire de données des droits Mpeg-21 ("RDD") (voir la section 2.3.9.3 pour une description des dictionnaires de données sur les droits.)

La norme RDD Mpeg-21 vise à favoriser la mise en œuvre d'un langage des droits pour l'échange sécurisé d'actifs de propriété intellectuelle sur les réseaux au moyen d'un dictionnaire interopérable de données sur les droits. Cette initiative, fondée sur l'analyse originale développée dans le cadre du projet <indecs> (voir la section 2.3), est en cours depuis la mi-2001.

2.5.3.4 Signalisation d'événements

La signalisation d'événements joue un rôle majeur dans les applications de commerce électronique relatives au contenu. Toute étape d'une transaction de commerce électronique produit généralement un événement. Par exemple, l'achat en ligne d'un morceau de musique, qui comprend la commande, l'expédition, l'écoute et le règlement du contenu, génère les événements représentés dans la figure ci-dessous :



Signalisation d'événements

Les normes de signalisation d'événements, telles que celle mise au point à l'égard du format Mpeg-21, peuvent donc constituer un aspect important d'une application de gestion numérique des droits. La norme de signalisation des événements Mpeg-21, qui est en cours d'élaboration, devrait comprendre une bibliothèque de "modèles" de signalisation d'événements : le langage de signalisation d'événements Mpeg-21 ("ERL"), fondé sur le Mpeg-21 REL, grâce auquel un utilisateur peut demander ou décrire un événement, et le dictionnaire de signalisation d'événements Mpeg-21, fondé sur le Mpeg-21 RDD, qui est la sémantique étayant le langage Mpeg-21 ERL.

2.5.3.5 Protection du contenu

Le dernier secteur, la protection du contenu, qui met en œuvre les restrictions associées au contenu numérique et empêche les utilisations non autorisées de celui-ci, est aussi un élément crucial de tout système de gestion numérique des droits.

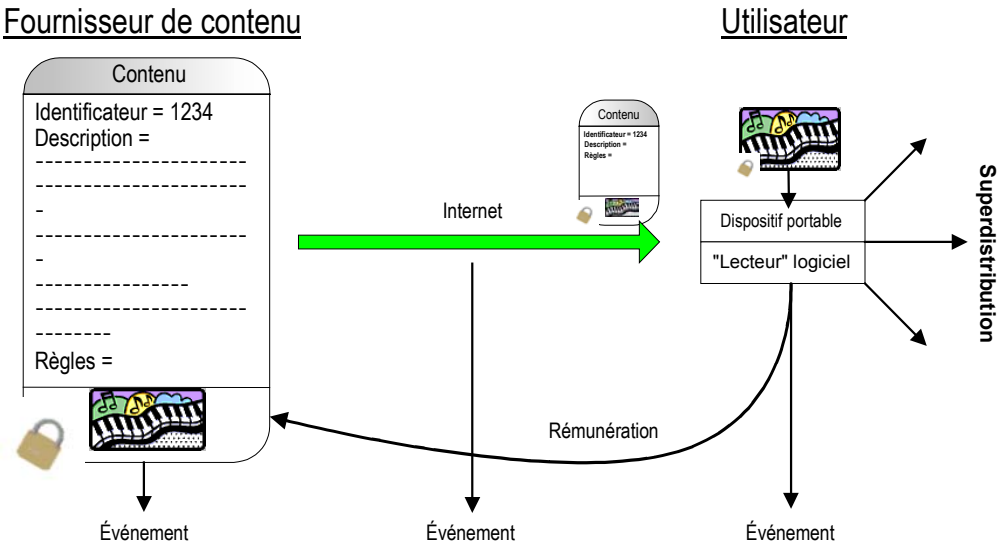
Les normes de protection du contenu traitent directement de la protection physique du contenu. Les normes de protection du contenu comprennent des normes simples, telles que des algorithmes cryptographiques, les normes relatives à l'accès conditionnel et les normes de tatouage, des normes intermédiaires telles que les normes de protection des supports à microprocesseurs et des normes complexes, telles que le format Mpeg-4 IPMP.

Le système de brouillage du contenu ("CSS") est un exemple de technologie de protection du contenu; il est utilisé pour protéger le contenu audiovisuel des disques numériques universels (DVD). La DVD CCA concède sous licence aux studios et aux fabricants de lecteurs de DVD (y compris les lecteurs et disques autonomes et les dispositifs intégrés, tels que les ordinateurs individuels), le CSS et divers composants du système. Le CSS est un système complet de protection du contenu. La protection conférée par cette technique est complétée par les clauses obligatoires de la licence CSS; celles-ci visent à assurer une protection maximale du contenu des DVD, en autorisant uniquement certaines utilisations et en imposant des normes de fiabilité aux fabricants. Bien que le CSS ait été piraté par DeCSS, cette technique continue d'être utilisée pour protéger le contenu des disques numériques universels.

Le groupe MPEG a mis en œuvre une autre conception des normes d'application. Le format MPEG ne définit pas un système de sécurité complet mais dessine seulement un cadre d'application pour la protection du contenu. Des solutions commerciales peuvent donc être intégrées à la norme.

2.5.3.6 Description d'ensemble

Comme indiqué ci-dessus, la représentation, l'identification et la description du contenu, la syntaxe des droits, la sémantique, la signalisation d'événements et la protection du contenu sont des éléments essentiels à l'élaboration d'un système de gestion numérique des droits. Il faut garder à l'esprit que chaque élément dépend d'un autre, ainsi qu'il ressort du diagramme ci-dessous :



Système de protection du contenu

Le fournisseur de contenu “habille” le contenu dans un conteneur, qui contient le fichier (dans ce cas, un morceau de musique). Ce conteneur comprend un identificateur unique (par exemple, un code ISRC), une série de descripteurs, une série de règles (avec la sémantique sous-jacente) et la piste musicale elle-même (par exemple, un fichier MP3).

Une fois habillé, le contenu peut “voyager” sur l’Internet jusqu’à l’utilisateur. Celui-ci peut lire le contenu sur un “lecteur” logiciel ou un appareil adapté. Il est important de noter que l’identification, la description, les règles et la protection initiales sont encore associées aux données. Cela permet au fournisseur de contenu d’être rémunéré par l’utilisateur pour l’utilisation du contenu et d’établir des rapports précis (signalisation d’événements), concernant par exemple la fréquence d’utilisation du contenu. L’utilisateur peut également (si les règles le permettent) envoyer le contenu à un autre utilisateur (superdistribution).

3. LE CADRE JURIDIQUE ACTUEL

3.1 Obligations découlant des traités internationaux

3.1.1 Traités Internet de l'OMPI

3.1.1.1 Les dispositions anticontournement

Les WCT et le WPPT ont établi les nouvelles normes juridiques internationales en matière de protection des mesures techniques, telles que les techniques de gestion numérique des droits, employées pour préserver le contenu contre l'accès et les utilisations non autorisés. Les traités de l'OMPI sont le fruit de longues négociations, conduites avant et pendant la conférence diplomatique. Pour comprendre les obligations imposées par les dispositions qui ont été finalement adoptées, il peut être utile de comparer la proposition de base[24] soumise aux délégués à la conférence diplomatique avec le texte final.

L'article 13 de la proposition de base aurait interdit les dispositifs et services de "neutralisation de la protection" – ou de contournement - sachant qu'ils seraient utilisés aux fins ou dans le cadre de l'exercice non autorisé des "droits prévus par le présent traité", c'est-à-dire des droits d'auteur[25]. Cet article aurait également imposé aux Parties contractantes l'obligation de prévoir des "sanctions appropriées et efficaces" contre ces actes illégaux. Enfin, les mesures techniques de protection n'étaient pas définies dans la proposition de base, mais le projet de texte aurait rendu illégal le contournement de "tout procédé, traitement, mécanisme ou système destiné à prévenir ou empêcher tout acte auquel s'appliquent les droits prévus par le présent traité".

La proposition de base se serait appliquée uniquement aux mesures de protection du droit d'auteur (et non au contrôle d'accès), et seulement aux dispositifs et services, et non à l'acte de contournement. Ce texte a été modifié au cours de la conférence diplomatique.

---

[24] Voir la *Proposition de base concernant les dispositions de fond du traité sur certaines questions relatives à la protection des œuvres litteraires et artistiques soumise à l'examen de la conférence diplomatique*, établie par le Président des comités d'experts sur un éventuel protocole relatif à la Convention de Berne et sur un éventuel instrument relatif à la protection des droits des artistes interprètes ou exécutants et des producteurs de phonogrammes (doc. OMPI CRNR/DC/4 du 30 août 1996), disponible à l'adresse *http://www.wipo.int/eng/dip/conf/4dc_all.htm* [ci-après dénommée "proposition de base"].

[25] Article 13 : Obligations relatives aux mesures techniques
1) Les Parties contractantes doivent déclarer illégale l'importation, la fabrication ou la distribution de dispositifs de neutralisation de la protection, ou l'offre ou la prestation de tous services ayant un effet identique, par quiconque sait ou peut raisonnablement penser que les dispositifs ou les services seront utilisés aux fins ou dans le cadre de l'exercice des droits prévus par le présent traité sans que celui-ci soit autorisé par le titulaire des droits ou par la loi.
2) Les Parties contractantes doivent prévoir des sanctions appropriées et efficaces contre les actes illégaux visés à l'alinéa 1).
3) Dans le présent article, l'expression "dispositif de neutralisation de la protection"s'entend de tout dispositif, produit ou composant incorporé dans un dispositif ou un produit ayant essentiellement pour objet ou pour effet de déjouer tout procédé, traitement, mécanisme ou système destiné à prévenir ou empêcher tout acte auquel s'appliquent les droits prévus par le présent traité.

L'article 11 du WCT, intitulé "Obligations relatives aux mesures techniques", est libellé comme suit :

> "*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 ou de la Convention de Berne et qui restreignent l'accomplissement, à l'égard de leurs œuvres, d'actes qui ne sont pas autorisés par les auteurs concernés ou permis par la loi.*"[26]

L'article 18 du WPPT reprend en grande partie ces termes.

Ces deux articles laissent aux parties contractantes une marge de manœuvre importante s'agissant de déterminer les moyens de donner effet à ces obligations. Il suffit que la protection juridique soit "appropriée" et que les sanctions soient "efficaces". Il ne s'agit pas d'empêcher tout type d'acte de contournement. En particulier, les textes n'interdisent pas aux parties contractantes de prévoir des exceptions et limitations appropriées aux mesures de protection et aux sanctions juridiques, pour autant que ces dérogations ne sapent pas la protection envisagée par les parties contractantes pour "les mesures techniques efficaces".

Quelles sont donc les obligations imposées par l'article 11? Premièrement, faut-il interdire à la fois l'acte de contournement et le trafic de dispositifs et de services de contournement? Bien que le libellé soit ambigu, il se prête à l'interprétation selon laquelle il vise plus l'acte de contournement que les dispositifs, comme la proposition de base. Néanmoins, l'interdiction des techniques seules peut être admise étant donné qu'elle peut constituer un moyen (ou un moyen supplémentaire) d'empêcher efficacement de tels actes de contournement.

Deuxièmement, l'article 11 interdit seulement le contournement des mesures techniques "efficaces". Une mesure n'a toutefois pas besoin d'être complètement "efficace" pour bénéficier de la protection prévue par l'article 11; si elle était complètement efficace, il est évident qu'aucune interdiction légale contre son contournement ne serait nécessaire, puisqu'elle serait, par définition, immunisée contre tout contournement.

Troisièmement, l'article 11 traite des mesures appliquées en rapport avec l'exercice des droits d'auteur prévus par la Convention de Berne et le WCT. Dans la mesure où un moyen technique est employé par un auteur aux fins de l'exercice de droits qui vont au-delà de ceux accordés par la Convention de Berne (par exemple, lorsque les utilisations entrent dans le cadre des limitations ou exceptions au droit d'auteur, telles que l'usage loyal), on peut penser que l'article 11 n'impose pas aux parties contractantes l'obligation d'interdire les actes de contournement en rapport avec une telle utilisation.

Quatrièmement, les mesures techniques qui portent seulement sur le "contrôle de l'accès", et non sur le contrôle du respect du droit d'auteur, bénéficient-elles de la protection prévue par l'article 11, sachant qu'aucun droit d'accès n'est expressément mentionné dans la Convention de Berne? Il a également été avancé que, puisque les auteurs peuvent autoriser l'accès à leurs œuvres et qu'ils le font, et qu'une mesure de contrôle d'accès peut "restreindre" efficacement les accès non autorisés, la dernière disposition de l'article 11

---

[26] Article 11 du Traité de l'OMPI sur le droit d'auteur (adopté le 20 décembre 1996).

s'applique aussi à ces mesures techniques (en plus des mesures qui donnent effet au contrôle du respect du droit d'auteur).

Quoi qu'il en soit, comme indiqué ci-dessus, l'article 11 n'interdit pas aux parties contractantes de prévoir pour les mesures techniques une protection qui va au-delà des dispositions des traités de l'OMPI. En outre, les traités de l'OMPI autorisent les parties contractantes à utiliser les sanctions juridiques existantes contre le contournement des mesures techniques, y compris dans le cadre de la gestion numérique des droits. À cet égard, l'article 11 du WCT et l'article 18 du WPPT n'imposent pas l'adoption d'une nouvelle législation anticontournement, et plusieurs États ont considéré depuis que leur régime juridique existant répondait de manière appropriée et efficace aux obligations découlant des traités de l'OMPI.

3.1.1.2 Information sur le régime des droits

Les traités de l'OMPI établissent également des normes pour la protection de l'information sur le régime des droits. L'information sur le régime des droits désigne les informations permettant d'identifier l'œuvre, l'auteur de l'œuvre, le titulaire de tout droit sur l'œuvre ou des informations sur les conditions et modalités d'utilisation de l'œuvre, et tout numéro ou code représentant ces informations.

L'article 12 du WCT et l'article 19 du WPPT imposent aux parties contractantes l'obligation de prévoir des "sanctions juridiques appropriées et efficaces" contre deux types d'actes. Les personnes qui accomplissent des actes dont elles savent (ou ont des raisons de penser) qu'ils vont entraîner, permettre, faciliter ou dissimuler une atteinte à un droit n'ont pas le droit :

– de supprimer ou modifier, sans y être habilitées, toute information relative au régime des droits se présentant sous forme électronique; ni

– de distribuer, importer aux fins de distribution, radiodiffuser ou communiquer au public, sans y être habilitées, des œuvres ou des exemplaires d'œuvres en sachant que des informations relatives au régime des droits se présentant sous forme électronique ont été supprimées ou modifiées sans autorisation.

3.1.1.3 L'environnement numérique

Le WCT a également consacré certains droits conférés aux auteurs, notamment le droit de distribution et le droit de communication au public, y compris "la mise à la disposition du public de leurs œuvres de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit de manière individualisée"[27]. Les titulaires de droits ont considéré qu'il était essentiel de jouir de ces droits pour tirer le meilleur parti des possibilités offertes par l'environnement numérique. Ces droits sont particulièrement importants pour la distribution de contenu sur l'Internet et d'autres vecteurs de diffusion numériques, tels que la télévision, la radiodiffusion et le câble. Pour répondre aux préoccupations de certains pays et de certains milieux d'utilisateurs, l'article 10 indique toutefois expressément que les parties contractantes peuvent prévoir des "limitations ou exceptions aux droits conférés aux auteurs", à condition

[27] Article 6 (droit de distribution) et article 8 (droit de communication au public) du WCT.

qu'il s'agisse de "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"[28]. Il importe de préciser que la déclaration commune concernant l'article 10 indique clairement que les États membres peuvent "étendre de manière adéquate dans l'environnement numérique les limitations et exceptions" et "concevoir de nouvelles exceptions et limitations" adaptées à l'environnement numérique[29]. On trouvera plus loin dans la section 3 et dans la section 5.1.2 un examen de la mesure dans laquelle les systèmes de gestion numérique des droits et les législations nationales ont concrétisé, sur les plans pratique et technique, les principes affirmés dans l'article 10 et la déclaration commune qui s'y rapporte.

3.1.2 Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (Accord sur les ADPIC)

3.1.2.1 Portée de l'Accord sur les ADPIC

L'Accord sur les ADPIC de l'Organisation mondiale du commerce (OMC) est un autre traité international d'une importance cruciale pour les titulaires de droits qui distribuent du contenu par des moyens de commerce électronique, y compris dans le cadre de systèmes de gestion numérique des droits. Signé en 1995, l'Accord sur les ADPIC fait partie intégrante des négociations commerciales entreprises pendant le cycle d'Uruguay de l'Accord général sur les tarifs et le commerce[30].

L'Accord sur les ADPIC est entré en vigueur le 1er janvier 1995. Il prévoit la protection et l'application de différents types de droits de propriété intellectuelle, notamment les droits d'auteur, les brevets, les marques et les secrets d'affaires. La partie II de l'Accord sur les ADPIC prévoit plus précisément pour les secteurs matériels de la propriété intellectuelle des normes minimales auxquelles les membres doivent adhérer. La partie III fixe des normes minimales concernant l'application interne des droits de propriété intellectuelle sur le territoire des membres. La partie V traite de la prévention et du règlement des différends, alors que la partie VI contient certaines dispositions transitoires[31]. D'une manière générale, l'Accord sur les ADPIC impose également l'application du traitement national (par un État membre à l'égard des ressortissants d'autres États) et de la clause de la nation la plus favorisée (interdisant la discrimination entre les ressortissants d'autres États membres).

En ce qui concerne la partie II, l'Accord sur les ADPIC incorpore par renvoi, en les élargissant dans une certaines mesure, les dispositions matérielles de protections requises par la Convention de Berne sur le droits d'auteur, la Convention de Paris pour la protection de la propriété industrielle et d'autres instruments. Il s'agit de normes minimales, de sorte que les membres sont entièrement libres de prévoir une protection plus forte pour la propriété

---

28 *Id.*, article 10.

29 *Id.,* déclaration commune concernant l'article 10.

30 *Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce*, disponible à l'adresse *http://www.wto.org*.

31 Parmi les dispositions transitoires figurent les calendriers de mise en conformité totale avec l'Accord sur les ADPIC. Les pays développés devaient être en pleine conformité avec l'accord au 1er janvier 1996. Les pays en développement bénéficiaient d'un délai de cinq ans, jusqu'au 1er janvier 2000. Les pays les moins avancés avaient 10 ans pour le faire, soit jusqu'au 1er janvier 2005.

intellectuelle. Quant à la partie III, l'Accord sur les ADPIC impose aux États membres de se conformer aux procédures d'application des droits de propriété intellectuelle, y compris les procédures et sanctions civiles et administratives, le droit des titulaires d'obtenir des mesures conservatoires contre les auteurs d'atteintes présumées et les conditions spéciales relatives aux mesures à la frontière et aux procédures pénales.

Bien que l'Accord sur les ADPIC établisse un socle juridique international commun important pour la protection du droit d'auteur et d'autres titres de propriété intellectuelle, et l'application de ces droits sur le plan interne, l'accord a été en grande partie négocié en décembre 1991, et il est entré en vigueur avant les traités de l'OMPI. À cet égard, certains commentateurs ont fait observer que l'Accord sur les ADPIC ne tient pas suffisamment compte des questions de propriété intellectuelle soulevées par la distribution numérique du contenu, en particulier sur l'Internet, et que la protection des systèmes de gestion numérique des droits prévue par les traités de l'OMPI n'est pas couverte par l'accord[32]. Une grande partie du débat sur la distribution électronique s'est toutefois écartée de la question fondamentale des normes de protection du droit d'auteur prévues par l'Accord sur les ADPIC pour se reporter sur les enjeux de l'environnement numérique et la question plus récente de la protection des mesures techniques contre le contournement, qui est prise en considération dans les traités de l'OMPI. Ainsi, on a pu dire que les traités de l'OMPI ont été motivés en partie par la nécessité de combler les "lacunes" de l'Accord sur les ADPIC et des conventions de Berne et de Rome[33].

3.1.2.2 Programme de travail de l'Organisation mondiale du commerce (OMC) sur le commerce électronique

À l'OMC, l'opportunité et les moyens d'intégrer l'interdiction du contournement des systèmes de gestion numérique des droits et d'autres mesures techniques dans l'Accord sur les ADPIC ont toutefois été pris en considération. Ces discussions ont eu lieu dans le contexte du programme de travail plus large de l'OMC sur le commerce électronique (ci-après dénommé "programme de travail"), qui a été lancé par une déclaration à la conférence ministérielle de mai 1998, selon laquelle le Conseil général devait établir un programme de travail global pour examiner "toutes les questions liées au commerce qui se rapportent au commerce électronique mondial"[34]. Le programme de travail a été établi le 25 septembre 1998 pour les organes pertinents de l'OMC, dont le Conseil des droits de propriété intellectuelle qui touchent au commerce (ci-après dénommé "Conseil des ADPIC"). Parmi les questions soumises à l'examen du Conseil des ADPIC figurent la protection du

---

32 Voir S. Baker, P. Lichtenbaum, M. Shenk et M. Yeo, *E-Products and the WTO*, 35 *The International Lawyer* 5, 20 (2001).

33 Voir le paragraphe 28 de la communication de l'Australie, intitulée *Electronic Commerce Work Programme*, document IP/C/W/233 de l'OMC (7 décembre 2000). Voir également *Electronic Commerce Work Programme : Background Note by the Secretariat*, paragraphe 75 du document IP/C/W/128 de l'OMC (février 10, 1999) (les mesures techniques n'ont pas été examinées dans des négociations sur les ADPIC et l'Accord sur les ADPIC ne contient aucune disposition spécifique sur ces mesures) [ci-après dénommée "note d'information"].

34 *Déclaration sur le commerce électronique mondial*, document WT/MIN(98)/DEC/2 de l'OMC (25 mai 1998).

droit d'auteur et des droits connexes et les moyens de faire respecter ces droits, ainsi que les nouvelles technologies et l'accès à la technologie[35].

Comme indiqué par le secrétariat du Conseil des ADPIC dans une note d'information datée du 10 février 1999, la question est de savoir si, dans l'environnement des réseaux numériques, les normes de l'Accord sur les ADPIC assurent une "protection efficace et appropriée des droits de propriété intellectuelle"[36]. La note d'information passe expressément en revue les questions abordées par les traités de l'OMPI, telles que la définition de la "publication" et la portée des droits de reproduction et communication au public dans un environnement en ligne. Il convient de préciser que la note d'information souligne l'importance des mesures techniques pour la protection contre la copie, le cryptage et le tatouage, et l'utilité de l'information sur la gestion électronique des droits, qui dépendent des mesures de protection juridique prévues dans les traités de l'OMPI[37]. La note d'information traite en détail des activités de l'OMPI, y compris les deux traités de l'OMPI et les incidences du commerce électronique sur la propriété intellectuelle[38].

La note d'information a favorisé une plus grande prise en considération de ces questions par le Conseil des ADPIC, ainsi que des contributions des membres de l'OMC et une présentation par un représentant de l'OMPI concernant les activités en cours dans son organisation. Les membres de l'OMC ont présenté au Conseil des contributions concernant la poursuite des travaux. L'une de ces suggestions visait à étudier l'opportunité d'adapter ou de préciser l'Accord sur les ADPIC lui-même pour tenir compte du progrès technique, et en particulier de l'utilisation de systèmes de gestion numérique des droits. D'autres contributions, en revanche, indiquaient qu'il était préférable de ne pas reproduire à l'OMC les travaux en cours à l'OMPI. Dans ses rapports de situation de juillet 1999 et de décembre 2000, le Conseil des ADPIC a exposé l'opinion générale de ses membres, à savoir que les questions touchant à la propriété intellectuelle qui se posent en rapport avec le commerce électronique sont tellement nouvelles et complexes que la communauté internationale doit les examiner plus avant pour mieux comprendre ce qui est en jeu et que l'OMC devrait continuer d'examiner l'évolution de la situation dans ce domaine, y compris les travaux complémentaires réalisés par l'OMPI[39]. Par la suite, toujours à l'OMC, la *Déclaration ministérielle* de Doha de novembre 2001 a pris acte des travaux en cours concernant le commerce électronique et demandé au Conseil général de rendre compte des arrangements institutionnels à mettre en œuvre pour poursuivre ces travaux à la cinquième session de la conférence ministérielle[40], prévue en septembre 2003.

---

35 Paragraphe 4.1 du *Programme de travail sur le commerce électronique*, WT/L/274 (30 septembre 1998).

36 Paragraphe 14 de la note d'information.

37 Paragraphes 75 et 76 de la note d'information.

38 *Id.,* paragraphes 80 à 92.

39 *Programme de travail sur le commerce électronique : Rapport de situation au Conseil général*, document IP/C/18 de l'OMC (30 juillet 1999); *Programme de travail sur le commerce électronique : Rapport du situation du Président au Conseil général*, document IP/C/20 de l'OMC (4 décembre 2000).

40 *Déclaration ministérielle*, document WT/MIN(01)/DEC/1 de l'OMC, paragraphe 34 (20 novembre 2001).

3.2 États-Unis d'Amérique

3.2.1 Cadre juridique

En octobre 1998, les États-Unis d'Amérique ont mis en œuvre les dispositions anticontournement des traités de l'OMPI dans le titre I du Digital Millennium Copyright Act (loi sur le droit d'auteur à l'ère du numérique) (ci-après dénommé "DMCA")[41]. D'autres lois fédérales et étatiques peuvent aussi protéger les techniques de gestion numérique des droits contre leur contournement illicite ou les titulaires de droits dont les œuvres sont utilisées sans leur autorisation.

Aux États-Unis d'Amérique, la protection juridique des techniques de gestion numérique des droits découle d'une interaction délicate entre les accords utilisés par le secteur privé pour céder sous licence les techniques de protection du contenu et l'action des pouvoirs public, y compris les lois fédérales et étatiques et la réglementation fédérale. La vue dominante aux États-Unis d'Amérique depuis le milieu des années 90 consiste à privilégier les solutions du secteur privé découlant, dans la mesure du possible, de négociations sectorielles. Ces solutions permettent aux titulaires de droits de s'appuyer sur des clauses contractuelles de protection et de sanctions pour lutter contre les produits qui ne se conforment pas à la norme convenue en matière de protection du contenu. Cette interaction, et ces arrangements contractuels, sont examinés en détail dans un document rédigé à l'origine pour l'OMPI par Dean S. Marks et Bruce H. Turnbull, intitulé "Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses"[42].

Pour récapituler les conclusions de cet exposé, de nombreux contrats de licence de techniques de protection du contenu dans le secteur privé prévoient des clauses spécifiques de protection de contenu tel que des films ou de la musique à l'entrée dans l'environnement familial et dans les réseaux personnels. Comme indiqué dans le document, ces accords contiennent :

– des règles de codage, qui définissent à quel moment le titulaire des droits peut "coder" le contenu pour en limiter la copier ou la redistribution;

– des règles de conformité, qui définissent les sorties vers lesquelles le contenu protégé peut être réorienté;

– des règles de fiabilité, qui définissent les normes de construction des produits pour résister au contournement de leurs éléments de protection contre la copie.

Bien qu'un examen détaillé de ces contrats dépasse le cadre de la présente étude, ils comprennent les éléments suivants : la Digital Transmission Content Protection ("DTCP") de la SARL Digital Transmission Licensing Administrator ("DTLA"); la High-bandwidth Digital Content Protection ("HDCP") de la SARL Digital Content Protection; la Content Protection For Prerecorded Media ("CPPM") et la Content Protection for Recordable Media

---

41 Loi de 1998 portant mise en œuvre du Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes, titre I du Digital Millennium Copyright Act (codifié au chapitre 12 du titre 17 du Code des États-Unis d'Amérique).

42 Document WCT-WPPT/IMP/3 de l'OMPI (3 décembre 1999) ["Marks/Turnbull"], disponible à l'adresse *http://www.wipo.int/eng/meetings/1999/wct_wppt/pdf/imp99_3.pdf*. Réédité dans 22 E.I.P.R. 198 (2000).

("CPRM") de la SARL 4C Entity; et le Content Scramble System ("CSS") de la DVD Copy Control Association, Inc. ("DVD CCA")[43].

Lorsque les lacunes dans la protection du contenu ne peuvent pas être comblées au moyen d'arrangements privés de ce type, les groupes d'industries aux États-Unis d'Amérique ont décidé de saisir les pouvoirs publics. Bien entendu, lorsque la conformité s'impose au niveau intersectoriel, l'action gouvernementale semble aller de soi. En outre, il arrive fréquemment que les solutions contractuelles soient inexistantes ou inefficaces, par exemple lorsque les techniques de gestion numérique des droits pourraient être neutralisées par des individus ou par des produits construits par des entités qui ne sont pas parties au contrat. Dans de telles situations, seules les sanctions civiles et pénales prévues par loi sont appropriées[44].

3.2.1.1 DMCA

3.2.1.1.a) Historique

La procédure législative et l'adoption du projet de loi qui est devenu le DMCA ont donné lieu aux débats les plus intenses – tant dans les salles du Congrès que sur la place publique – sur la législation de propriété intellectuelle des États-Unis d'Amérique depuis la loi de 1976 sur le droit d'auteur. D'un côté – favorables à une mise en œuvre large et cohérente des prescriptions des traités de l'OMPI – se tenaient les titulaires de droits sur les œuvres, c'est-à-dire principalement les industries cinématographique, de l'enregistrement et de l'édition. De l'autre, appelant à la prudence, à la mesure et à des exceptions plus larges aux interdictions frappant le contournement, se trouvaient les sociétés de haute technologie telles que des sociétés d'informatique et d'électronique grand public, ainsi que des représentants des utilisateurs, notamment des bibliothèques, des établissements d'enseignement et des organismes de défense des consommateurs. Le DMCA a fait l'objet de nombreuses critiques de la part de ces groupes, que ce soit à l'époque ou plus récemment.

Diverses commissions du Congrès, chacune avec sa perspective particulière, ont été impliquées dans le débat législatif. Les questions ci-après figurent parmi les plus significatives des nombreuses questions examinées par le Congrès :

– la question de savoir si le DMCA devait interdire les instruments (et les services) de contournement[45], ou seulement les actes de contournement;

– la question de savoir si le contournement d'une mesure technique pour favoriser l'accomplissement d'un acte non illicite, tel qu'un usage loyal, devait être autorisé;

– la question de savoir si des activités légitimes, telles que l'ingénierie inverse et l'essai des systèmes de cryptage, devaient être interdites;

---

43 *Id.*

44 *Id.* Ce point est traité de manière plus détaillée dans la section 5.2.3, qui porte sur le rôle du gouvernement dans l'établissement de normes de gestion numérique des droits.

45 En définitive, le concept d'instruments de contournement a été incorporé dans l'expression "technique, produit, service, dispositif, composant ou partie de ces éléments" qui figure à l'article 1201.a)2) et b.1), du titre 17 du Code des États-Unis d'Amérique.

– la question de savoir si des instruments qui sont licites aux termes de la réglementation en vigueur sur les atteintes indirectes au droit d'auteur devaient être interdits parce qu'ils sont conçus pour neutraliser les mesures techniques;

– la question de savoir si le DMCA devait interdire seulement les "boîtes noires" conçues pour le contournement, et non les produits informatiques, d'électronique grand public et de télécommunications ordinaires;

– la question de savoir si le DMCA devait définir les "mesures techniques" dont la neutralisation était interdite; et

– la mesure dans laquelle le DMCA représentait une transition vers une "société de paiement à l'utilisation", limitant l'accès aux seules œuvres sous forme codée.

3.2.1.1.b) Les dispositions anticontournement

À haut niveau, les dispositions anticontournement du DMCA, qui donnent effet à l'article 11 du WCT et à l'article 18 du WPPT, tissent une matrice d'interdictions :

	Acte de contournement	**Instruments de contournement**
Mesure technique de contrôle d'accès	Interdit (art.1201.a)1))	Interdits (art. 1201.a)2))
Mesure technique de protection du droit d'auteur	Non interdit (par le DMCA)	Interdits (art. 1201.b))

Comme nous l'avons déjà indiqué, on peut considérer que les traités de l'OMPI exigent seulement une protection appropriée et efficace contre les *actes* de contournement et seulement à l'égard des mesures utilisées pour protéger l'exercice par les auteurs des *droits d'auteur* qui leur sont reconnus par la Convention de Berne, le WCT et le WPPT. Toutefois, le DMCA va au-delà des exigences minimales des traités de l'OMPI en interdisant à la fois les actes et les produits ayant pour fin le contournement et à l'égard des mesures techniques de "contrôle d'accès" et de "protection du droit d'auteur" utilisées pour protéger les œuvres.

Article 1201.a) : cet article interdit les actes et les produits ayant pour fin le contournement des mesures techniques de contrôle d'accès. La définition du "contournement" est vaste. Elle comprend le désembrouillage, le décryptage ou "tout autre procédé visant à éviter, contourner, supprimer, désactiver ou altérer une mesure technique sans l'autorisation du titulaire du droit d'auteur"[46].

Le DMCA ne définit pas le terme "mesure technique". En revanche, il définit si une mesure technique "contrôle efficacement l'accès à une œuvre" : l'accès est contrôlé "si la mesure, dans son fonctionnement ordinaire, suppose l'application d'informations, d'un processus ou d'un traitement, avec le consentement du titulaire du droit d'auteur, pour accéder à l'œuvre"[47]. L'histoire législative du DMCA donne à penser que le Congrès avait considéré que le cryptage et l'authentification feraient partie des mesures techniques de contrôle de

[46] Article 1201.a)3)A) du titre 17 du Code des États-Unis d'Amérique.
[47] Article 1201.a)3)B).

l'accès aux œuvres, tout en adoptant une définition suffisamment large pour tenir compte d'éventuelles innovations.

Parmi les diverses mesures techniques dont les tribunaux et le Librarian of Congress (conservateur de la bibliothèque du Congrès) ont déterminé qu'elles contrôlaient effectivement l'accès aux œuvres figurent : les séquences d'authentification permettant de vérifier que le contenu a bien été diffusé sur un lecteur autorisé; le CSS, qui est utilisé pour protéger les DVD vidéo contre l'accès non autorisé; les codes régionaux utilisés sur les DVD vidéo pour les rendre lisibles dans certaines régions seulement; et les codes régionaux appliqués aux jeux vidéo.

Article 1201.a)1) : cet article interdit le contournement des mesures techniques qui "contrôlent efficacement l'accès à une œuvre". Cette disposition rend purement et simplement illégal tout acte de contournement, même accompli à des fins rigoureusement licites et autorisées par la loi sur le droit d'auteur. Au cours de l'examen du DMCA, l'une des questions les plus controversées a porté sur l'opportunité de prévoir expressément une exception au titre de "l'usage loyal" (ou de tout autre principe similaire). Le Congrès a finalement conclu qu'aucune exception de cette sorte ne devrait être prévue et que le contournement, même aux fins d'un usage loyal, était illicite.

Toutefois, un certain compromis a été ménagé pour tenir compte des préoccupations relatives aux incidences de cette interdiction. Tout d'abord, la date d'entrée en vigueur de cet article a été repoussée de deux ans, soit jusqu'au 28 octobre 2000. Il s'agissait de permettre au Librarian of Congress, sur recommandation du Directeur de l'enregistrement des droits d'auteur, d'entreprendre une étude pour déterminer si cette interdiction aurait des "conséquences regrettables" pour les utilisateurs d'œuvres protégées s'agissant d'utiliser de manière licite certaines classes d'œuvres. Ensuite, le DMCA impose au Librarian of Congress de réaliser la même étude tous les trois ans par la suite. Cette procédure réglementaire, les conclusions du Librarian of Congress en 2000 et l'étude en cours (qui doit être achevée courant 2003) sont décrites à la section 3.2.1.3.a).

D'autre part, en interdisant le contournement des mesures techniques de contrôle d'accès aux œuvres, le DMCA aurait indirectement créé pour les titulaires de droits un nouveau "droit d'accès" à leurs œuvres; quoi qu'il en soit, il est certain que l'exercice de ce nouveau droit est expressément subordonné à l'utilisation d'une mesure technique. Un tel droit d'accès n'est prévu ni dans la Convention de Berne ni dans le WCT.

Les bibliothécaires et d'autres utilisateurs ont fait valoir que ce nouveau droit – en l'absence d'un droit de contournement au titre de l'usage loyal – conduirait inexorablement à une nouvelle société de "paiement à l'utilisation". Ils ont souligné que l'avenir serait radicalement différent du monde traditionnel des copies tangibles, où l'utilisateur qui achète un livre ou un disque peut en profiter autant de fois qu'il le souhaite sans devoir payer de nouveau à chaque utilisation. Dans cette perspective, l'équilibre des intérêts entre les titulaires de droits et les utilisateurs garanti dans la loi sur le droit d'auteur des États-Unis d'Amérique était ou serait remis en cause.

Les titulaires de droits ont répondu à ces préoccupations en soulignant que le contrôle de l'accès pouvait favoriser l'émergence de modèles de distribution susceptibles de répondre à un plus large éventail de préférences des consommateurs. En effet, les utilisateurs pourraient bien préférer payer pour une utilisation unique, plutôt que d'acheter le droit d'utiliser à plusieurs reprises un exemplaire commercialisé à un prix sans doute plus élevé.

Ils font également valoir que, s'il existe un marché pour un type particulier d'utilisation, ils feront tout pour répondre à cette demande.

Article 1201.a)2) : cet article interdit la fabrication, la vente, la mise à la disposition du public ou la fourniture (c'est-à-dire, le "trafic") de toute technique, produit, service, dispositif, composant, ou partie de ceux-ci (c'est-à-dire, tout "instrument") destiné à contourner une mesure technique de protection. Il convient de noter que même si une telle technologie dans son ensemble ne viole pas l'interdiction législative, n'importe quel élément – voire toute partie d'élément – peut être interdit. Toutefois, pour être interdit, un tel instrument doit remplir au moins l'une des trois conditions suivantes :

– être "principalement conçu ou produit pour contourner la mesure technique qui contrôle efficacement l'accès à une œuvre"[48] ;

– avoir "une destination ou une utilisation commercialement limitée en dehors du contournement d'une mesure technique qui contrôle efficacement l'accès à une œuvre"[49] ; ou

– être "commercialisé par une personne, ou un tiers agissant de concert avec elle, qui possède les connaissances requises pour contourner une mesure technique qui contrôle efficacement l'accès à une œuvre"[50].

Ces trois critères indépendants étaient controversés à l'époque de l'adoption du DMCA et le restent aujourd'hui. En particulier, le critère selon lequel l'instrument doit être "principalement conçu ou produit aux fin de contournement s'écarte considérablement du critère établi par la Cour suprême des États-Unis d'Amérique en 1984, dans une affaire portant sur la légalité du magnétoscope à cassettes Betamax de Sony. La Cour suprême a considéré que la responsabilité indirecte de Sony ne pouvait être engagée au titre des pratiques des utilisateurs de Betamax en matière d'enregistrement à domicile, étant donné que le caméscope, comme d'autres articles courants du commerce, pouvait remplir des fonctions commercialement significatives ne portant pas atteinte au droit d'auteur[51]. Le DMCA interdit toutefois purement et simplement les instruments (dans la mesure où ils neutralisent des mesures techniques) en fonction de l'objectif principal de leur conception ou de leur production, indépendamment de la question de savoir s'ils peuvent être ou seront utilisés à des fins licites.

Pour répondre au tournant législatif en matière de responsabilité potentielle des fabricants pour leurs produits, le Congrès a adopté l'article 1201.c)3), examiné ci-après dans la section 3.2.1.1.c).

Un autre point d'incertitude concerne la signification des termes "principalement conçu ou produit". À cet égard, l'histoire législative du DMCA n'est pas claire. Toutefois, il semblerait que l'utilisation du terme "principalement" désigne uniquement le plus significatif des "objectifs"; il ne peut donc probablement exister qu'un seul objectif "principal". Un instrument de contournement, mais qui vise des objectifs multiples d'égale importance, ne saurait donc avoir été "principalement conçu ou produit" aux fins de contournement.

---

48 Article 1201.a)2)A).
49 Article 1201.a)2)B).
50 Article 1201.a)2)C).
51 *Sony Corp* c. *Universal City Studios, Inc.*, 464 U.S. 417 (1984).

Article 1201.b) : cet article interdit seulement le trafic d'instruments de contournement des techniques de protection des droits d'auteur d'un titulaire sur une œuvre ou une partie de celle-ci. Pour être interdit, l'instrument doit remplir l'une au moins de trois conditions qui sont fondamentalement semblables à celles décrites ci-dessus[52]. Cet article définit également le contournement de la même manière que l'article 1201.a). Là encore, la mesure technique n'est pas définie, mais une telle mesure "protège efficacement le droit d'un titulaire de droits d'auteur" si, "dans son fonctionnement ordinaire, elle empêche, restreint, ou limite d'une autre manière l'exercice d'un droit [d'auteur] conféré à un titulaire". En d'autres termes, si une mesure technique est utilisée pour empêcher une reproduction non autorisée, une distribution, une exécution ou une exposition publique non autorisées – c'est-à-dire, une "utilisation" non autorisée du droit d'auteur – l'instrument de contournement est interdit (à condition que l'un des trois critères, comme celui de "l'objectif principal de la conception ou de la production", soit rempli).

Il convient de noter que le DMCA n'interdit pas l'acte de contournement d'une mesure technique qui protège le droit exclusif d'un titulaire de droits d'auteur d'autoriser l'utilisation d'une œuvre. Le congrès a considéré qu'il n'était pas nécessaire que le DMCA lui-même interdise l'acte de contournement, afin de réaliser une copie d'une œuvre, par exemple, parce que, dans la plupart des cas, l'acte final – c'est-à-dire, la copie non autorisée – porterait atteinte au droit d'auteur. En conséquence, le titulaire des droits pourrait se prévaloir de la loi sur le droit d'auteur et le défendeur pourrait invoquer toutes les exceptions et limitations prévues par cette loi.

3.2.1.1.c) Limitations et exceptions

Le DMCA fourmille de limitations et exceptions qui traduisent à la fois l'intensité exceptionnelle des débats qui ont eu lieu au Congrès et les intérêts de groupes particuliers. Certaines d'entre elles parmi les plus importantes sont passées en revue ci-après.

Lien avec les atteinte au droit d'auteur, y compris l'usage loyal : il est indiqué dans le DMCA que l'article 1201 est sans effet sur les "droits, voies de recours, limitations ou exceptions aux atteintes au droit d'auteur, y compris l'usage loyal"[53]. Superficiellement, cette disposition pourrait être interprétée comme protégeant les activités qui relèvent de l'usage loyal. Néanmoins, ainsi qu'il ressort clairement de l'interprétation des tribunaux, tous les droits et exceptions prévus par la loi sur le droit d'auteur sont indépendants des nouveaux droits, recours et exceptions prévus dans les dispositions anticontournement : on ne saurait donc contester un argument avancé en vertu de l'article 1201.a)1) en arguant du fait que le contournement a été effectué aux fins d'une activité parfaitement licite et loyale[54].

Lien avec les atteintes au droit d'auteur indirectes ou du fait d'autrui : le DMCA porte que l'article 1201 "n'élargit ni ne restreint" en rien "la responsabilité indirecte ou du fait d'autrui" pour les atteintes au droit d'auteur à l'égard de telle ou telle technologie[55]. Ce libellé est toutefois sans grand intérêt étant donné que, comme indiqué ci-dessus, si un produit viole les dispositions de l'article 1201.a)2) ou de l'article 1201.b), cette violation peut donner

---

52 Article 1201.b)1)A) à C) du titre 17 du Code des États-Unis d'Amérique.
53 Article 1201.c)1).
54 Voir la section 3.2.2 (*Universal City Studios, Inc.* c. *Corley*).
55 Article 1201.c)2) du titre 17 du Code des États-Unis d'Amérique.

lieu à des poursuites – en vertu de l'article 1201 – indépendamment de la question de savoir si le produit contribue à l'atteinte au droit d'auteur.

Clause d'exemption pour le matériel courant : en réponse aux préoccupations des fabricants de produits informatiques, électroniques et de télécommunications grands publics, qui craignaient que leurs produits ne puissent être considérés comme contrevenant à l'article 1201, le DMCA prévoit qu'il n'est pas nécessaire que leurs produits licites soient conçus, ou que les pièces et les composants de ces produits soient conçus ou sélectionnés, "de manière à réagir à telle ou telle mesure technique"[56]. Cette disposition est généralement désignée sous le nom de "clause d'exemption" (no mandate) car elle signifie que ces produits ne sont pas tenus de réagir à une mesure technique pour éviter des poursuites en vertu des dispositions anticontournement; en d'autres termes, seuls les actes de contournement (et non la réaction à une mesure technique) sont contraires à l'article 1201.

Les fabricants ne peuvent toutefois se prévaloir cette disposition que pour autant que le produit, la partie ou le composant "ne tombe pas d'une autre manière sous le coup des interdictions" prévues dans cet article. Bien que la signification de cette réserve ne soit pas tout à fait claire, l'historique de l'adoption de la loi milite en faveur d'une interprétation selon laquelle un produit doit être considéré dans son intégralité pour déterminer pourquoi il n'a pas réagi à une mesure, que ce soit pour une raison légitime de conception ou dans un but illicite de contournement. Le libellé lui-même donne à penser qu'un fabricant ne pourra invoquer cette disposition lorsque telle ou telle fonction du produit consiste effectivement à contourner ou neutraliser une mesure technique.

Outre ces limitations, l'article 1201 prévoit d'autres exceptions spécifiques. Les traités de l'OMPI n'interdisent pas aux parties contractantes de prévoir des exceptions à l'interdiction générale du contournement. La condition selon laquelle les sanctions juridiques doivent être "appropriées" et "efficaces" implique toutefois la possibilité de peser les avantages et les inconvénients de l'interdiction du contournement, pour les titulaires de droits et les utilisateurs, dans les pays où ces traités doivent être mis en œuvre. C'est précisément ce qui s'est passé au Congrès, qui a adopté sept exceptions, qui sont néanmoins largement considérées comme très restreintes et spécialisées. Elles seraient en effet inapplicables dans la plupart des cas. Toutes ces exceptions sont applicables à l'acte de contournement du contrôle de l'accès, mais cinq d'entre elles seulement aux dispositions interdisant le trafic des techniques de contournement.

---

[56] Article 1201.c)3). Un autre article important du DMCA prévoit expressément la nécessité de réaction dans un cas particulier : essentiellement, tous les magnétoscopes analogiques doivent être conformes à certains procédés analogiques de protection contre la copie de Macrovision Corp (article 1201.k). Dans le cadre du compromis entre les fabricants de ces appareils et les titulaires de droits, cette disposition contient expressément des règles de codage, qui prévoient que ces techniques anticopie ne peuvent être appliquées aux émissions de télévision radiodiffusées par voie hertzienne; elles peuvent toutefois être employées pour restreindre la copie 1) de copies d'émissions de télévision par abonnement; 2) d'émissions de télévision à paiement sélectif ou à la demande, ou de programmes enregistrés; ou 3) de copies de ces émissions ou programmes (article 1201.k)2)).

Ces sept exceptions sont les suivantes :

– Bibliothèques, services d'archives et établissements d'enseignement publics[57] : ces établissements, s'ils sont ouverts au public ou aux personnes non affiliées à la bibliothèque, peuvent contourner une mesure de protection uniquement pour accéder à une œuvre afin de déterminer de bonne foi s'ils souhaitent en faire l'acquisition. L'accès n'est autorisé que le temps nécessaire pour décider s'il y a lieu de se procurer un exemplaire licite. Tout contournement à des fins commerciales ou financières est interdit.

– Organes d'application des lois, services de renseignement et autres organismes gouvernementaux[58] : les activités relatives à la sécurité nationale et à l'application des lois, y compris les activités relatives à la sécurité de l'information, lorsqu'elles sont dûment autorisées, ne sont pas soumises aux interdictions relatives aux actes de contournement et au trafic de techniques énoncées aux articles 1201.a) et 1201.b). Elles ne tombent pas non plus sous le coup des dispositions de l'article 1202, qui sont décrites dans la section 3.2.1.1.d) ci-après[59].

– Ingénierie inverse de programmes d'ordinateur[60] : l'ingénierie inverse de programmes d'ordinateur – et uniquement de programmes d'ordinateur - par une personne qui s'est procurée de manière licite une copie du programme est autorisée (nonobstant le contrôle d'accès), sous réserve d'une série de conditions. Premièrement, le contournement doit avoir pour "seul objectif" l'identification et l'analyse des éléments de programme "nécessaires pour réaliser l'interfonctionnement" avec un "programme informatique créé de manière indépendante". Deuxièmement, ces éléments de programme ne doivent pas avoir été préalablement "aisément accessible" à l'auteur du contournement. Troisièmement, les activités ne doivent pas être constitutives d'atteinte par elles-mêmes (d'une manière générale, selon la jurisprudence en vigueur aux États-Unis d'Amérique, la réalisation d'une reproduction en rapport avec une décompilation licite par ailleurs est considérée comme une utilisation licite)[61]. Par ailleurs, une personne peut "mettre au point et utiliser" des instruments de contournement à des fins licites. De plus, cette personne peut mettre à la disposition de tiers les informations obtenues par l'activité d'ingénierie inverse, mais uniquement pour permettre l'interfonctionnement.

– Recherche cryptographique[62] : la recherche cryptographique "de bonne foi" sur une mesure technique de contrôle d'accès est autorisée sous réserve de quatre conditions : 1) la personne qui se livre à ces recherches s'est procurée une copie de manière licite; 2) l'acte est nécessaire à la conduite de la recherche; 3) la personne s'est efforcée "de bonne foi" d'obtenir l'autorisation; et 4) l'acte n'est pas constitutif d'infraction ou de violation d'une autre loi. La recherche cryptographique est définie comme recouvrant "les activités nécessaires pour détecter et analyser les défauts et les failles des techniques de cryptage … pour faire progresser la technique … ou contribuer à la mise au point de produits de cryptage". Pour déterminer si l'exemption est applicable, le tribunal doit se demander si et comment les informations résultant de la recherche cryptographique ont été diffusées, si la

---

57 Article 1201.d).
58 Article 1201.e).
59 Article 1202.d).
60 Article 1201.f).
61 Voir *Sega Enterprises Ltd* c. *Accolade, Inc.*, 977 F.2d 1510, 1527-28 (9th Cir. 1992).
62 Article 1201.g) du titre 17 du Code des États-Unis d'Amérique.

personne concernée est habilitée à se livrer à la recherche cryptographique et si les résultats et les documents relatifs à la recherche sont communiqués au titulaire du droit d'auteur sur l'œuvre protégée par la mesure technique.

À l'époque de l'adoption de la loi, il a été considéré que les limitations et les conditions de cette exception restreindraient considérablement ses possibilités d'application et que la recherche cryptographique légitime pourrait être compromise par le DMCA. C'est pourquoi la loi impose qu'un rapport soit établi dans un délai d'un an sur les effets du DMCA sur la recherche cryptographique, sur l'adéquation et l'efficacité des mesures techniques et sur la protection des titulaires de droits d'auteur contre l'accès non autorisé aux œuvres cryptées[63]. Ce rapport, publié en juillet 1999 par le Directeur de l'enregistrement des droits d'auteur et le Secrétaire adjoint aux communications et à l'information, aboutissait à la conclusion selon laquelle nul n'avait détecté une quelconque incidence sur ces questions et que les inconvénients n'étaient pas prouvés, ce qui n'avait rien d'étonnant puisque l'interdiction des actes de contournement visée à l'article 1201.a)1) doit encore se concrétiser[64].

– Protection des mineurs[65] : cette exception prévoit qu'un tribunal, dans l'application à un composant ou à une partie des dispositions de l'article 1201.a) relatives à la lutte contre le trafic d'instruments de contournement, peut déterminer si l'exception à l'interdiction du contournement s'impose pour une technique qui "a pour seul objet d'empêcher l'accès des mineurs à du matériel publié sur l'Internet".

– Protection des données à caractère personnel[66] : cette exception, visant les témoins de connexion (cookies), autorise l'acte de contournement lorsque la mesure technique (ou l'œuvre qu'elle protège) recueille ou diffuse des données à caractère personnel réunies au cours des activités en ligne; lorsque cette collecte d'informations est opérée sans "signalisation évidente"; lorsque l'acte a pour "seul effet" de détecter et neutraliser cette fonction de collecte ou de diffusion; et que cet acte est effectué uniquement pour empêcher ces activités et ne contrevient pas d'une autre manière à la loi.

– Essai de sécurité[67] : cette exception permet à une personne de procéder à un essai de bonne foi de la sécurité d'un ordinateur, d'un système ou d'un réseau informatique, avec l'autorisation du propriétaire. Elle autorise l'acte de contournement et permet à la personne de mettre au point, distribuer et utiliser des moyens techniques à la seule fin d'essais de sécurité. Les actes sont autorisés uniquement s'ils ne sont pas constitutifs d'infraction et ne violent pas les dispositions d'une autre loi. Si un défendeur invoque cette exception, le tribunal doit examiner si les informations ont été utilisées "uniquement pour renforcer la sécurité du propriétaire" de l'ordinateur ou ont été partagées avec celui-ci et si elles ont été "utilisées ou conservées" afin de ne pas faciliter la réalisation d'infractions ou la violation de toute autre loi.

---

63 Article 1202.g)5).

64 Voir Register of Copyrights and Assistant Secretary for Communications and Information, *Report to Congress: Joint Study of Section 1201(g) of The Digital Millennium Copyright Act,* Part III (1999), à l'adresse *http://www.copyright.gov/reports/studies/dmca_report.html*.

65 Article 1201.h) du titre 17 du Code des États-Unis d'Amérique.

66 Article 1201.i).

67 Article 1201.j).

3.2.1.1.d) Information sur le régime des droits

À l'article 1202, le DMCA prévoit séparément la protection de "l'information sur le régime des droits". L'information sur le régime des droits est un élément clé pour l'efficacité de tout système de gestion numérique des droits, car c'est elle qui décrit l'œuvre et la manière dont elle peut être utilisée.

Le DMCA donne de l'information sur le régime des droits une définition relativement vague, qui couvre toutes les informations transmises avec une œuvre qui décrivent l'œuvre, notamment le titre, l'auteur, les données figurant dans la mention de réserve du droit d'auteur, le nom des artistes interprètes ou exécutants (dans certaines circonstances, non compris les interprétations ou exécutions publiques d'une œuvre retransmises par une station de radio ou de télévision, ni les œuvres audiovisuelles), le nom des auteurs, metteurs en scène et interprètes (dans une œuvre audiovisuelle, sauf en cas de radiodiffusion), les conditions d'utilisation, les numéros ou symboles d'identification et toute autre information prescrite par le Directeur de l'enregistrement des droits d'auteur[68].

L'article 1202 contient deux dispositions de fond. La première interdit la fourniture d'informations erronées sur le régime des droits et la diffusion ou l'importation de telles informations, lorsque la personne le fait en connaissance de cause et avec l'intention de "favoriser, permettre, faciliter ou dissimuler l'infraction"[69].

La seconde interdit à une personne non autorisée de supprimer ou de modifier intentionnellement l'information sur le régime des droits; ou de distribuer ou d'importer l'information sur le régime des droits tout en sachant qu'elle a été supprimée ou modifiée sans autorisation; ou de distribuer, d'importer ou d'exécuter publiquement une copie d'une œuvre ou une œuvre tout en sachant que l'information sur le régime des droits a été supprimée ou modifiée sans l'autorisation du titulaire du droit d'auteur. Les actes ci-dessus sont interdits lorsque la personne concernée sait ou a des raisons de penser que cette activité favorisera, permettra, facilitera ou dissimulera une infraction[70].

3.2.1.1.e) Recours

Le DMCA prévoit des sanctions civiles et pénales[71]. Parmi les sanctions civiles figurent la mise en demeure et la saisie, ainsi que l'imposition de dommages-intérêts pour le préjudice matériel et le préjudice moral. Les dommages-intérêts pour le préjudice moral peuvent, à la discrétion du tribunal, aller de 200 à 2500 dollars É.-U. par acte ou produit de contournement (pour les violations de l'article 1201) et de 2500 à 25 000 dollars É.-U. (pour l'article 1202). Les peines pécuniaires peuvent être majorées en cas de récidive ou minorées en cas d'atteinte commise de bonne foi. La responsabilité des bibliothèques, services d'archives et établissements d'enseignement publics ne peut être engagée pour des activités dont ils ignoraient le caractère illicite et aucune sanction pénale ne peut être imposée à leur encontre.

---

68 Article 1202.c).
69 Article 1202.a).
70 Article 1202.b).
71 Article 1204.

3.2.1.2 Autres lois/lois étatiques

Une grande variété de lois fédérales et étatiques assurent une protection contre le contournement des mesures techniques susceptibles d'être utilisées dans des systèmes de gestion numérique des droits. Elles sont brièvement passées en revue ci-après :

– Loi sur le droit d'auteur : lorsqu'un produit facilite les atteintes au droit d'auteur, notamment par la neutralisation d'un système de gestion numérique des droits pour permettre la copie non autorisée, une action pour atteinte au droit d'auteur peut être intentée contre le fabricant ou tout autre fournisseur du dispositif. Par conséquent, outre les poursuites intentées au titre de l'article 1201.b) du DMCA, ces derniers peuvent également voir leur responsabilité engagée du fait d'atteinte indirecte au droit d'auteur si le dispositif permet à l'utilisateur de porter directement atteinte au droit d'auteur ou s'il existe d'autres incitations à le faire. Le fabricant d'un "produit courant du commerce" – défini par la Cour suprême comme un produit susceptible "d'utilisations commerciales licites significatives" – n'est toutefois pas responsable d'atteinte indirecte au droit d'auteur[72].

– Loi TEACH : à la fin de 2002, le Congrès a promulgué la loi d'harmonisation sur la technologie, l'enseignement et le droit d'auteur, portant modification de la loi sur le droit d'auteur afin de tenir compte des moyens numériques d'enseignement à distance. La loi TEACH a élargi la portée des exceptions traditionnelles au droit exclusif du titulaire d'autoriser une représentation ou exécution publique en faveur des retransmissions dans des classes et des émissions pédagogiques[73]. Ces exceptions étaient liées aux moyens techniques existants et étaient devenues obsolètes avec l'apparition de l'Internet.

La loi TEACH autorise les transmissions en rapport avec l'enseignement en ligne, sous réserve de certaines conditions. L'une de ces conditions concerne l'obligation d'utiliser des mesures techniques de protection, telles qu'une protection par mot de passe pour permettre l'accès aux sites Web. Et lorsque la transmission numérique est utilisée pour diffuser le matériel, l'établissement doit mettre en œuvre des techniques de gestion numérique des droits susceptibles "d'empêcher raisonnablement" les étudiants de conserver les œuvres pendant une période excédant la durée de la session de cours et de rediffuser les œuvres[74].

La loi TEACH fait également obligation au Sous-Secrétaire au commerce pour la propriété intellectuelle, après consultation du Directeur de l'enregistrement des droits d'auteur, de présenter un rapport au Congrès sur les mesures techniques de protection des œuvres numériques et de prévention des atteintes au droit d'auteur. Ce rapport, qui donne une vue d'ensemble utile et de haut niveau de la question, a été présenté en décembre 2002[75]. Il recense plusieurs techniques de base utilisées pour la protection du contenu, telles que le cryptage, le tatouage numérique et les systèmes d'authentification et de gestion numérique des droits. Sur ce dernier point, le rapport traite de "l'informatique de confiance" et des "modèles de gestion et langages d'expression des droits" et passe en revue différents types d'architectures et de systèmes de gestion numérique des droits. Enfin, le rapport recense et décrit brièvement un large éventail d'entreprises, d'initiatives privées et volontaires menées

---

72 *Sony Corp.* c. *Universal City Studios, Inc.,* 464 U.S. 417, 442-43 (1984).

73 Article 110.2) du titre 17 du Code des États-Unis d'Amérique.

74 Article 110.2)d)ii).

75 Voir *Protection Systems for Digitized Copyrighted Works: A Report to Congress* (décembre 2002), à l'adresse *http://www.uspto.gov/web/offices/dcom/ olia/teachreport.pdf*.

par l'industrie, d'organismes de normalisation et d'organisation apparentées, ainsi que d'associations commerciales participant au développement, à la promotion et à la normalisation des techniques de gestion numérique des droits et d'autres mesures techniques de protection.

– Exonération de responsabilité des prestataires de services en ligne : la loi de limitation de la responsabilité pour les atteintes au droit d'auteur commises en ligne a été promulguée en 1998 en tant que partie intégrante du DMCA. Elle prévoit des clauses d'exonération de responsabilité au titre de différentes activités, telles que la transmission, la réalisation de copies dans la mémoire cache, la sauvegarde de matériel tiers et la fourniture de moteurs de recherche[76]. Ces exonérations ne sont toutefois applicables que si le prestataire de services se conforme à certaines conditions. L'une d'entre elles impose à celui-ci de "tenir compte des mesures techniques standard et de ne pas s'y opposer"[77]. Un prestataire de services qui modifierait son système ou ne l'adapterait pas à ces mesures ne serait pas spécifiquement sanctionné mais perdrait le bénéfice des exonérations.

C'est pourquoi, il n'est pas étonnant que la définition des "mesures techniques standard" repose sur des notions telles que le consensus et la facilité de mise en œuvre. Elle indique expressément que ces mesures - telles qu'elles sont utilisées par les titulaires de droits d'auteur pour identifier et protéger leurs œuvres – doivent "avoir été élaborées dans le cadre d'un processus de normalisation ouvert, équitable, volontaire et sectoriel découlant d'un large consensus parmi les titulaires de droits et les prestataires de services; être accessibles à des conditions raisonnables et non discriminatoires; et ne pas imposer des coûts importants aux prestataires de services ni surcharger leurs systèmes ou réseaux"[78]. Par contraste, l'article 1201 du DMCA ne contient pas de définition de la "mesure technique". À la différence des principes incorporés dans la définition de la " mesure technique standard", cet article protégerait des systèmes de gestion numérique commerciaux mis au point ou adoptés unilatéralement, qui coûtent cher ou qui peuvent exiger des efforts d'adaptation techniques conséquents – sauf dans la mesure où la mise en conformité du produit ne serait pas nécessaire compte tenu de la clause d'exemption.

– Loi sur l'enregistrement à domicile : la loi sur l'enregistrement à domicile adoptée en 1992 impose l'incorporation du système de régulation de la copie en série SCMS, ou d'un système aux fonctions équivalentes, dans tous les appareils d'enregistrement audionumérique fabriqués, importés ou distribués aux États-Unis d'Amérique[79]. Cette loi a pour but de contrôler la copier en série de la musique; il est possible de réaliser un nombre illimité de copies numériques de première génération d'un enregistrement, mais la fabrication d'autres copies numériques à partir de ces copies est techniquement impossible. La loi interdit également le trafic d'appareils ou la prestation de services qui ont pour "but ou effet principal" le contournement de tout programme ou circuit mettant en œuvre le SCMS (ou un système remplissant les mêmes fonctions)[80]; l'acte de contournement lui-même n'est pas interdit.

---

76 Article 512 du titre 17 du Code des États-Unis d'Amérique.
77 Article 512.i)1)B).
78 Article 512.i)2).
79 Article 1002 du titre 17 du Code des États-Unis d'Amérique.
80 Article 1002.c).

La loi protège également les informations codées contenues dans l'enregistrement numérique d'un enregistrement sonore. Il est interdit de coder des donner erronées concernant le code générique (qui se rapporte au type d'appareil dans lequel le système est mis en œuvre), le statut du droit d'auteur (droit revendiqué ou non) ou la génération (original ou copie) du matériel original d'un enregistrement[81]. La loi impose également des taxes sur les appareils et les supports d'enregistrement audionumérique[82]. Enfin, elle prévoit des sanctions civiles, y compris des mesures conservatoires et des dommages-intérêts pour le préjudice matériel ou moral[83].

– Loi sur la fraude informatique : en 1986, le Congrès a promulgué la loi sur la fraude informatique, qui peut s'appliquer lorsque le contournement d'un système de gestion numérique des droits passe par l'accès non autorisé à un ordinateur, qu'il s'agisse d'un serveur ou d'un ordinateur individuel. Cette loi prévoit des sanctions civiles et pénales contre l'accès intentionnel à un ordinateur sans autorisation ou en dehors de l'autorisation d'accès, afin d'obtenir des informations à partir de tout ordinateur protégé, si cet acte implique une communication avec un autre État ou avec l'étranger[84]. Elle interdit également l'accès intentionnel à un ordinateur protégé sans autorisation lorsque cet acte est à l'origine d'un préjudice[85]. D'une manière générale, le préjudice imputable à l'accès non autorisé doit s'élever à 5000 dollars É.-U. au moins pour pouvoir donner lieu à des poursuites.

– Loi sur les communications : la loi sur les communications contient trois dispositions interdisant la vente et la distribution de "boîtes noires" permettant de décrypter les signaux codés. Premièrement, elle protège les techniques d'accès conditionnel utilisées pour crypter les émissions diffusées par le câble ou les services de diffusion directe par satellite en interdisant la fabrication, l'assemblage, la modification et le trafic de tout dispositif dont une personne sait (ou a des raisons de penser) qu'il servira principalement à favoriser le décryptage non autorisé de ces émissions[86]. Elle prévoit sanctions civiles (dommages-intérêts pour le préjudice matériel et le préjudice moral) et des sanctions pénales (amende allant jusqu'à 500 000 dollars É.-U. et peine d'emprisonnement pouvant aller jusqu'à cinq ans).

Deuxièmement, la loi sur les communications interdit l'interception non autorisée de toute communication radio, ainsi que la réception non autorisée (ou l'aide à la réception non autorisée) d'une communication radio pour son propre compte ou pour le compte d'un tiers non autorisé[87]. Des dommages-intérêts peuvent être prononcés. Les auteurs d'infractions sont passibles d'une amende pouvant aller jusqu'à 2000 dollars É.-U. et d'une peine de prison pouvant aller jusqu'à six mois. Si l'acte a été commis aux fins de l'obtention d'un avantage commercial direct ou indirect ou d'un gain financier privé, les peines prévues vont jusqu'à 50 000 dollars d'amende et une privation de liberté de deux ans pour la première condamnation.

---

81 Article 1002.d).
82 Article 1003.
83 Article 1009.
84 Article 1030.a)2)C) du titre 18 du Code des États-Unis d'Amérique.
85 Article 1030.a)5)A)iii).
86 Article 605.e)4) du titre 47 du Code des États-Unis d'Amérique.
87 Article 605.a).

Troisièmement, l'interception ou la réception non autorisée de tout service de communications proposé sur un réseau câblé est interdite[88]. Parmi les actes interdits figurent la fabrication ou la distribution de dispositifs destinés à une telle réception non autorisée. Ceux-ci peuvent donner lieu au versement de dommages-intérêts. Les atteintes sont punies d'une amende pouvant aller jusqu'à 1000 dollars É.-U. et d'une peine d'emprisonnement pouvant aller jusqu'à six mois, ces peines étant aggravées si les actes ont été commis pour l'obtention d'un avantage commercial ou d'un gain financier privé (50 000 dollars d'amende et deux ans d'emprisonnement pour la première condamnation).

– Lois sur la sécurité des communications d'État : de nombreux États disposent depuis longtemps de lois qui interdisent le vol de services de câbles et de télécommunications, le piratage audiovisuel et la fraude informatique. Depuis 2002, des efforts importants sont déployés pour adapter ces lois à l'environnement numérique. Une coalition de l'industrie cinématographique et de prestataires de services tels que des câblo-opérateurs et des programmeurs demande instamment que les États facilitent le commerce électronique en se penchant sur la question du contenu diffusé en transit ou téléchargé sur l'Internet et autres réseaux à large bande passante.

Ce groupe milite en faveur de l'adoption d'une loi type sur la sécurité des communications, qui assurerait une protection juridique plus complète pour tous les services fondés sur les réseaux à large bande passante et l'Internet contre l'accès, la réception, la transmission et le décryptage non autorisés. En outre, les mesures techniques utilisées pour protéger le contenu des émissions seraient juridiquement protégées contre le contournement grâce à l'interdiction des dispositifs facilitant l'accès illicite. La loi type sur la sécurité des communications est considérée par ses adversaires comme le pendant étatique du DMCA. Lors de la rédaction du présent document, la loi type ou des lois dérivées de celle-ci avaient été adoptées dans plusieurs États et étaient à l'étude dans plusieurs autres.

Pour récapituler, la loi type, telle qu'elle a évolué au cours des discussions avec les entreprises de technologie et les autres parties intéressées, interdirait notamment les actes suivants :

– la possession, l'utilisation, la fabrication, la mise au point, la promotion et le trafic, avec l'intention de frauder un prestataire de services de communication, de tout "dispositif de communication" pour le vol d'un "service de communication" ou la réception, l'interception, le décryptage, ou l'acquisition d'un service de communication sans l'autorisation visée dans le contrat;

– la modification, l'altération ou la reprogrammation d'un dispositif de communication pour de tels buts;

– la possession, l'utilisation, la fabrication, la mise au point, la promotion et le trafic de tout "dispositif d'accès illégal"; ou

– la possession, l'utilisation ou le trafic de tous 1) plans ou instructions pour fabriquer ou assembler tout "dispositif de communication" ou "dispositif d'accès illégal" dans l'un quelconque de ces buts interdits ou 2) équipements, y compris matériel, données, logiciels ou autres informations, en sachant que l'acheteur ou un tiers utilisera ces équipements pour la fabrication, l'assemblage ou la mise au point d'un dispositif d'accès illégal ou d'un dispositif de communication à des fins interdites.

---

[88] Article 553.

Le non-respect de ces dispositions tombe sous le coup de sanctions civiles et pénales.

La législation type sur la sécurité des communications contient des définitions détaillées, qui sont résumées ci-dessous :

– par “dispositif de communication” on entend tout matériel susceptible d’intercepter, de transmettre, d’acquérir, de décrypter ou de recevoir n’importe quel service de communication, ainsi que tout composant de ce matériel, y compris tout numéro, circuit, commutateur, carte, logiciel ou puce “capable de faciliter” toute interception, transmission, décryptage, acquisition ou réception de n’importe quel service de communication;

– le terme “service de communication” est défini de manière détaillée et couvre essentiellement tout service imaginable donnant accès, contre redevance, à un contenu diffusé sur tout support de communication, y compris l’Internet;

– enfin, le terme “dispositif d’accès illégal” est défini largement comme comprenant tout dispositif, technique ou logiciel qui est “principalement conçu, mis au point, assemblé, fabriqué” ou vendu de manière illicite “afin de neutraliser ou de contourner toute technique, dispositif ou logiciel efficace, ou tout composant ou partie de ceux-ci” utilisé pour protéger toutes communications, données ou services contre l’acquisition, l’interception, l’accès, le décryptage ou la divulgation non autorisés.

La loi type sur la sécurité des communications est considérée comme étant plus large que le DMCA lui-même, raison pour laquelle elle a été controversée dans certains milieux. Elle interdit à la fois l’acte et les instruments de contournement. La loi type n’incorpore pas les exceptions et les limitations prévues dans le DMCA (en faveur par exemple de l’ingénierie inverse et de la recherche cryptographique). Des versions plus récentes prévoient toutefois une “clause d’exemption” en faveur des produits licites.

3.2.1.3 Activités normatives

3.2.1.3.a) Bureau du droit d’auteur

Comme indiqué ci-dessus, le Congrès craignait que l’article 1201.a)1) du DMCA ne compromette des utilisations traditionnelles loyales de matériel protégé parce que la loi interdit le contournement des techniques de contrôle d’accès même pour de tels usages. Au cours de la lecture législative, le Congrès a néanmoins décidé de ne pas modifier le projet pour autoriser le contournement des mesures de contrôle d’accès dans le cas d’une activité licite. À la place, il a institué une procédure selon laquelle le Librarian of Congress devrait définir les classes particulières d’œuvres à l’égard desquelles l’acte de contournement des mesures techniques serait autorisé à certaines personnes[89]. Le Librarian est tenu de déterminer tous les trois ans (après la période initiale de deux ans) si, en ce qui concerne ces classes, des personnes voient, ou risquent de voir, leur capacité d’utiliser ces œuvres de manière licite compromise en vertu de l’article 1201.a)1).

Pour parvenir à sa décision, le Librarian doit tenir compte d’une variété de facteurs, tels que la possibilité d’utiliser les œuvres (en particulier à des fins non lucratives d’archivage, de conservation et d’enseignement), les incidences de l’article 1201.a)1) sur les utilisations loyales traditionnelles et l’effet du contournement sur les débouchés des œuvres.

---

[89] Article 1201.a)1)C) du titre 17 du Code des États-Unis d’Amérique.

Le 28 octobre 2000, dans sa première décision du genre, le Librarian a considéré que deux classes restreintes d'œuvres bénéficieraient d'une exemption de l'interdiction pendant les trois années à venir : les compilations de sites Web bloqués par des logiciels de filtrage et les œuvres littéraires auxquelles il n'est pas possible d'accéder en raison d'un défaut de fonctionnement, de dommages ou de l'obsolescence[90]. Actuellement, le Bureau du droit d'auteur de la Bibliothèque du Congrès, qui doit présenter une recommandation au Librarian, est à mi-parcours de la deuxième procédure réglementaire, qui doit être achevée le 28 octobre 2003[91].

Les difficultés qui attendent ceux qui tentent d'obtenir une exemption se sont révélées tout à fait considérables. Tout d'abord, il leur faut prouver qu'ils ont été, ou seront réellement lésés dans leur utilisation des œuvres du fait des dispositions anticontournement. Bien entendu, c'est d'autant plus difficile que les techniques de contrôle d'accès ne sont pas encore très répandues.

Ensuite, ils doivent prouver qu'ils sont lésés en ce qui concerne une "classe d'œuvres". Or, le Bureau du droit d'auteur a éprouvé des difficultés pour définir de terme. Bien que certaines parties aient sollicité une exemption pour les œuvres d'usage loyal, le Bureau du droit d'auteur a rejeté cette demande au motif qu'une "classe d'œuvres" ne saurait être déterminée par la façon dont les œuvres peuvent être utilisées. Le Bureau a conclu que le texte de la loi et l'histoire de son adoption excluaient l'octroi de larges exemptions au titre de l'usage loyal.

Certains partisans de l'usage loyal et d'autres opposants au DMCA en général et au caractère restrictif de ses exceptions en particulier ont sans doute espéré que cette procédure aurait permis d'équilibrer davantage le DMCA qu'il n'avait été possible de le faire pendant l'examen du projet au Congrès. Ainsi, dans la procédure en cours, ont-ils par exemple demandé au Bureau du droit d'auteur d'autoriser le contournement à des fins spécifiques telles que la suppression du code régional ou des messages publicitaires sur les DVD, ou encore l'accès à des films du domaine public sur DVD, et à des fins générales telles que la recherche en matière de techniques de contrôle d'accès et l'accès à toute œuvre protégée par des mécanismes de contrôle d'accès nécessitant l'utilisation d'un système de gestion numérique des droits spécifié par le titulaire des droits. Compte tenu des règles édictées dans la décision d'octobre 2000 du Librarian, du texte du DMCA et de la charge de la preuve qui s'y rapporte, il est peu probable que les "classes d'œuvres" exemptées de l'interdiction visée à l'article 1201.a)1) seront vastes ou nombreuses. À cet égard, le Directeur de l'enregistrement des droits d'auteur a suggéré que tout argument en faveur de l'élargissement des catégories d'œuvres bénéficiant d'une exemption ou d'un allégement de la charge de la preuve devrait être présenté au Congrès[92].

Enfin, il convient de préciser que, même lorsqu'une exemption est prévue pour une certaine classe d'œuvres, seul l'acte de contournement serait autorisé. Les instruments de contournement restent interdits[93]. Or, en l'absence d'instruments permettant à des utilisateurs

---

90 Exemptions to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64556 (27 octobre 2000); article 201 du titre 37 C.F.R.

91 Exemptions to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 67 Fed. Reg. 63578 (15 octobre 2002).

92 65 Fed. Reg., 64562.

93 Article 1201.a)1)E) du titre 17 du Code des États-Unis d'Amérique.

ordinaires de contourner une mesure de contrôle d'accès, le droit de se livrer à un tel acte risque d'être d'une utilité très limitée. Nonobstant toute exemption de l'acte lui-même, l'article 1201.a)2) continuerait d'interdire le trafic d'instruments de contournement; un tel instrument peut ne pas satisfaire aux critères énoncés dans cet article s'il est principalement conçu ou produit aux fins de contournement dans des cas où le Librarian a autorisé ce contournement (et limité d'autres usages).

3.2.1.3.b) Commission fédérale des communications : décret relatif au "broadcast flag"

Les titulaires de droits font savoir depuis plusieurs années que la protection des émissions libres de télévision numérique qui sont radiodiffusées par voie hertzienne sans cryptage d'origine est l'un des éléments de la protection du contenu qui fait le plus cruellement défaut à l'ère du numérique. Les systèmes d'accès conditionnel peuvent protéger le contenu jusqu'à l'entrée du domicile. Comme indiqué à la section 3.2.1, de nouvelles techniques – DTCP, HDCP et CPRM – permettent de protéger le contenu audio et audiovisuel contre sa distribution non autorisée sur des réseaux internes, ou du domicile à l'Internet, et de sécuriser l'enregistrement de ce contenu. Pour bénéficier de cette protection, le contenu doit toutefois être diffusé sous une forme protégée, soit par un système d'accès conditionnel, soit par un autre mécanisme signalant que le contenu doit être protégé à domicile.

Les titulaires de droits sont très préoccupés par le fait que le contenu des émissions de télévision numérique, qui n'est pas protégé à l'entrée du domicile, peut être copié, retransmis sur l'Internet ou distribué sans autorisation par d'autres moyens. En conséquence, ils risquent d'être réticents à autoriser la diffusion d'émissions de qualité sur les chaînes de télévision numérique hertzienne.

Pour répondre à ces préoccupations, divers groupes d'intérêts privés ont commencé à évaluer des solutions possibles au sein du Groupe de travail technique sur la protection contre la copie ("Copy Protection Technical Working Group - CPTWG"), qui a établi en novembre 2001 le Groupe de discussion sur la protection de la radiodiffusion ("Broadcast Protection Discussion Group") (depuis 1996, le CPTWG se réuni chaque mois à Los Angeles (Californie) pour évaluer les solutions techniques en matière de protection contre la copie). En juin 2002, les coprésidents de ce groupe ont publié un rapport qui traduisait en grande partie l'opinion prédominante au niveau sectoriel sur les moyens de résoudre ce problème. Le rapport recommande que le descripteur de contrôle de redistribution visé dans la norme ATSC A/6A – dénommé "broadcast flag" – soit utilisé pour signaler que le contenu d'une émission de télévision numérique doit être protégé.

Parmi les principaux problèmes recensés par toutes les parties figurait la question de l'application : tout consensus du secteur privé sur l'utilisation d'un descripteur du type broadcast flag serait sans intérêt en l'absence d'un mécanisme garantissant que les appareils détecteront ce signal et réagiront en conséquence. En particulier, pour s'assurer que tous les produits recevant des émissions numériques terrestres fonctionneraient de la manière prévue, la nécessité d'une certaine forme d'intervention gouvernementale a été largement (sinon universellement) admise.

Une autre série de questions se rapporte aux règles applicables aux appareils de réception du contenu radiodiffusé, soit avant la détection du broadcast flag, soit après. Ces questions portent 1) sur la mesure dans laquelle le contenu radiodiffusé doit être protégé et

2) sur les sorties numériques protégées et les sorties analogiques vers lesquelles un produit soumis à ces règles peut diffuser un contenu marqué par le broadcast flag. Une question concerne le contournement : à quel niveau de fiabilité doivent répondre les normes de conception et de production des appareils soumis à ces règles pour prévenir le contournement ou la neutralisation du broadcast flag.

Pour répondre à ces questions ainsi qu'à d'autres, la Commission fédérale des communications ("FCC") a lancé une procédure de normalisation en août 2002[94]. La FCC évalue la nécessité d'imposer que les appareils reconnaissent le descripteur ATSC ou un autre signal et y donnent effet; s'il convient d'imposer, et de quelle manière, que les dispositifs en aval du récepteur protègent le contenu numérique diffusé par voie hertzienne; et les critères à utiliser pour déterminer quelles techniques de protection en sortie sont autorisées à recevoir du contenu identifié par le broadcast flag.

La FCC a reçu de nombreux commentaires sur ces propositions de la part de l'industrie et du grand public. Les principaux partisans de la publication d'un décret de la FCC sont les titulaires de droits, tels que l'industrie cinématographique, les radiodiffuseurs et certaines grandes entreprises technologiques. Beaucoup d'opinions divergentes ont toutefois été exprimées, par certaines entreprises technologiques (principalement sur le point de savoir si la FCC devrait réglementer le matériel), ainsi que par de nombreux consommateurs et groupes d'intérêt publics. Parmi les principaux points de controverse figure la question de savoir si une norme selon laquelle l'enregistrement des émissions numériques diffusées par voie hertzienne et identifiées par le broadcast flag doit être sécurisé compromettrait la pratique de l'enregistrement et de la consultation légitime à domicile et à des fins privées ou la possibilité de diffuser le contenu sur un réseau numérique à domicile. D'autres sujets de discussion ont porté sur la question de savoir si l'utilisation du broadcast flag devrait être interdite à l'égard de certains types de contenu dont la diffusion devrait être autorisée, ou souhaitable, comme les programmes d'urgence.

Enfin, en ce qui concerne la protection du contenu numérique diffusé par voie hertzienne, la nécessité d'adopter une démarche commune au niveau international est largement admise par les titulaires de droits et certaines grandes entreprises technologiques. Même si l'adoption du broadcast flag par la FCC peut se traduire par une réduction significative de la redistribution sur l'Internet du contenu protégé par le broadcast flag aux États-Unis d'Amérique, les émissions de télévision hertzienne diffusées aux États-Unis d'Amérique peuvent être reçues dans les pays limitrophes, à partir desquels elles pourraient alors être rediffusées. De même, lorsque de tels programmes sont radiodiffusés sous forme numérique non cryptée à l'extérieur des États-Unis d'Amérique, ils peuvent aussi être captés à l'aide de récepteurs et rediffusés sur l'Internet. Par conséquent, il est admis que, si la FCC décide d'adopter un décret relatif au broadcast flag, des règles gouvernementales semblables devront être adoptées dans d'autres ressorts juridiques.

3.2.1.3.c) Commission fédérale des communications : règles de compatibilité entre les réseaux câblés et l'électronique grand public

---

94 *In the Matter of Digital Broadcast Copy Protection*, Notification of Proposed Rulemaking, dossier MB n° 02-230, 67 Fed. Reg. 53903 (20 août 2002).

La FCC est intervenue dans un autre secteur de la gestion des droits pour tenter d'assurer la compatibilité entre les services câblés et les appareils électroniques grand public, tels que les téléviseurs haute définition ("HDTV"). En décembre 2002, à l'issue de négociations prolongées et intenses, les principaux fabricants d'appareils électroniques grand public et les principaux câblo-opérateurs ont conclu un accord détaillé en vue d'assurer la compatibilité sans configuration ("plug and play") entre les services de câble univoques et la prochaine génération de téléviseurs numériques, sans décodeur, pour permettre aux consommateurs de recevoir et d'enregistrer les signaux HDTV et favoriser la connexion de nouveaux appareils aux téléviseurs HDTV.

Après avoir conclu leurs négociations privées, les parties à l'accord ont soumis celui-ci à la FCC. Elles ont conjointement recommandé que la FCC officialise cet accord et rende obligatoire l'application des normes sur lesquelles elles s'étaient entendues à l'égard de tous les diffuseurs d'émissions de télévision à péage, aussi bien sur le câble que par satellite, ainsi qu'à l'égard des fabricants de matériel. L'intervention des pouvoirs publics est cruciale aux yeux des instigateurs de l'accord, afin d'assurer des conditions équivalentes à tous les acteurs de l'industrie. Et ils ont fortement insisté sur le fait que tant le Congrès que la FCC ont été d'avis que la FCC devait mettre en œuvre des normes de compatibilité universelles, applicables à la fois au satellite et au câble.

Il importe de souligner que, tout au long du processus, la FCC a encouragé au plus haut point ces négociations au sein du secteur privé. Elle a en effet sollicité cette soumission conjointe parce qu'elle était convaincue que les litiges continuels et non résolus au sujet de la protection du contenu des émissions télévisées constituaient des obstacles significatifs à la transition vers la télévision numérique aux États-Unis d'Amérique.

En ce qui concerne la gestion numérique des droits, les parties demandent à la FCC d'adopter des règles relatives à la protection contre la copie des émissions de télévision à péage comprenant des règles fédérales officielles en matière de codage. Si elles sont adoptées par la FCC, ces règles régiraient la mesure dans laquelle les consommateurs pourraient enregistrer certaines catégories d'émissions diffusées par satellite et sur le câble (non compris les services reçus par l'intermédiaire d'un modem numérique ou de l'Internet). Du point de vue des fabricants de matériel électronique grand public et des consommateurs, ces règles doivent nécessairement faire partie de l'accord.

D'une manière générale, les règles le codage spécifiques convenues par les parties et examinées par la FCC sont alignées sur celles indiquées dans la licence technique DTCP et à l'article 1201.k) du DMCA[95]. Ces règles permettraient aux titulaires de droits sur des émissions télévisées de marquer leur contenu de sorte que 1) une seule génération de copies puisse être faite à partir d'une émission diffusée par un service d'abonnement mensuel; 2) les émissions vendues dans le cadre de services de paiement à l'utilisation, de vidéo à la demande ou de vidéo à la demande par abonnement mensuel soient impossibles à copier, mais puissent être stockées pendant 90 minutes (ou plus, en cas d'accord) sur un magnétoscope individuel; et 3) le contenu gratuit diffusé par voie hertzienne puisse être copié librement. Les règles proposées régiraient également la question de savoir si et comment il convient d'autoriser le codage du contenu diffusé dans le cadre de services de distribution nouveaux et non définis (c'est-à-dire, autrement que dans le cadre des services décrits dans la phrase précédente) et de mettre à jour ces règles en matière de codage; la proposition prévoit que les

[95] Voir la note 56, relative à l'article 1201.k).

opérateurs pourront appliquer des règles de codage différentes aux nouveaux modèles de distribution, mais que ces règles pourront donner lieu au dépôt d'une plainte devant la FCC, qui pourra statuer sur le litige.

Peu de temps après avoir été saisie de l'accord, la FCC a lancé un appel public à commentaires, y compris sur les règles proposées[96]. Bien entendu, les règles de codage (de même que les autres éléments de l'accord) sont appuyées par les parties à l'accord et les entités apparentées. Les opérateurs de satellites sont quant à eux opposés à l'application des règles à leur égard.

En outre, quelques groupes d'intérêts des consommateurs au moins ont émis de vives réserves, concernant en particulier l'opportunité de règles officielles en matière de codage; ils craignent que ces règles ne suppriment la possibilité d'enregistrer à des fins d'usage loyal certaines catégories d'émissions dont l'enregistrement à domicile est actuellement autorisé. De nombreux titulaires de droits, tout en manifestant un appui limité en faveur de ces accords, se sont aussi montrés relativement critiques, notamment à l'égard des règles de codage qui, selon eux, restreindraient leur choix du modèle de distribution à l'égard du contenu diffusé sur les systèmes d'accès conditionnels. À l'inverse, d'autres participants ont estimé que, aux termes de l'accord, les règles de codage étaient trop faciles à modifier ou à désactiver par les opérateurs.

3.2.1.4 Projets de loi

Après l'adoption du DMCA, beaucoup d'autres projets de loi ont été soumis au Congrès en vue de régler diverses questions, visant à modifier le DMCA lui-même, à renforcer le rôle des pouvoirs publics dans l'élaboration de systèmes de gestion numérique des droits ou encore à autoriser les titulaires de droits à mettre en œuvre des solutions d'auto-assistance contre la distribution non autorisée de contenu. Aucun des projets soumis au Congrès à sa 107e législature (qui s'est achevée en 2002) n'a été adopté. Aucun des projets présentés à la législature actuelle du Congrès (108e) n'a encore été adopté. Néanmoins, ces projets sont instructifs dans la mesure où ils mettent en lumière des questions controversées restées en suspens après la mise en œuvre des traités de l'OMPI aux États-Unis d'Amérique. Ces projets sont récapitulés ci-dessous :

– Modification du DMCA afin d'autoriser le contournement aux fins de l'usage loyal : en octobre 2002, deux projets ont été présentés en vue modifier le DMCA pour permettre le contournement dans certaines circonstances. Tout d'abord le projet de loi H.R. 5544 sur les droits des consommateurs sur les supports numériques (Digital Media Consumers' Rights Act) aurait créé une exception pour les activités de "poursuite exclusive de recherches scientifiques sur les mesures techniques de protection"[97]. Ce projet de loi aurait également autorisé le contournement d'une mesure technique "lorsque cet acte n'est pas constitutif d'atteinte" - c'est-à-dire, dans le cadre de l'usage loyal[98]. Enfin, la loi aurait

---

96 *In the Matter of Implementation of Section 304 of the Telecommunications Act of 1996*, Commercial Availability of Navigation Devices, CS dossier n° 97-80, Compatibility Between Cable Systems and Consumer Electronics Equipment, PP dossier n° 00-67, Further Notice of Proposed Rulemaking, 68 Fed. Reg. 2278 (16 janvier 2003).

97 H.R. 5544, 107e législature du Congrès, 2e session, article 5.a) (2002).

98 *Id.* article 5.b).

autorisé la fabrication, la distribution ou l'utilisation non illicite d'un produit "permettant une utilisation licite significative d'une œuvre protégée par le droit d'auteur", essentiellement pour rétablir la règle en matière de responsabilité indirecte édictée par la Cour suprême[99]. Le député Richard Boucher, principal instigateur du projet de loi, a déclaré que son texte permettait de répondre à la menace que faisaient peser sur l'usage loyal les mesures techniques protégées par le DMCA. En janvier 2003, le même député a réintroduit le projet de loi sur les droits des consommateurs sur les supports numériques sous le numéro H.R. 107[100].

Ensuite, un projet de loi sur la liberté de choix en matière numérique (Digital Choice and Freedom Act) a aussi été présenté, sous le numéro H.R. 5522, afin de remédier à la remise en cause des droits et aspirations légitimes des consommateurs par le DMCA[101]. Ce projet aurait modifié la loi sur droit d'auteur et le DMCA de plusieurs façons. Il aurait ajouté une nouvelle limitation aux droits exclusifs des titulaires de droit d'auteur : les personnes ayant acquis de manière légale une copie d'une œuvre numérique ou recevant de manière légale une œuvre diffusée auraient été autorisées à "reproduire, stocker ou adapter l'œuvre ou à accéder à l'œuvre" à des fins d'archivage ou pour exécuter ou présenter l'œuvre à des fins non commerciale[102], vraisemblablement indépendamment de l'application de toute mesure technique. En outre, ce projet aurait modifié le DMCA afin d'indiquer expressément qu'une personne peut contourner toute mesure technique dès lors que celle-ci empêcherait une utilisation licite et que le titulaire des droits d'auteur ne rendrait pas accessibles les moyens nécessaires aux fins d'une telle utilisation[103]. Enfin, le projet de loi aurait expressément exempté des dispositions anticontournement du DMCA relatives au matériel les produits conçus, fabriqués ou commercialisés aux fins du contournement d'une mesure si cette mesure empêche des utilisations licites et que le titulaire des droits ne rend pas accessibles les moyens nécessaires aux fins de telles utilisations[104].

Un large éventail de titulaires de droits d'auteur et d'intérêts connexes se sont opposés à la fois aux projets H.R. 5544 et H.R. 5522 lors de la 107e législature du Congrès et au projet H.R. 107 au cours de législature actuelle. Ils ont argué du fait que ces projets de loi feraient augmenter les prix et étoufferaient l'innovation en matière de techniques numériques de gestion des droits et de distribution. En outre, bien qu'ils reconnaissent que ces projets auraient autorisé le contournement des techniques de gestion numérique des droits aux fins d'un usage loyal, ils soulignent que les produits qui seraient ainsi autorisés pourraient aussi être utilisés pour contourner des systèmes de gestion numérique des droits à des fins tout à fait illégitimes. Ils affirment par ailleurs que, dans la mesure où le DMCA est un instrument équilibré utilisé comme modèle par d'autres pays, l'adoption du projet de loi H.R. 107 donnerait à penser que les États-Unis d'Amérique considèrent qu'un certain niveau de contournement est acceptable, ce qui établirait un précédent fâcheux au niveau international.

– Normalisation des techniques de gestion numérique des droits par les pouvoirs publics : l'un des projets de loi les plus controversés examinés par le Congrès postérieurement à la mise en œuvre du DMCA a sans doute été le projet S. 2048, sur la promotion de la

---

99 *Id.*

100 H.R. 107, 108e législature du Congrès, 2e session (2003).

101 H.R. 5522, 107e législature du Congrès, 2e session (2002).

102 *Id.* article 3 (visant à ajouter un nouvel article 123 à la loi sur le droit d'auteur).

103 *Id.* article 5.

104 *Id.*

télévision numérique à haut débit (Consumer Broadband and Digital Television Promotion Act), qui a été présenté en mars 2002[105]. Ce projet mettait en lumière les importantes différences de conception sur les rôles respectifs du secteur privé et du gouvernement dans la fixation de normes, notamment en ce qui concerne les systèmes de gestion numérique des droits. Le sénateur Ernest Hollings, sur les instances de quelques compagnies cinématographiques, a été l'artisan et le principal promoteur du projet S. 2048. Cet instrument visait à mettre en place des incitations substantielles pour que les représentants du secteur privé aboutissent à un accord sur des "normes en matière de systèmes de sécurité" pour les appareils numériques et sur des règles de codage. S'ils n'y parvenaient pas, les pouvoirs publics prendraient le relais et imposeraient des normes. Les normes agréées devaient répondre à certains critères indiqués dans le projet de loi, et les règles en matière de codage devaient permettre la copie privée des émissions radiodiffusées par voie hertzienne et des émissions diffusées sur les chaînes à péage du câble et par satellite[106].

Fondamentalement, le projet de loi donnait au secteur privé 12 mois pour conclure un tel accord. Si, à l'issue de cette période, la FCC constatait que le secteur privé y était parvenu, elle devait officialiser ces normes techniques et règles de codage par voie réglementaire[107]. En revanche, si elle constatait que les efforts du secteur privé n'avaient pas abouti, le projet de loi prévoyait que la commission adopte elle-même, dans un délai de 13 mois à compter de cette constatation, des normes de gestion des numérique des droits et des règles de codage élaborées par les pouvoirs publics et répondant aux critères indiqués dans la législation[108]. Le projet de loi aurait permis au secteur privé de modifier les normes agréées ou imposées par le gouvernement dans le cas où la technologie aurait été compromise ou compte tenu du progrès technique[109].

En outre, le projet S. 2048 contenait une série de dispositions visant à s'assurer que les fabricants et les titulaires de droits se conformeraient aux normes. La première aurait interdit la vente de futurs "dispositifs numériques" – définis en tant qu'appareils d'enregistrement, de conversion, de lecture ou d'accès à des supports numériques qui ne répondraient pas aux normes[110]. La deuxième aurait interdit la suppression ou l'altération délibérée d'une technique conforme aux normes ou la transmission délibérée de matériel protégé en cas de suppression ou d'altération de la mesure de sécurité[111]. La troisième aurait interdit l'application d'une technique de sécurisation en violation des règles de codage[112].

---

105 S. 2048, 107e législature du Congrès, 2e session (2002).
106 *Id.* article 3.d).
107 *Id.* article 3.b).
108 *Id.* article 3.c).
109 *Id.* article 3.h).
110 *Id.* article 5.
111 *Id.* article 6.
112 *Id.*

Le projet S. 2048 n'indiquait pas à quels problèmes ou lacunes spécifiques des techniques de gestion numérique des droits – ou déficiences du secteur privé – il était censé remédier. Il appartenait au Congrès de constater que les accords existants n'assuraient pas un environnement numérique sécurisé et que les systèmes existants de gestion numérique des droits apportaient seulement des solutions commerciales et partielles. Les constatations du Congrès auraient également pu être critiques à l'égard du secteur privé, indiquant que "les intérêts commerciaux concurrents ont empêché un accord sur l'installation des techniques existantes dans les appareils numériques pour protéger le contenu numérique sur l'Internet ou la télévision numérique hertzienne"[113]. Il était connu, et les auditions du Congrès l'ont démontré, que trois points préoccupaient le sénateur Hollings et les partisans du projet S. 2048 : 1) l'absence de protection des émissions de télévision numérique hertzienne contre leur retransmission sur l'Internet; 2) la difficulté d'empêcher la retransmission de contenu analogique qui avait été converti à partir d'une source numérique protégée (le problème dit de la "faille analogique"); et 3) les menaces constituées par le partage point à point non contrôlé et non autorisé de fichiers numériques.

Le projet S. 2048 s'est heurté à une opposition farouche et pratiquement unanime des entreprises d'informatique, des fabricants d'appareils électroniques grand public, des groupes de consommateurs et des utilisateurs de contenu. Plusieurs arguments ont été avancés contre ce projet. Premièrement, le secteur privé faisait des progrès dans ce domaine, ainsi qu'en témoigne la publication du rapport sur le broadcast flag, qui a incité la FCC à adopter le décret décrit ci-dessus. Deuxièmement, il serait hautement contreproductif et malvenu que le gouvernement se mêle de l'élaboration et de l'application de normes dans ce domaine. Troisièmement, le gouvernement ne devrait pas fixer des délais arbitraires concernant l'aboutissement des recherches du secteur privé pour trouver des solutions techniques, notamment en ce qui concerne le problème extrêmement épineux du partage de fichiers. Les principaux promoteurs du projet étaient les studios cinématographiques et des intérêts connexes.

– Solutions d'auto-assistance pour lutter contre le partage de fichiers : une conception tout à fait différente des moyens à mettre en œuvre pour la protection du contenu aurait consisté à encourager l'élaboration et l'utilisation de solutions d'auto-assistance pour empêcher l'échange illicite de fichiers point à point. Les titulaires de droits et le Congrès étaient frustrés par l'incapacité des mesures techniques de lutter contre ces systèmes. Les procès pour atteinte au droit d'auteur intentés contre Napster et d'autres systèmes d'échange de fichiers, bien que concluants du point de vue des titulaires de droits, étaient longs et ne permettaient d'attaquer qu'un système à la fois. Et lorsque les systèmes sont entièrement distribués, sans aucun des répertoires ou serveurs centralisés utilisés par Napster et les services semblables, le recours à la justice pour stopper l'énorme volume de fichiers échangés pourrait se révéler extrêmement complexe.

Les titulaires de droits ont par conséquent commencé à explorer les moyens d'interférer avec les techniques d'échange illicite de fichiers, tels que les interdictions, les leurres, les réacheminements, le blocage des fichiers ou d'autres contre-mesures. En utilisant ces outils, les titulaires de droits craignaient néanmoins que ces activités ne puissent en elles-mêmes susciter des actions judiciaires de la part des personnes se livrant au partage de fichiers, d'autres utilisateurs lésés et des organismes de défense des consommateurs.

---

[113] *Id.* article 2.

Pour répondre à ces préoccupations, le projet de loi H.R. 5211 sur la prévention du piratage point à point (Peer-to-Peer Piracy Prevention Act) a été présenté en juillet 2002 sous l'impulsion du député Howard Berman[114]. Lors de la présentation de son projet, celui-ci a indiqué que, bien que l'élaboration et la mise en œuvre de solutions de gestion numérique des droits soient à encourager, ces solutions ne permettent pas de résoudre complètement le problème du partage de fichiers puisque les œuvres protégées qui sont diffusées sur les systèmes point à point sont déjà "en clair" sur l'Internet.

Le projet H.R. 5211 aurait accordé aux titulaires de droits d'auteur une exemption indéterminée pour ses activités d'auto-assistance visant à lutter contre le partage de fichier, à condition qu'elles n'aient pas de conséquences indirectes. Les titulaires auraient été complètement exonérés de toute responsabilité pénale ou civile en vertu des lois fédérales ou étatiques en cas de "neutralisation, interférence, blocage, détournement ou autre altération" de toute utilisation non autorisée de leurs propres œuvres protégées sur "un réseau point à point d'échange de fichiers accessible au public"[115]. Cette exemption n'aurait toutefois été applicable que si l'acte du titulaire des droits d'auteur n'avait altéré aucun autre fichier électronique ni aucune donnée sur l'ordinateur de la personne se livrant au partage de fichiers. Elle n'aurait pas été applicable en cas de préjudice économique causé à une autre personne ou de préjudice supérieur à 50 dollars É.-U. pour la personne se livrant au partage de fichiers (non compris les œuvres du titulaire du droit d'auteur)[116].

Une autre condition à l'application de la clause d'exonération était que le titulaire du droit d'auteur devait avoir notifié plusieurs jours à l'avance le Ministère de la justice des techniques spécifiques qu'il avait l'intention d'employer pour contrecarrer les activités illicites de partage de fichiers[117]. Les titulaires de droits d'auteur devaient également, sur demande, indiquer aux personnes se livrant au partage de fichiers la raison des mesures prises pour contrecarrer cette activité; toutefois, cette notification ne devait pas obligatoirement être effectuée avant la mise en œuvre de la mesure technique. Les activités abusives des titulaires de droits d'auteur entraînant un préjudice économique réel pour les personnes qui se livrent au partage de fichiers pouvaient donner lieu à une action en dommages-intérêts de la part des personnes lésées. Le Ministère de la justice aurait pu prendre des mesures conservatoires à l'encontre des titulaires qui mettraient en œuvre des mesures abusives d'altération sans raison valable de penser qu'une atteinte aux droits s'était produite[118].

Le projet de loi H.R. 5211 s'est heurté à l'opposition de certains groupes d'intérêts qui estimaient qu'il ne se limitait pas à autoriser les titulaires à contrecarrer uniquement l'utilisation non autorisée de leurs propres œuvres. Selon eux, ce projet aurait établi une immunité pour toutes les activités – même celles qui se seraient traduites par la destruction d'autres fichiers – qu'un titulaire aurait entreprises pour tenter de mettre fin à un acte illicite sur un réseau point à point. Ils ont également argué du fait que le titulaire des droits d'auteur pourrait attaquer par tous les moyens l'ordinateur d'une personne pratiquant l'échange de fichiers, à la seule condition d'en avoir informé au préalable le Ministère de la justice. Les promoteurs du projet de loi ont souligné le caractère limité de l'exemption et l'interdiction faite aux titulaires d'altérer ou de supprimer tout fichier sur l'ordinateur d'une personne

---

114 H.R. 5211, 107e législature du Congrès, 2e session (2002).
115 *Id.*article 1.a) (visant à ajouter un nouvel article 514 à la loi sur le droit d'auteur).
116 *Id.*
117 *Id.*
118 *Id.*

pratiquant le partage de fichiers, même si le blocage de la transmission des œuvres propres du titulaire était permis.

– Interdiction du trafic de dispositifs d'authentification illicites : le Congrès a également envisagé de renforcer la loi anticontrefaçon pour interdire le trafic de tout "dispositif d'authentification illicite apposé sur ou incorporé à" une copie de programme d'ordinateur, de film, de toute autre œuvre audiovisuelle ou d'un enregistrement phonographique. Le projet de loi S. 2395 sur les modifications à apporter à la loi anticontrefaçon a été introduit en avril 2002 précisément à cette fin[119].

Le projet S. 2395 définissait les "dispositifs d'authentification" comme incluant les tatouages, symboles, codes, certificats, hologrammes et autres moyens utilisés pour indiquer qu'une copie ou un phonogramme n'est pas contrefait. Les "dispositifs d'authentification illicites" étaient définis comme des dispositifs d'authentification licites au départ mais modifiés ou altérés "afin d'inciter un tiers à reproduire ou à accepter la distribution" de la copie ou qui ont été distribués sans l'autorisation du titulaire des droits d'auteur et pas en rapport avec une copie effectuée de manière licite à laquelle le dispositif d'authentification devait être incorporé. En d'autres termes, il aurait été illicite de modifier un élément d'un système de gestion numérique des droits, tel qu'un tatouage ou un code informatique, qui contrôle l'authenticité d'une copie d'une œuvre, et de distribuer ensuite cet élément pour faciliter la distribution de copies piratées. Des sanctions civiles et pénales auraient été prévues.

Dans la mesure où le projet S. 2395 contenait essentiellement des dispositions anticontrefaçon, il n'a guère suscité d'opposition dans un premier temps. Quelques groupes intérêts s'y sont toutefois opposés lorsqu'ils ont considéré qu'il pouvait potentiellement s'appliquer aux techniques ou aux actes qui altéreraient les tatouages numériques. En mars 2003, le projet a été réintroduit sous le numéro S. 731 (Secure Authentication Feature and Enhanced Identification Defense Act), mais dans une forme beaucoup plus restreinte, visant à protéger uniquement les dispositifs d'authentification émis par le gouvernement[120].

– Obligation de divulgation des mesures techniques : un projet de loi impliquant le gouvernement dans les techniques de gestion numérique des droits mais qui, s'il était adopté, serait moins contraignant que plusieurs des autres projets décrits ci-dessus, imposerait simplement l'obligation d'informer les consommateurs de l'utilisation des dispositifs techniques limitant les usages du contenu. Le projet S. 692 (Digital Consumer Right to Know Act) a été présenté en mars 2003 pour créer des incitations commerciales à la mise au point de systèmes de gestion numérique des droits qui traitent des problèmes de reproduction et de distribution non autorisées, tout en préservant au maximum les possibilités d'utilisation et de manipulation licites[121].

Le projet S. 692 exigerait que la Commission fédérale du commerce édicte des règles imposant aux producteurs ou aux distributeurs de contenu numérique protégé l'obligation de déclarer clairement tous les dispositifs techniques susceptibles de restreindre la capacité des consommateurs de lire, copier, transmettre ou transférer ce contenu entre des appareils

---

119 S. 2395, propositions d'amendement de la loi anticontrefaçon, 107e législature du Congrès, 2e session (2002).

120 S. 731, 108e législature du Congrès, 1re session (2003).

121 S. 692, 108e législature du Congrès, 1re session (2003).

courants[122]. Pour le promoteur du projet de loi, cette notification préalable est une simple question d'équité, afin que les utilisations courantes ne soient pas inopinément bloquées. Plus précisément, le projet de loi S. 692 imposerait la divulgation de toutes les limitations techniques sur les pratiques suivantes : enregistrement d'une émission de télévision hertzienne ou à péage (mais non d'une émission reçue moyennant paiement à l'utilisation) aux fins de l'aménagement du temps d'écoute; transfert de support ou de plate-forme pour le contenu audiovisuel (par exemple, entre le domicile et le bureau ou entre appareils portatifs); réalisation de copies de sauvegarde de contenu acquis légalement; utilisation d'extraits à des fins d'usage loyal; et transfert ou vente de contenu légalement acquis à un autre consommateur (lorsque le cédant ou vendeur ne conserve aucun autre droit sur le contenu)[123].

3.2.2 Jurisprudence

Plusieurs décisions de justice interprétant les dispositions anticontournement de l'article 1201 on déjà été rendues aux États-Unis d'Amérique.

Universal City Studios, Inc. c. Corley[124]: l'action la plus significative au titre du DMCA a été intentée par huit grands studios cinématographiques contre les défendeurs, qui exploitaient une publication fondée sur le Web. Les défendeurs avaient mis en ligne un algorithme de décryptage connu sous le nom de DeCSS et avaient encouragé des tiers à le copier et à le distribuer. DeCSS permet aux utilisateurs de forcer ou de contourner la mesure technique (dénommée CSS) limitant l'accès non autorisé aux DVD vidéo. Les défendeurs avaient également publié des liens vers d'autres sites Web où le logiciel DeCSS pouvait être téléchargé. Le principal argument avancé par la défense dans cette affaire était que les dispositions antitrafic de l'article 1201.a)2) étaient anticonstitutionnelles parce qu'elles violaient le droit à la liberté d'expression garanti par le premier amendement, invoqué par les défendeurs pour justifier l'échange du code source du programme.

Le tribunal de district a déterminé que le CSS "contrôle efficacement l'accès" aux longs métrages sur les DVD vidéo, puisque des clés sont nécessaires pour accéder aux films et que ces clés ne peuvent pas être obtenues sans licence CSS de la DVD CCA. Le tribunal a également rejeté l'argument des défendeurs selon lequel, compte tenu de sa faiblesse, le système de cryptage CSS ne pouvait être considéré comme une mesure technique "efficace", faisant observer que la loi serait sans objet si elle protégeait seulement les mesures complètement efficaces.

Le tribunal a rejeté tous les arguments de la défense. Il a conclu catégoriquement que les défendeurs ne remplissaient pas les conditions requises pour bénéficier des trois exemptions de l'article 1201 à l'égard de leurs activités (ingénierie inverse, recherche cryptographique et essais de sécurité). Il a par ailleurs déterminé que l'usage loyal n'était pas applicable dans le cadre d'une action intentée en vertu de l'article 1201.

---

122 *Id.* article 3.a).

123 *Id.* article 3.c). Le projet H.R. 107 susmentionné contient aussi une disposition relative à la divulgation; elle imposerait à la Commission fédérale du commerce l'obligation d'assurer un étiquetage approprié des CD protégés contre la copie.

124 273 F.3d 429 (2d cercle. 2001), *Universal City Studios, Inc. c. Reimerdes*, 111 F. Supp. 346 2d (S.D.N.Y. 2000).

Les défendeurs ont été enjoints ne pas publier le DeCSS sur leur site Web. L'ordonnance leur interdisait également de publier des liens vers d'autres sites proposant le logiciel. Le tribunal a noté que l'interdiction de créer de tels liens contribuerait à empêcher la diffusion du DeCSS, en particulier lorsque les liens renvoyaient vers des sites Web en dehors des États-Unis d'Amérique.

En novembre 2001, la Cour d'appel des États-Unis d'Amérique pour le deuxième circuit a confirmé en tous points la décision du tribunal de district. Elle a considéré que l'injonction était constitutionnelle parce qu'elle n'était pas liée au contenu : elle visait seulement les éléments fonctionnels et non expressifs du code de décryptage (et, dans le cas des liens, seulement leurs aspects fonctionnels et non expressifs) et qu'elle n'avait qu'une incidence fortuite sur la liberté d'expression des défendeurs.

La Cour d'appel a spécifiquement examiné la question de savoir si le contournement du CSS était permis lorsqu'il visait à contribuer à un usage loyal des films sur DVD vidéo. Interprétant l'article 1201.c)1), la Cour a conclu que le DMCA visait le contournement des protections numériques dans ses dispositions antitrafic, mais qu'il ne se préoccupait pas de l'utilisation du contenu après le contournement. Elle a rejeté l'argument selon lequel le Congrès avait eu l'intention d'autoriser le contournement aux fins d'un "usage loyal". Enfin, la Cour n'a pas retenu l'argument des défendeurs selon lequel le DMCA était inconstitutionnel dans la mesure où il supprimait la possibilité de faire un usage loyal des œuvres protégées par une mesure de contrôle d'accès; elle a considéré que la doctrine de l'usage loyal ne garantissait pas que chacun devrait avoir accès aux œuvres protégées par le droit d'auteur.

RealNetworks, Inc. c. Streambox, Inc[125]: une décision antérieure avait été rendue dans une action intentée par RealNetworks en vertu de l'article 1201.a) et 1201.b). RealNetworks avait mis au point un système de distribution de contenu permettant à des titulaires de droits de coder leurs œuvres sous une forme numérique, et de les diffuser aux consommateurs, par l'intermédiaire de RealServer, au moyen d'une méthode sécurisée. Les consommateurs devaient utiliser le logiciel RealPlayer pour accéder aux œuvres. Ensemble, RealServer et RealPlayer permettaient la diffusion en continu des œuvres, mais non leur copie, grâce à une séquence d'authentification et à un commutateur de copie (qui permettait au titulaire des droits de déterminer si la copie était autorisée ou non). Streambox avait pour sa part mis au point un produit qui se substituait au RealPlayer et faisait croire à RealServer que l'authentification avait été effectuée; le produit ne répondait pas à la commutation de copie, de sorte que les consommateurs pouvaient enregistrer le contenu diffusé en continu.

Le tribunal a conclu que l'authentification était une mesure technique qui contrôlait efficacement l'accès au sens de l'article 1201.a). Le commutateur de copie, dès lors qu'il était utilisé avec l'authentification, constituait une mesure technique au sens de l'article 1201.b) parce qu'il permettait à un titulaire de droits de contrôler la copie par les consommateurs. En conséquence, le tribunal a rendu une ordonnance interdisant la distribution du produit, considérant qu'il était principalement conçu pour contourner des mesures techniques de contrôle d'accès et de contrôle de la copie et qu'il n'avait pas d'autre fonction commercialement significative. Les parties ont conclu un accord à l'amiable en septembre 2000.

---

[125] 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000).

Sony Computer Entertainment America, Inc. c. GameMasters, Inc[126]: dans une première décision rendue peu de temps après l'adoption du DMCA, la justice avait considéré qu'un produit vendu par le défendeur contrevenait aux dispositions de l'article 1201.a)2)A). Les consoles de jeux PlayStation de Sony sont conçues pour authentifier les jeux vidéo; chaque jeu vidéo a un code géographique qui doit correspondre à celui de console pour permettre l'utilisation du jeu. Le produit du défendeur se connectait sur la PlayStation et permettait de jouer aux jeux importés ou provenant d'autres régions. Le tribunal a interdit le produit parce qu'il a considéré que sa fonction principale consistait à contourner l'authentification du code géographique.

États-Unis d'Amérique c. Elcom, Ltd.[127]: un informaticien russe du nom de Dmitry Sklyarov a été inculpé de violation des dispositions antitrafic du DMCA. Alors salarié de la société russe Elcom, il avait mis au point un programme de décryptage du logiciel de protection d'Adobe eBook qui permettait aux utilisateurs de lire des livres électroniques dans une multitude de formats et de les copier. Elcom est intervenu pour tenter d'obtenir un non-lieu en contestant le DMCA sur divers points de droit constitutionnel, selon lesquels notamment l'article 1201.b) était trop vague, limitait la liberté d'expression et portait atteinte aux droits des tiers en matière d'usage loyal des œuvres protégées par le droit d'auteur. En mai 2002, le tribunal de district a rejeté chacune de ces prétentions et débouté Elcom. Faisant écho à la décision rendue dans l'affaire *Corley*, le tribunal a conclu que, même si le DMCA réglementait directement la liberté d'expression garantie dans la Constitution, il ne portait pas atteinte au droit du public d'utiliser des œuvres du domaine public ou des œuvres protégées parce qu'il influait seulement sur la capacité d'accéder à certaines copies de ces œuvres et de les utiliser.

Plusieurs autres affaires sont en instance en ce qui concerne l'interprétation et l'application du DMCA. Dans l'une de ces affaires, un fabricant de logiciels cherche à obtenir un jugement déclaratoire indiquant qu'un logiciel qui permet de copier des DVD vidéo n'est pas contraire aux dispositions anticontournement du DMCA[128]. L'une des tendances les plus intéressantes observée aux États-Unis d'Amérique est que le DMCA est maintenant interprété de manière large pour interdire le contournement d'autres techniques employées par les fabricants dans diverses applications industrielles afin d'empêcher les concurrents et leurs produits d'avoir accès au code informatique utilisé par les fabricants pour vérifier que seuls leurs produits sont utilisés par un consommateur[129].

3.3 Union européenne

3.3.1 Cadre juridique

Le 22 mai 2001, l'Union européenne a adopté la directive sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information

---

126 87 F. Supp. 976 2d (N.D. Cal. 1999).

127 203 F. Supp. 1111 2d (N.D. Cal. 2002).

128 *321 Studios* c. *Metro-Goldwyn-Mayer Studios, Inc.*, n° C-02-1955 (N.D. Cal., 23 avril 2002).

129 Voir, par exemple, *Lexmark International, Inc.* c. *Static Control, Components, Inc.*, 253 F. Supp. 2d 943 (E.D. Ky. 2003) (ordonnance de référé) (l'accès au programme de commande de l'imprimante suppose une séquence d'authentification entre l'imprimante et la cartouche d'encre).

(ci-après dénommée “directive sur le droit d’auteur”)[130]. La directive sur le droit d’auteur donne effet aux différentes dispositions des traités de l’OMPI, y compris les dispositions relatives au droit d’auteur sur le droit de reproduction, de communication au public et de distribution, ainsi que les dispositions interdisant le contournement des mesures techniques et de l’information sur le régime des droits. Avant l’adoption de la directive sur le droit d’auteur, le contournement des mesures techniques était traité au niveau européen dans trois autres directives, concernant la protection juridique des programmes d’ordinateur, l’accès conditionnel et le commerce électronique, qui sont décrites ci-dessous.

Ces directives visent à harmoniser la législation des États membres. Les principes qu’elles consacrent ont été ou doivent être transposés par les États membres dans leurs législations nationales respectives. À cet égard, la directive sur le droit d’auteur, par exemple, est moins détaillée, en particulier en ce qui concerne les exceptions, que le DMCA : les contours précis de ces exceptions doivent être définis par la législation interne de chaque État membre. La date limite pour la transposition en droit interne de la directive sur le droit d’auteur était fixée au 22 décembre 2002.

3.3.1.1 Directive sur le droit d’auteur

3.3.1.1.a) Historique

La directive sur le droit d’auteur a été initialement proposée en 1997 et, depuis lors jusqu’à son adoption, elle a fait l’objet de débats intenses à l’échelle communautaire entre les parties intéressées : titulaires de droits, fabricants de matériel informatique et d’électronique grand public et organisations de défense des consommateurs. Le premier projet du texte qui allait devenir la directive sur le droit d’auteur interdisait “toutes les activités” de contournement, prohibant principalement le trafic d’instruments de contournement et non pas les actes de contournement eux-mêmes. Avec le temps, de multiples versions de la directive ont été élaborées et débattues. Parmi les questions les plus importantes discutées pendant cette période figuraient la distinction fondamentale entre l’interdiction, d’une part, de l’acte de contournement et, d’autre part, du trafic d’instruments de contournement, ainsi que la portée des éventuelles exceptions. En outre, la portée de la directive a été élargie, passant de l’interdiction des instruments de contournement des mesures de contrôle du droit d’auteur à l’interdiction des instruments qui permettaient également de contourner les mesures de contrôle d’accès.

3.3.1.1.b) Les dispositions anticontournement

L’article 6 de la directive sur le droit d’auteur donne effet à l’article 11 du WCT et à l’article 18 du WPPT. Comme le DMCA, l’article 6 s’applique à la fois aux actes et aux instruments de contournement et s’applique également d’une manière générale aux mesures techniques de contrôle de l’accès et de gestion du droit d’auteur.

---

130 Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l’harmonisation de certains aspects du droit d’auteur et des droits voisins dans la société de l’information, Journal officiel L167/10, 22/06/2001.

L'article 6.1) interdit les actes de contournement : les États membres doivent prévoir "une protection juridique appropriée contre le contournement de toute mesure technique efficace". Seuls les actes commis en "sachant" ou en ayant des raisons de penser que l'objectif poursuivi est le contournement sont interdits.

L'article 6.2) traite des instruments (et des services) de contournement : les États membres doivent prévoir "une protection juridique appropriée" contre le trafic, ainsi que la possession à des fins commerciales, des instruments qui

– font l'objet d'une promotion, d'une publicité ou d'une commercialisation, dans le but de contourner la protection, ou

– n'ont qu'un but commercial limité ou une utilisation limitée autre que de contourner la protection, ou

– sont principalement conçus, produits, adaptés ou réalisés dans le but de permettre ou de faciliter le contournement de toute mesure technique efficace. Ces critères sont tout à fait semblables à ceux prévus dans le DMCA et, de ce fait, recèlent de semblables ambiguïtés (concernant, par exemple, la signification du terme "principalement"). Il convient toutefois de noter que l'un des alinéas du préambule de la directive sur le droit d'auteur suggère que la législation nationale pourrait également aller au-delà de l'article 6.2) et interdire la "détention à des fins privées" de produits de contournement[131].

La directive sur le droit d'auteur suit ensuite le schéma du DMCA en donnant la définition des "mesures techniques efficaces". À la différence du DMCA, toutefois, c'est cette définition, et non des dispositions distinctes (comme celles figurant à l'article 1201.a) et 1201.b)), qui fixe la portée générale des dispositions anticontournement en indiquant qu'elles s'appliquent à la fois aux mesures de contrôle d'accès et aux mesures de gestion du droit d'auteur.

L'article 6.3) définit les mesures techniques comme comprenant toute technologie qui, "dans le cadre normal de son fonctionnement, est destinée à empêcher ou à limiter, en ce qui concerne les œuvres ou autres objets protégés, les actes non autorisés par le titulaire d'un droit d'auteur ou d'un droit voisin du droit d'auteur prévu par la loi, ou du droit *sui generis* prévu au chapitre III de la directive 96/9/CE [concernant les bases de données]". En conséquence, lorsqu'une mesure technique est utilisée pour s'assurer du consentement du titulaire de droits avant d'accéder à une œuvre ou d'utiliser celle-ci, le contournement de cette mesure – par l'acte ou le produit – est interdit. À cet égard, la notion de "mesures techniques" est plus large que dans le DMCA.

L'article 6.3) définit également ce que l'on entend par mesure technique "efficace". Une mesure technique est "efficace" lorsque l'utilisation d'une œuvre protégée ou d'un autre objet protégé est contrôlée par les titulaires du droit grâce à "l'application d'un code d'accès ou d'un procédé de protection, tel que le cryptage, le brouillage ou toute autre transformation de l'œuvre ou de l'objet protégé ou d'un mécanisme de contrôle de copie qui atteint cet objectif de protection". Dans la mesure où il indique que les mesures à protéger contre le contournement sont uniquement celles qui "atteignent l'objectif de protection", cet article pourrait être interprété comme signifiant que seules les mesures qui sont "efficaces" dans la réalité seront considérées comme "efficaces" aux fins de la directive sur le droit d'auteur et de

---

[131] Alinéa 49 du préambule de la directive sur le droit d'auteur.

la législation d'application. En outre, il n'est pas précisé si un procédé de contrôle d'accès ou de protection doit faire obligatoirement appel au "cryptage, au brouillage ou à toute autre transformation de l'œuvre" pour être "efficace", ni si tout type de "mécanisme" peut être utilisé pour le "contrôle de la copie". En outre, l'article emploie ici le terme de "contrôle de copie" et non celui de "contrôle du droit d'auteur", de sorte que la question s'est posée de savoir si les mesures techniques qui contrôlent des utilisations d'œuvres protégées à d'autres fins que la copie, telles que des interprétations ou exécutions publiques ou la distribution, tombaient réellement sous le coup de l'article 6.

La directive sur le droit d'auteur est plus large que le DMCA car elle interdit également les actes de contournement des mesures de contrôle du droit d'auteur et d'autres actes non autorisés par le titulaire des droits. Supposons, par exemple, qu'une mesure technique soit utilisée pour assurer le caractère conditionnel de l'accès à un contenu protégé et son utilisation, et que l'accès soit consenti à l'utilisateur sur la base d'un accord qui régit l'utilisation ultérieure du contenu. Si l'utilisateur ne respecte pas ces conditions d'utilisation, on serait en présence d'un "acte non autorisé par le titulaire des droits". Un tel acte serait interdit par les dispositions anticontournement de la directive sur le droit d'auteur (aux États-Unis d'Amérique, en revanche, une telle violation de contrat pourrait constituer une infraction à la loi sur le droit d'auteur, mais pas un acte de contournement interdit par le DMCA). Le tableau des interdictions dans la directive sur le droit d'auteur se présente de la manière suivante :

	Acte de Contournement	**Instruments de contournement**
Mesure technique de contrôle de l'accès	Interdit (art. 6.1))	Interdits (art. 6.2))
Mesure technique de contrôle du droit d'auteur	Interdit (art. 6.1))	Interdits (art. 6.2))

3.3.1.1.c) Limitations et exceptions

Comme le DMCA, la directive sur le droit d'auteur prévoit également des limitations et des exceptions, mais en quelque sorte d'une manière tout à fait différente de la législation des États-Unis d'Amérique. L'article 6.4) ne prévoit pas d'exception directe aux dispositions anticontournement comme le fait l'article 1201 du DMCA. Il privilégie à la place les arrangements du secteur privé. L'article 6.4) s'appuie essentiellement sur la volonté des titulaires de droits d'autoriser librement l'accès aux œuvres protégées par des mesures techniques et leur utilisation dans certaines circonstances. Ce n'est que s'ils ne le font pas que les États membres doivent, aux termes de directive sur le droit d'auteur, prendre des "mesures appropriées pour s'assurer que les bénéficiaires des exceptions ou des limitations" spécifiques prévues à l'article 5 puissent en tirer parti. La question de savoir quand et comment un État membre doit déterminer qu'il convient d'agir, parce qu'il n'existe aucun accord volontaire avec les titulaires de droits donnant réellement effet à ces exceptions et limitations, n'est pas abordée dans la directive sur le droit d'auteur.

La démarche retenue dans la directive sur le droit d'auteur envisage donc plusieurs étapes avant qu'une exception ou une limitation ne soit applicable. Premièrement, les États

membres doivent agir uniquement "en l'absence de mesures volontaires prises par les titulaires de droits, y compris les accords entre titulaires de droits et d'autres parties". Ces "autres parties" pourraient notamment être des fabricants de produits d'électronique grand public et de matériel informatique, des consommateurs et des vendeurs de mesures techniques. En ce qui concerne les bénéficiaires des exceptions qui sont des utilisateurs, on ne voit pas clairement quelles pourraient être les autres parties à un dialogue ou à un accord. La directive sur le droit d'auteur impose d'observer un "délai raisonnable" pour laisser au titulaires de droits le temps de conclure de tels accords avant l'intervention des États membres[132].

Deuxièmement, les mesures que les États membres doivent prendre ne supposent pas que les exceptions soient incorporées dans la législation nationale. Elles peuvent supposer que les titulaires de droits (et, vraisemblablement, les mesures techniques qu'ils emploient) mettent en place des soupapes de sûreté pour certains actes bien précis des utilisateurs. Il convient également de noter que rien ne permet de penser que les États membres mettront en application ces exceptions d'une manière harmonisée. En outre, la forme de l'intervention des États membres, en cas d'absence de mesures volontaires, n'est pas précisée non plus, de sorte qu'elle peut différer selon les États membres.

Troisièmement, les exceptions prévues par les titulaires de droits à l'intention des bénéficiaires ne doivent être accordées que "dans la mesure nécessaire" et pas plus. Quatrièmement, seules les personnes qui ont un "accès licite" à l'œuvre peuvent bénéficier d'une exception. Cinquièmement, et comme indiqué ci-dessous, un régime spécial s'applique en ce qui concerne les exceptions ou limitations applicables au contournement à des fins privées.

Ce régime entier d'exceptions comporte toutefois une mise en garde supplémentaire qui, à certains égards, peut être lourde de conséquences pour l'ensemble. L'article 6.4)4) prévoit qu'aucune des obligations en ce qui concerne les accords volontaires et l'intervention des États membres ne s'applique aux œuvres "qui sont mises à la disposition du public à la demande selon les dispositions contractuelles convenues entre les parties de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit individuellement". Cette réserve vise à tenir compte de différents modèles de distribution et vise principalement les œuvres mises à la disposition des utilisateurs dans le cadre de services interactifs à la demande[133]. Ces services comprendraient les services de paiement à l'utilisation, de lecture, téléchargement ou vidéo à la demande, qui sont distincts des services d'abonnement ou de diffusion en ligne. Dans ces conditions, la directive sur le droit d'auteur prévoit que les titulaires de droits, compte tenu du contrat direct conclu avec l'utilisateur en ce qui concerne l'utilisation déterminée de l'œuvre, n'ont pas à prévoir d'exceptions ni de limitations aux mesures de contrôle de l'accès ou de la copie.

L'article 5 énonce les exceptions et limitations au droit d'auteur que les États membres peuvent prévoir (sans être tenus de le faire) en ce qui concerne l'utilisation des œuvres protégées (d'ailleurs, plusieurs États membres ne prévoient pas de larges exceptions en ce qui concerne la copie privée, par exemple). Par conséquent, l'article 5 et de l'article 6 se combinent de la manière suivante : le contournement des mesures techniques est autorisé lorsque l'acte en question (ou le trafic de produits de contournement proprement dits) est

---

132 Alinéa 51 du préambule.

133 Alinéa 53 du préambule.

entrepris afin de bénéficier des exceptions et limitations inscrites dans la législation nationale. Ainsi, à la différence du DMCA, où les exceptions visées à l'article 1201 sont essentiellement des défenses contre un acte de contournement, la directive sur le droit d'auteur suggère qu'un État membre peut (sans être tenu de le faire) autoriser certains actes que les mesures techniques sont censées permettre (que ce soit sur une base volontaire ou d'une autre manière). Les actes qui peuvent être autorisés sont indiqués ci-dessous.

Reproductions autorisées : l'article 5 porte que les États membres peuvent prévoir dans leur législation nationale des exceptions aux droits de reproduction (5.2)) et de reproduction et de communication (5.2) et 3)). Les exceptions ci-après sont notamment visées :

– reproductions effectuées sur papier, à condition que les titulaires de droits reçoivent une compensation équitable[134];

– reproductions effectuées par des bibliothèques accessibles au public, des établissements d'enseignement ou des musées ou par des archives à des fins non commerciales[135];

– enregistrements éphémères effectués par des organismes de radiodiffusion et archivage de ces enregistrements[136];

– reproductions effectuées par des institutions sociales sans but lucratif, telles que les hôpitaux ou les prisons, à condition que les titulaires de droits reçoivent une compensation équitable[137];

– utilisations à des fins d'enseignement ou de recherche scientifique non commerciales, sous réserve de l'indication de la source, à moins que cela ne s'avère impossible[138];

– utilisations au bénéfice de personnes affectées d'un handicap qui sont directement liées au handicap en question et sont de nature non commerciale, dans la mesure requise par ledit handicap[139]; et

– utilisation à des fins de sécurité publique ou pour assurer la couverture de procédures publiques[140].

Comme indiqué précédemment, ces actes semblent être privilégiés aux fins de l'article 6 dans la mesure où les mesures techniques sont censées s'y adapter. L'article 5 énonce des exceptions et limitations à l'égard d'autres actes, tels que compte rendu d'événements d'actualité, critique ou revue, utilisation de discours politiques ou utilisation à des fins de célébrations religieuses. Ces actes sont aussi des usages légitimes et font à ce titre l'objet d'exceptions dans les lois nationales sur le droit d'auteur. Cela étant, l'article 6 n'exige pas que ces exceptions supplémentaires soient privilégiées par les titulaires de droits ou les États membres.

---

134 Article 5.2)a) de la directive sur le droit d'auteur.
135 Article 5.2)c).
136 Article 5.2)d).
137 Article 5.2)e).
138 Article 5.3)a).
139 Article 5.3)b).
140 Article 5.3)e).

Copie privée : l'article 5.2)b) permet aux États membres de prévoir une exception pour les reproductions faites par "une personne physique pour un usage privé". Là encore, un alinéa du préambule de la directive sur le droit d'auteur dispose que les États membres doivent encourager le recours aux mesures volontaires pour permettre d'atteindre les objectifs visés par ladite exception et qu'ils peuvent prendre eux-mêmes des mesures si aucune mesure volontaire n'a été prise "dans un délai raisonnable"[141]. De plus, rien ne dit que les États membres interviendront réellement en l'absence de telles mesures ni qu'ils le feront de manière harmonisée.

Ces reproductions ne sont autorisées qu'à des fins qui ne sont ni directement ni indirectement commerciales. En outre, les titulaires de droits doivent recevoir une "rémunération équitable" qui "prend en compte l'application ou la non-application des mesures techniques". En ce qui concerne ce dernier point, le lien entre l'utilisation des systèmes de gestion numérique des droits et d'autres mesures techniques ou régimes de taxes pour la copie privée, qui visent à assurer aux titulaires de droits une rémunération équitable, a fait l'objet d'intenses débats au niveau communautaire et est examiné à la section 5.1.3.

Cette disposition a été parmi les plus discutées avant l'adoption de la directive sur le droit d'auteur. L'article 6.4)2) prévoit expressément que les États membres peuvent prendre des mesures vis-à-vis des titulaires de droits pour s'assurer que ce type de copie privée à des fins non commerciales soit autorisé, à moins que les titulaires de droits prévoient cette possibilité dans les mesures techniques qu'ils emploient. À cet égard, la directive sur le droit d'auteur autorise également l'utilisation de mesures techniques visant à limiter le nombre de reproductions pouvant être faites en application de cette exception (il s'agit vraisemblablement du nombre de copies privées autorisées par personne.)

Dans cette disposition, la directive sur le droit d'auteur est beaucoup plus directe et permissive que le DMCA dans le lien entre copie privée et contournement. Alors que le contournement aux fins de l'usage loyal (y compris la copie privée) reste interdit aux États-Unis d'Amérique, la directive sur le droit d'auteur considère que la copie à usage privé peut justifier l'obligation faite aux titulaires de droits de prévoir cette utilisation dans les mesures techniques qu'ils mettent en œuvre.

D'autres exceptions et limitations sont énoncées dans le préambule de la directive sur le droit d'auteur. Toutefois, les alinéas du préambule n'ont pas la même force obligatoire que les articles du dispositif.

Ingénierie inverse : un alinéa du préambule de la directive sur le droit d'auteur prévoit que les États membres ne doivent ni empêcher, ni gêner la mise au point ou l'utilisation de tout moyen permettant de contourner une mesure technique nécessaire pour permettre la décompilation ou le fonctionnement de programmes d'ordinateur, conformément à la directive sur les programmes d'ordinateur[142]. Cette activité d'ingénierie inverse doit être conforme à la directive au sens où elle doit être entreprise à des fins d'interfonctionnement.

---

141 Aliéna 52 du préambule.

142 Alinéa 50 du préambule de la directive sur le droit d'auteur, mentionnant l'article 5.3) et l'article 6 de la directive 91/250/CEE du Conseil concernant la protection juridique des programmes d'ordinateur, Journal officiel L 122/42, 17/05/1991 [ci-après dénommée "directive sur les programmes d'ordinateur"].

Recherche cryptographique : un autre alinéa du préambule stipule que la protection juridique ne doit pas "faire obstacle à la recherche sur la cryptographie"[143].

Clause d'exemption : en ce qui concerne la clause d'exemption, la directive sur le droit d'auteur ne protège pas autant les produits courants que le DMCA, selon lequel ces produits n'ont pas à être adaptés à des mesures techniques particulières. La directive sur le droit d'auteur ne contient aucune exemption spécifique à cet effet, bien qu'un alinéa du préambule soit calqué sur l'article 1201.c)3) du DMCA : la protection juridique assurée par les États membres "n'implique aucune obligation de mise en conformité des dispositifs, produits, composants ou services avec ces mesures techniques, pour autant que lesdits dispositifs, produits, composants ou services ne tombent pas, par ailleurs, sous le coup de l'interdiction prévue à l'article 6"[144]. Cet alinéa prévoit que la protection juridique ne doit pas interdire les dispositifs ou activités qui ont, "sur le plan commercial, un objet ou une utilisation autre que le contournement de la protection technique". Cet alinéa va plus loin que le texte du DMCA lui-même, bien que l'histoire de l'adoption du DMCA milite en faveur de la même interprétation.

3.3.1.1.d) Information sur le régime des droits

L'article 7 de la directive sur le droit d'auteur impose aux États membres de prévoir une protection juridique appropriée contre quiconque supprime ou modifie "sciemment" "l'information sur le régime des droits" se présentant sous forme électronique ou distribue des œuvres à l'égard desquelles cette information a été supprimée ou modifiée sans autorisation. Cette suppression ou cette modification est interdite si et dans la mesure où la personne sait ou a des raisons valables de penser que, ce faisant, elle entraîne, permet, facilite ou dissimule une atteinte à un droit d'auteur ou droit voisin du droit d'auteur, ou au droit *sui generis* sur les bases de données.

"L'information sur le régime des droits" est définie comme à l'article 1202 du DMCA. Elle comprend les informations permettant d'identifier l'œuvre ou qui s'y rapporte, ainsi que les informations sur les conditions et modalités d'utilisation de l'œuvre et tout numéro ou code représentant ces informations.

L'alinéa du préambule de la directive sur le droit d'auteur relatif à l'information sur le régime des droits souligne le lien entre le traitement des données à caractère personnel obtenues au moyen des systèmes de gestion numérique des droits ou d'autres moyens techniques et les exigences de la législation européenne sur le respect de la vie privée[145]. Ce lien est examiné à la section 5.2.1.

3.3.1.1.e) Voies de droit

Bien que la directive sur le droit d'auteur impose aux États membres de transposer ses dispositions dans leur législation nationale, elle ne prévoit pas de sanctions en cas de violation de ses dispositions anticontournement. Cet aspect est laissé au soin des États membres.

---

143 Alinéa 48 du préambule de la directive sur le droit d'auteur.

144 *Id.*

145 Alinéa 57 du préambule de la directive sur le droit d'auteur.

L'article 8 de la directive impose toutefois expressément aux États membres de prévoir des "sanctions et voies de recours appropriées" en cas d'atteinte aux droits. Ces voies de recours doivent notamment donner aux titulaires de droits la possibilité d'intenter une action en dommages-intérêts, d'obtenir une ordonnance sur requête et la saisie du matériel concerné ainsi que des produits de contournement. Cet article s'inspire en grande partie des dispositions de l'Accord sur les ADPIC relatives aux moyens de faire respecter les droits qui sont examinées à la section 3.2.1.1.

3.3.1.1.f) Suivi et mise en œuvre

La directive sur le droit d'auteur prévoit plusieurs mécanismes pour évaluer les incidences de l'utilisation des mesures techniques sur le marché intérieur et les utilisateurs. Premièrement, tous les trois ans, la Commission européenne doit présenter un rapport sur l'application de la directive. Le rapport doit indiquer si l'article 6 "confère un niveau suffisant de protection et si des actes permis par la loi sont affectés par l'utilisation de mesures techniques efficaces"[146]. Cette étude s'apparente en quelque sorte à la procédure bisannuelle que doit mettre en œuvre le Bureau du droit d'auteur en vertu de l'article 1201.a)1) du DMCA, pour déterminer si les utilisateurs sont lésés par les mesures techniques.

Deuxièmement, si besoin est, la Commission pourrait présenter des propositions de modification de la directive sur le droit d'auteur[147]. Troisièmement, la directive sur le droit d'auteur institue un comité de contact chargé d'examiner les effets de la directive sur le fonctionnement du marché intérieur et "de fonctionner comme un forum d'évaluation du marché numérique des œuvres et des autres objets, y compris la copie privée et l'usage de mesures techniques"[148]. D'une manière générale, le processus d'examen et de modification prévu dans la directive sur le droit d'auteur semble être plus large que celui prévu dans le DMCA, qui est de portée limitée et qui place très haut la barre des exceptions.

---

146 Article 12.1) de la directive sur le droit d'auteur.

147 *Id.*

148 Article 12.3) et 4).

3.3.1.1.g) Mise en œuvre

Le 14 juillet 2003, la Commission européenne a publié un communiqué de presse indiquant que seuls la Grèce et le Danemark avaient respecté la date limite du 22 décembre 2002 pour mettre en œuvre la directive sur le droit d'auteur, et que l'Italie et l'Autriche l'avaient fait ultérieurement (en avril et juin 2003, respectivement); la Commission a déclaré qu'elle intenterait des procédures à l'encontre des États membres qui n'avaient pas transposé la directive sur le droit d'auteur dans leur droit interne[149]. L'Allemagne a aussi adopté une loi de mise en application de la directive. D'autres États membres sont en train de faire de même. Un avant-projet de loi a par exemple été établi en France, et des consultations sont en cours dans divers autres États membres.

Italie : l'Italie a transposé la directive sur le droit d'auteur au moyen d'un décret-loi du 9 avril 2003[150]. Ce décret-loi porte modification de la loi sur le droit d'auteur et les droits voisins. L'article 23 du décret reprend les dispositions de l'article 6.3) de la directive sur le droit d'auteur concernant la définition des "mesures techniques" et de leur efficacité. L'utilisation abusive de procédés de contournement (c'est-à-dire, l'acte de contournement), y compris l'achat ou la location d'instruments de contournement, est passible de sanctions administratives[151]. Le trafic d'instruments et de services de contournement fait l'objet de sanctions pénales[152].

Allemagne : à la mi-juillet 2003, l'Allemagne a adopté une loi d'application de la directive sur le droit d'auteur. Cette loi définit les "mesures techniques" et les mesures techniques "efficaces" conformément à la directive sur le droit d'auteur. Un nouvel article 95a a été ajouté à la loi de 1965 afin d'interdire le contournement délibéré des mesures techniques efficaces et le trafic d'instruments de contournement[153].

Certains actes de trafic d'instruments de contournement, de même que la propriété ou la détention de tels instruments à des fins commerciales ou la fourniture d'un service de ce type, constituent des infractions administratives (et non pénales); chaque Land allemand décide de l'autorité compétente pour les sanctions administratives contre les auteurs d'infractions. Le trafic d'instruments de contournement à des fins commerciales tombe sous le coup de sanctions pénales. Il en va de même du contournement intentionnel, mais uniquement lorsque l'acte n'est pas destiné exclusivement à l'usage privé de la personne concernée (ou de personnes proches); une sanction plus sévère est prévue lorsque l'acte a été commis dans un but commercial[154]. Bien que la loi ne l'indique pas expressément, on suppose que les

---

149 Voir Commission européenne, *Internal Market: Commission moves against 13 Member States for failure to implement EU legislation* (14 juillet 2003), disponible à l'adresse *http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/1005|0|RAPID&lg=en&display*.

150 Voir le décret-loi n) 68 du 9 avril 2003, *Gazzetta Ufficiale*, n° 87 (14 avril 2003), à l'adresse *http://www.giustizia.it/cassazione/leggi/dlgs68_03.html*.

151 *Id.* article 28 (portant modification de l'article 174-ter de la loi sur le droit d'auteur et les droits voisins (loi numéro 633 du 22 avril 1941, modifiée par le décret-loi n° 154 du 26 mai 1997)).

152 *Id.*, article 26 (portant modification de l'article 171-ter de la loi sur le droit d'auteur et les droits voisins).

153 Voir *Drucksache* 271/03 (2 mai 2003), art. 1, alinéa 34 (visant à modifier la loi sur le droit d'auteur en y ajoutant un nouvel article 95a à 95d).

154 *Id.*, article 42 (visant à insérer un nouvel article 111a).

titulaires de droits auront également le droit d'intenter des actions privées contre les auteurs d'infraction.

La solution allemande pour la mise en œuvre des exceptions et limitations prévues à l'article 5 de la directive sur le droit d'auteur a retenu une certaine attention, et a été source de préoccupation pour les titulaires de droits. Un nouvel article 95b de la loi sur le droit d'auteur leur impose en effet l'obligation de donner aux utilisateurs les moyens de bénéficier des exceptions prévues par la loi sur le droit d'auteur dès lors qu'ils ont accès de manière licite aux œuvres. La loi sur le droit d'auteur prévoit notamment une exception en faveur de la réalisation d'une reproduction unique d'une œuvre pour l'usage privé sur n'importe quel support. Or, bien que l'article 95b mentionne cette exception, il limite l'autorisation de contournement (à la seule fin de la mise en œuvre de l'exception) aux reproductions effectuées sur papier. L'exception au titre de la copie privée n'est toutefois pas applicable lorsque les copies sont réalisées à partir de sources manifestement illicites.

Il est difficile de savoir comment les titulaires de droits peuvent se conformer à ces exigences lorsque, par exemple, la mesure technique n'est pas associée directement à l'œuvre elle-même mais au mode de distribution. Cette question préoccupe les titulaires de droits car, s'ils ne donnent pas aux utilisateurs les moyens de bénéficier de l'exception, ils se rendent coupables d'une infraction administrative. La loi prévoit en outre expressément la nullité des clauses contractuelles qui empêcheraient les utilisateurs de tirer parti des exceptions; toutefois, conformément à l'article 6.4) de la directive sur le droit d'auteur, le droit de bénéficier des exceptions serait inapplicable s'agissant d'œuvres distribuées en application d'accords contractuels qui permettent à des utilisateurs d'y accéder de l'endroit et au moment de leur choix[155]. En outre, les bénéficiaires des exceptions pourraient exiger des titulaires de droits qu'ils leur fournissent les moyens (à la discrétion des titulaires de droits) d'en bénéficier. Pour remplir leurs obligations, les titulaires de droits pourraient, par exemple, mettre à la disposition des bénéficiaires une copie analogique ou une autre copie protégée de l'œuvre, la loi n'autorisant pas les bénéficiaires à pirater ou contourner les mesures de protection.

La loi prévoit que les titulaires de droits doivent étiqueter les œuvres et objets protégés par des mesures techniques; toute omission à cet égard constituerait une faute administrative. Cette obligation va au-delà des conditions imposées par la directive sur le droit d'auteur. La question de l'étiquetage des œuvres téléchargées, par exemple, depuis des serveurs situés à l'extérieur de l'Allemagne reste à trancher.

La loi prévoit en outre que ses dispositions entreront en vigueur de manière progressive. La mise en œuvre des dispositions concernant les exceptions devrait être différée d'un an afin de permettre aux titulaires de droits et organismes de représentation des bénéficiaires de négocier des arrangements volontaires.

France : en France, le Ministère de la culture et de la communication a rédigé un projet de loi pour transposer la directive sur le droit d'auteur dans le droit interne. Le projet actuel contient un chapitre sur les mesures techniques qui modifierait le Code de la propriété intellectuelle en y ajoutant des articles autorisant les auteurs à employer de telles mesures. Les actes de contournement et le trafic d'instruments de contournement seraient interdits. En revanche, les auteurs seraient tenus de permettre aux destinataires des exceptions prévues

---

155 *Id.*, article 34 (visant à l'inclusion d'un nouvel article 95b).

dans le code (notamment le droit à la copie privée) de bénéficier de ces exceptions, malgré l'utilisation des mesures techniques, lorsqu'ils ont accès de manière licite à l'œuvre (l'exception visée à l'article 6.4) de la directive sur le droit d'auteur, en ce qui concerne les services "sur demande", est aussi reprise dans le projet de loi.). D'une manière générale, les sanctions en cas de contournement non autorisé et de trafic seraient alignées sur celles prévues dans le code pour les atteintes au droit d'auteur.

Royaume-Uni : en août 2002, la Direction du droit d'auteur de l'Office des brevets a publié un document consultatif sur la mise en œuvre de la directive au Royaume-Uni, qui présentait également les modifications à apporter à la législation[156]. De nombreux commentaires ont été reçus sur les amendements à mettre en œuvre pour donner effet à l'article 6 de la directive sur le droit d'auteur. Compte tenu de ces commentaires, l'Office des brevets a indiqué en juin 2003 que l'examen des amendements à apporter à la législation avait été différé mais que les travaux de mise en œuvre de la directive sur le droit d'auteur au Royaume-Uni étaient bien avancés.

3.3.1.2 Autres directives applicables

La directive sur le droit d'auteur n'était pas la première tentative faite par l'Union européenne pour protéger la gestion numérique des droits et d'autres mesures techniques de protection des œuvres. Trois directives antérieures méritent d'être mentionnées à cet égard. Elles sont décrites brièvement ci-après.

3.3.1.2.a) Directive sur les programmes d'ordinateur

La directive sur les programmes d'ordinateur, qui a été adoptée en 1991, traite des mesures techniques utilisées pour protéger les logiciels[157]. L'article 7 de cette directive impose expressément aux États membres de prévoir des mesures appropriées contre quiconque met "en circulation" ou détient à des fins commerciales "tout moyen ayant pour seul but de faciliter la suppression non autorisée ou la neutralisation de tout dispositif technique éventuellement mis en place pour protéger un programme d'ordinateur"[158].

3.3.1.2.b) Directive sur l'accès conditionnel

La directive sur l'accès conditionnel a été adoptée en 1998 pour protéger l'accès à différentes sortes de services assurés par voie électronique et par des moyens d'accès

---

156 Voir EC Directive 2001/29/EC on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society: Consultation Paper on Implementation of the Directive in the United Kingdom (Copyright Directorate : 7 août 2002), à l'adresse *http://www.patent.gov.uk/about/consultations/eccopyright/pdf/ 2001_29_ec.pdf*.

157 Directive 91/250/CEE du Conseil concernant la protection juridique des programmes d'ordinateur, Journal officiel L 122/42, 17/05/1991 [ci-après dénommée "directive sur les programmes d'ordinateur"].

158 Article 7 de la directive sur les programmes d'ordinateur.

conditionnel et garantir la rémunération de ces services[159]. La directive sur l'accès conditionnel vise à garantir la rémunération du prestataire de services et non le contenu du service proprement dit. Le champ d'application de la directive sur l'accès conditionnel est particulièrement vaste. Il va des services en ligne à la radiodiffusion télévisuelle et sonore avec et sans fil (y compris par satellite), en passant par les "services de la société de l'information"[160].

L'accès conditionnel est défini comme désignant "toute mesure et/ou tout dispositif techniques subordonnant l'accès au service protégé sous une forme intelligible à une autorisation individuelle préalable"[161]. La directive sur l'accès conditionnel interdit le trafic de "dispositifs illicites". Les dispositifs illicites s'entendent de "tout équipement ou logiciel conçu ou adapté pour permettre l'accès à un service protégé sous une forme intelligible sans l'autorisation du prestataire de services"[162].

La directive sur l'accès conditionnel impose aux États membres d'interdire la fabrication, la vente et la location de tels dispositifs, ainsi que leur détention à des fins commerciales, de même que leur installation, leur entretien ou leur remplacement et leur promotion commerciale[163]. Les dispositions relatives aux sanctions et voies de droit figurant à l'article 5 sont semblables à celles de la directive sur le droit d'auteur. La directive sur l'accès conditionnel n'interdit ni l'acte de contournement ni la détention d'un dispositif illicite pour usage personnel. La date limite pour la transposition en droit interne était fixée au 28 mai 2000.

En s'inspirant en grande partie de la directive sur l'accès conditionnel, le Conseil de l'Europe a rédigé la Convention européenne sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel[164]. La convention, qui a été adoptée par le Comité des ministres en octobre 2000 et est ouverte à la signature depuis le 24 janvier 2001, s'appliquerait aux pays européens, qu'ils soient membres ou non de l'Union européenne.

3.3.1.2.c) Directive sur le commerce électronique

La directive sur le commerce électronique a été adoptée en juillet 2000 pour dresser le cadre de base du commerce électronique au sein de la Communauté européenne[165]. La date limite pour la transposition en droit interne était fixée au 17 janvier 2002. La directive sur le

---

159 Directive 98/84/CE du Parlement européen et du Conseil du 20 novembre 1998 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel, Journal officiel L 320/54, 28/11/1998 [ci-après dénommée "directive sur l'accès conditionnel"].

160 Article 2.a) de la directive sur l'accès conditionnel.

161 Article 2.b).

162 Article 2.e).

163 Article 4.

164 Convention européenne sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel, STE 178, disponible à l'adresse *http://conventions.coe.int/Treaty/FR/Cadreprincipal.htm*

165 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, Journal officiel L 178/1, 17/07/2000 [ci-après dénommée "directive sur le commerce électronique"].

commerce électronique contient plusieurs dispositions importantes qui sont applicables à l'utilisation des techniques de gestion numérique des droits pour la distribution et la protection du contenu acheminé aux consommateurs par voie électronique.

Tout d'abord, les États membres sont tenus de veiller à la possibilité de conclure des contrats par voie électronique, ainsi qu'aux effets et à la validité juridique de ces contrats[166]. En conséquence, les licences en ligne et autres contrats électroniques peuvent servir de base à la distribution en ligne de contenu à l'intention des utilisateurs. Diverses dispositions imposent aux prestataires de services l'obligation d'informer clairement les consommateurs avant la passation de commande et d'accuser réception des commandes électroniques[167].

Ensuite, la directive sur le commerce électronique exonère les prestataires de services agissant en qualité d'intermédiaires de la responsabilité au titre du contenu qu'ils transmettent ou qu'ils stockent. Ces clauses d'exonération sont semblables à celles du DMCA, comme indiqué à la section 3.2.1.2. L'article relatif au stockage temporaire ("caching") prévoit que les États membres ne peuvent pas engager la responsabilité d'un prestataire de services au titre du stockage automatique, intermédiaire et temporaire d'informations aux fins de leur transmission ultérieure, sous réserve de plusieurs conditions. L'une de ces conditions est que le prestataire ne doit pas entraver "l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information". Cette disposition est calquée sur la principale condition à la reconnaissance de l'immunité prévue à l'article 512.i)1)B) du DMCA. Comme aux États-Unis d'Amérique, la directive sur le commerce électronique prévoit en Europe que le prestataire de services perd son immunité dès lors que le processus de stockage temporaire du contenu interfère avec les systèmes de gestion numérique des droits et d'autres mesures techniques mises en place par les titulaires de droits pour suivre l'utilisation de l'information. Les prestataires de services sont donc fortement encouragés à préserver les mesures techniques reconnues par l'industrie s'ils ne veulent pas être poursuivis pour atteinte au droit d'auteur (ou à d'autres droits).

3.3.2 Direction générale de la société de l'information de la Commission européenne : atelier sur la gestion numérique des droits

Après avoir adopté la directive sur le droit d'auteur, la Commission européenne a entamé un processus visant à explorer une série de questions de suivi, dont les moyens que la Commission elle-même pourrait mettre en œuvre pour favoriser l'élaboration d'un régime de gestion numérique des droits. En février 2002, la Direction générale de la société de l'information a lancé ce qui est devenue un processus d'ateliers multiples pour mettre en présence les différentes parties prenantes afin d'étudier les questions relatives à la gestion numérique des droits et notamment l'éventuelle existence d'un consensus sur les mesures à prendre par la Commission[168].

---

166 Article 9.1) de la directive sur le commerce électronique.

167 Articles 10 et 11.

168 Voir le rapport sur l'atelier sur la gestion numérique des droits (16 avril 2002), disponible à l'adresse *http://europa.eu.int/information_society/topics/multi/digital_rights/doc/workshop2002/workshop_report1.pdf*.

Parmi les principaux thèmes abordés – en particulier du point de vue des entreprises technologiques et des consommateurs – figurait la question de savoir si la mise en œuvre de mesures de gestion numérique des droits justifiait l'abandon des taxes imposées sur les dispositifs et les supports d'enregistrement. Les titulaires de droits, quant à eux, étaient plus enclins à exhorter la Commission ou d'autres institutions à intervenir pour régler les problèmes de protection du contenu en l'absence de progrès et d'accords dans le secteur privé. Ce processus a été entamé pour faciliter les discussions et les échanges de vues plutôt qu'avec un but fixe à l'esprit. Il convient de noter que la Commission – dans la recherche du rôle qu'elle pourrait jouer – a lancé cette série d'ateliers à un moment où le Congrès des États-Unis d'Amérique examinait le projet de loi sur la télévision numérique à haut débit (Consumer Broadband and Digital Television Promotion Act), qui aurait défini le rôle du gouvernement en matière d'établissement de normes.

Ce processus était également motivé par l'alinéa 54 du préambule de la directive sur le droit d'auteur, concernant le risque selon lequel les différences entre mesures techniques pourraient conduire à une incompatibilité des systèmes au sein de la Communauté. Dans la mesure où cela pourrait créer des obstacles au commerce interne, la Direction générale de la politique des entreprises s'intéressait aussi à la question de savoir s'il fallait normaliser les systèmes de gestion numérique des droits.

À la suite de l'adoption de la directive sur le droit d'auteur, la Commission européenne avait demandé que le CEN/ISSS (le système de normalisation de la société de l'information au sein du Comité européen de normalisation) examine la situation de la gestion numérique des droits. Le groupe chargé de la gestion numérique des droits du CEN/ISSS a été établi en octobre 2001. Un projet de rapport très volumineux, dont la première version est datée du 31 janvier 2003, a été publié aux fins de commentaires[169]. Le rapport récapitule essentiellement les vues des diverses parties prenantes, sans proposer de recommandations de politique générale, de normes ni de conclusions.

Le processus de la Direction générale de la société de l'information sur la gestion numérique des droits a donné lieu à quatre ateliers. Chacun d'entre eux était dirigé par un secteur particulier, mais des représentants de tous les secteurs étaient invités à y participer. L'atelier final, au cours duquel ces vues ont été présentées, a eu lieu le 25 mars 2003[170].

Organismes de défense des utilisateurs et des consommateurs : le premier atelier a été dirigé par des organismes de défense des utilisateurs et des consommateurs, tels que le Bureau européen des unions de consommateurs, ou "BEUC", et des distributeurs de contenu représentés par la European Digital Media Association ("EdiMA"). Parmi les thèmes abordés figurait le risque que les systèmes de gestion numérique des droits ne restreignent la capacité des consommateurs d'accéder au contenu, y compris par la copie privée. Ils ont demandé instamment que les systèmes de gestion numérique des droits eux-mêmes respectent le cadre juridique, y compris la possibilité de bénéficier des exceptions prévues par la directive sur le droit d'auteur, et d'assurer l'interfonctionnement des techniques. À cet égard, les consommateurs ont exprimé des préoccupations quant au risque de renoncer par contrat, dans

---

169 Voir *Digital Rights Management : Draft Report*, CEN/ISSS (Projet 1.2, 5 février 2003), à l'adresse *http://www.cenorm.be/isss/DRM/draft_report1_2.pdf*.

170 Voir *http://europa.eu.int/information_society/topics/multi/digital_rights/events/index_en.htm* (décrivant les divers événements qui ont eu lieu dans le cadre du processus de la Direction générale de la société de l'information sur la gestion numérique des droits).

le cadre de systèmes de gestion numérique des droits, à des droits qui leur sont reconnus en vertu des exceptions au droit d'auteur. Ils ont également demandé aux gouvernements de veiller à ce que les titulaires de droits ne puissent employer les systèmes de gestion numérique des droits pour entraver l'accès aux œuvres du domaine public.

Parmi les autres questions de politique générale soulevées par les utilisateurs figurait la nécessité d'une information claire sur le fait que les produits sont protégés contre la copie et d'une suppression des taxes, afin que les titulaires ne soient pas indemnisés deux fois, une première fois par le biais d'une taxe et une seconde dans le cadre d'un paiement facilité par les systèmes de gestion numérique des droits. Ils ont donc demandé que les taxes soient progressivement supprimées après la mise en œuvre des systèmes de gestion numérique des droits.

La possibilité de voir les systèmes de gestion numérique des droits recueillir des données personnelles et porter atteinte à la vie privée constitue un autre sujet de préoccupation pour les consommateurs. Ils ont également demandé instamment que les normes de gestion numérique des droits ne soient pas édictées par le gouvernement mais soient le fruit d'efforts menés par l'industrie.

Industries de l'infocommunication et de l'électronique grand public : les industries technologiques, par l'intermédiaire de la European Information and Communication Technology Association ("EICTA"), ont dirigé le deuxième atelier. La session a été consacrée à s'assurer que les participants avaient une vision commune de l'état de la technique dans le domaine de la gestion numérique des droits et à expliquer que les systèmes de gestion numérique des droits visaient à faire en sorte que les personnes honnêtes le restent plutôt qu'à éradiquer le piratage commercial. Les industries ont également demandé que les titulaires de droits s'assurent que les systèmes de gestion numérique des droits permettent aux consommateurs de bénéficier des exceptions au droit d'auteur, conformément à leurs demandes et à leurs attentes légitimes.

L'un des arguments fondamentaux des industries technologiques est que les taxes pour la copie privée frappant les dispositifs et supports numériques sont inutiles. Tout d'abord, les titulaires de droits peuvent contrôler la copie privée de leurs œuvres au moyen des systèmes de gestion numérique des droits, qui ouvrent la perspective de paiements multiples de la part des consommateurs. Ensuite, le champ d'application des taxes dans l'environnement numérique pourrait s'élargir de manière démesurée, étant donné qu'une large gamme des dispositifs et de supports – allant des ordinateurs individuels et des agendas personnels aux décodeurs numériques, en passant par les mémoires amovibles ou intégrées – permet de manipuler et de stocker du contenu. Il ne serait pas judicieux d'imposer des taxes sur des dispositifs et des supports universels indépendamment de leur utilisation réelle.

Les industries technologiques ont continué de privilégier la participation du secteur privé, plutôt que public, à l'établissement des systèmes de gestion numérique des droits. Le secteur de l'infocommunication et de l'électronique grand public s'est opposé à toute suggestion en faveur de normes gouvernementales concernant les techniques à employer. Il a également fait valoir que les questions d'interfonctionnement devraient être abordées au sein d'instances volontaires et dirigées par l'industrie.

Titulaires de droits : les organismes de représentation des titulaires de droits, y compris la Motion Picture Association ("MPA"), la Fédération internationale de l'industrie phonographique ("IFPI") et la Fédération des éditeurs européens, ont organisé le troisième

atelier. Selon eux, les systèmes de gestion numérique des droits devraient être considérés comme des techniques d'habilitation : ils facilitent la diffusion du contenu (au lieu de le verrouiller), rendent possibles de nouveaux modèles de distribution et élargissent de ce fait le choix des consommateurs et la gamme des utilisations qu'ils peuvent faire des œuvres protégées. En ce qui concerne plus précisément les systèmes de gestion numérique des droits, les titulaires de droits ont fait observer que le marché de la gestion numérique des droits était encore jeune et doté d'une logistique insuffisante, et qu'il était impératif de s'assurer que les techniques de gestion numérique des droits soient sécurisées et renouvelables (c'est-à-dire, qu'elles puissent être de nouveau sécurisées en cas de piratage ou d'autres actes de contournement).

En outre, étant donné que les techniques de gestion numérique des droits ne sont pas encore mûres, les titulaires de droits ont estimé qu'il était prématuré de supprimer les taxes eu égard aux moyens de contrôle techniques. Les titulaires de droits ont également exprimé des préoccupations quant aux possibilités limitées d'interfonctionnement des techniques actuelles de gestion numérique des droits et ont encouragé le gouvernement et l'industrie à appuyer les travaux entrepris au sein des instances internationales pour la mise au point de normes ouvertes. Ils se sont clairement prononcés en faveur de normes imposées par l'industrie. Cela étant, ils ont également souligné que le gouvernement pouvait avoir un rôle à jouer s'agissant d'assurer l'application d'une nouvelle norme, voire en cas d'échec des négociations du secteur privé.

Les titulaires de droits ont également recensé les domaines d'action futurs. Parmi les plus urgents figure la nécessité d'assurer la sécurisation du contenu sur les ordinateurs individuels, ce qui constitue un véritable défi étant donné que ces appareils sont multifonctionnels et librement programmables. Les titulaires de droits ont recensé au nombre des projets actuels et futurs ce qu'ils décrivent comme les lacunes des systèmes de gestion numérique des droits, dont la "faille analogique" constituée par la conversion du format numérique sous forme analogique sans conservation de la protection originale, et la nécessité de protéger les émissions de télévision hertzienne numérique contre leur retransmission non autorisée (ce qui est l'objet du décret de la FCC sur le broadcast flag décrit à la section 3.2.1.3.b)).

Sociétés de gestion collective : les sociétés de gestion collective représentent les titulaires de droits dans la négociation et l'administration des contrats de licence, y compris la perception et la distribution des redevances, par l'intermédiaire de sociétés d'auteurs implantées dans le monde entier. Comme elles le décrivent elles-mêmes dans leur contribution au processus sur la société de l'information, elles se chargent de fixer les droits et de les céder sous licence, d'appliquer les lois de propriété intellectuelle, de surveiller et de vérifier les comptes et d'instruire et d'informer le public sur la nécessité de respecter le droit d'auteur. Au cours de l'atelier, les sociétés de gestion collective ont exprimé des préoccupations quant à la connaissance insuffisante de leur rôle dans la société de l'information en général – alors qu'elles donnent les moyens d'accéder aux œuvres protégées dans le monde entier et d'utiliser ces œuvres sous licence – et plus particulièrement en ce qui concerne l'élaboration et l'utilisation de systèmes de gestion numérique des droits pour les aider dans l'exercice de leurs fonctions. Plus précisément, les sociétés de gestion collective craignent de voir leur rôle diminuer dans la mesure où la gestion numérique des droits peut faciliter les relations directes, tant pour la gestion des droits que pour la rémunération des titulaires, entre les titulaires de droits et les consommateurs. À cet égard, les sociétés de gestion collective sont résolues à continuer de jouer un rôle qui viendrait compléter les fonctions des systèmes de gestion numérique des droits sans s'y substituer. Elles ont indiqué

qu'elles élaboraient elles-mêmes des éléments de gestion numérique des droits, tout en soulignant l'importance de la coopération dans ce domaine.

En outre, comme les titulaires de droits, les sociétés de gestion collective ont fait observer que les systèmes de gestion numérique des droits étaient encore peu développés et qu'ils ne pouvaient pas s'appliquer dans de nombreuses situations, notamment en ce qui concerne des dispositifs anciens, la reconversion numérique-analogique et la copie privée. D'une manière générale, les sociétés de gestion collective ne pensent pas que le temps soit venu de supprimer les taxes pour la copie privée.

En outre, les sociétés de gestion collective ont demandé instamment que des travaux supplémentaires soient entrepris en ce qui concerne l'interfonctionnement – nécessitant l'élaboration et l'application de normes internationales – ainsi que la sécurité et l'application des droits (y compris l'adaptation à de nouveaux modes de distribution). Elles ont considéré que les normes volontaires élaborées sous l'impulsion de l'industrie semblaient suffire et n'ont pas préconisé de rôle plus actif pour les pouvoirs publics.

Résumé des résultats : bien qu'aucun rapport synthétique officiel n'ait été établi à l'issue de la série d'ateliers sur la gestion numérique des droits, les grandes idées suivantes semblent avoir émergé des discussions :

– Des efforts supplémentaires doivent être entrepris afin de mieux comprendre la portée et les possibilités des solutions de gestion des droits dans l'environnement numérique.

– Les techniques de gestion numérique des droits – y compris sous l'angle de l'interfonctionnement entre les différents systèmes – devraient être élaborées sur la base d'efforts volontaires menés sous l'impulsion de l'industrie, le rôle du gouvernement n'étant pas encore arrêté.

– Une protection particulière et discrète du contenu mérite davantage d'attention de la part de tous les groupes concernés du secteur privé.

– Si les systèmes de gestion numérique des droits autorisent de nouveaux modèles de distribution et de nouveaux choix du consommateur, il convient de tenir compte des attentes des consommateurs et des exceptions au droit d'auteur.

– Un complément d'étude s'impose sur la mise en œuvre des systèmes de gestion numérique des droits sous l'angle du maintien des taxes sur les dispositifs et les supports numériques.

3.3.3 Jurisprudence

Étant donné que la directive sur le droit d'auteur a été adoptée relativement récemment et qu'elle n'a pas encore été transposée dans le droit interne de la plupart des États membres, il n'est pas surprenant que la jurisprudence d'application des dispositions anticontournement soit encore peu développée. Il existe toutefois des décisions interprétant les législations nationales existantes pour interdire certains types de dispositifs de contournement.

Sony Computer Entertainment c. Owen[171] : au Royaume-Uni, par exemple, Sony Computer Entertainment a intenté une action en justice contre plusieurs défendeurs qui

[171] [2002] EWHC 45 (CH).

importaient des puces de modification ("modification chips") pouvant être utilisées pour contourner les techniques de protection contre la copie et les codes régionaux sur les disques PlayStation 2. Les arguments invoqués étaient pour l'essentiel identiques à ceux en cause dans la décision précédemment rendue dans l'affaire *GameMasters* aux États-Unis d'Amérique.

Le tribunal anglais s'est appuyé sur un droit d'action fondé sur le droit d'auteur consacré à l'article 296 de la loi 1988 sur le droit d'auteur, les dessins et modèles et les brevets. L'article 296 s'applique lorsque des exemplaires d'une œuvre sont publiés sous une forme électronique "protégée contre la copie" et donne au distributeur des exemplaires – comme s'il était le titulaire du droit d'auteur dans une action pour atteinte aux droits – des droits contre quiconque vend un dispositif qui est "spécifiquement conçu ou adapté pour contourner" la protection contre la copie, sachant que ce dispositif sera utilisé pour faire réaliser des copies illicites[172]. Le terme "protégé contre la copie" est défini comme englobant "tout moyen destiné à empêcher ou à limiter la copie de l'œuvre". Le tribunal s'est prononcé en faveur de Sony parce que la copie qu'il s'agissait d'empêcher était le chargement non autorisé du jeu dans l'ordinateur et parce que les codes figurant sur les disques entraient dans le cadre de la définition de la protection contre la copie. Les défendeurs ont violé l'article 296 parce que leurs puces de modification étaient spécifiquement conçues pour contourner la technique de protection contre la copie de Sony.

3.4 Australie

3.4.1 Cadre juridique

3.4.1.1 Loi de 2000 portant modification de la loi sur le droit d'auteur (Digital Agenda)

3.4.1.1.a) Historique

L'Australie a mis en œuvre les traités de l'OMPI par la loi de 2000 portant modification de la loi de 1968 sur le droit d'auteur (Digital Agenda), qui est entrée en vigueur le 4 mars 2001 (ci-après dénommée DAA)[173]. L'examen des moyens de cette mise en œuvre en Australie a débuté avec un document de discussion de 1997 intitulé *Copyright reform and the Digital Agenda* et a continué en 1999 avec la publication d'un appel à commentaires sur les modifications à apporter à la loi sur le droit d'auteur à l'ère du numérique. En définitive, la conception australienne de la mise en œuvre des traités de l'OMPI a été jugée plus favorable aux utilisateurs que ses contreparties aux États-Unis d'Amérique et dans l'Union européenne. Cela traduirait le fait que l'Australie importe plus de produits protégés par le droit d'auteur qu'elle n'en exporte.

---

172 Loi de 1988 sur le droit d'auteur, les dessins et modèles et les brevets (titre 48), article 296.2).

173 Les dispositions pertinentes sont incorporées dans une nouvelle division A de la partie V de la loi de 1968 (Cth) sur le droit d'auteur.

3.4.1.1.b) Dispositions anticontournement

Le DAA interdit le trafic d'instruments de contournement, y compris la fabrication, la vente, la location, l'offre à la vente, la promotion, la publicité, la commercialisation, la distribution et l'exposition de tels dispositifs. Figure également parmi les activités interdites le fait de rendre le dispositif de contournement accessible en ligne, mais uniquement "dans la mesure où cela porte préjudice au titulaire du droit d'auteur"[174]. Lorsque l'acte en cause est l'offre d'un "service de contournement", le DAA, comme ses contreparties aux États-Unis d'Amérique et en Europe, interdit cette activité[175]. L'une des conditions de l'interdiction est que le défendeur doit savoir, ou avoir des raisons de penser, que le dispositif pourrait être utilisé pour contourner une mesure technique de protection ou faciliter son contournement[176]. Cela étant, le DAA n'interdit pas expressément l'acte de contournement.

La définition des "mesures techniques de protection" anticipe la démarche suivie dans l'Union européenne en matière d'intégration des mesures de contrôle d'accès et de contrôle de la copie. Son libellé suit toutefois largement celui du DMCA. Plus précisément, le DAA définit une mesure technique de protection comme un dispositif ou un produit (y compris les composants) qui est conçu "dans son fonctionnement ordinaire, pour empêcher ou entraver une atteinte au droit d'auteur sur une œuvre ou tout autre objet par l'un ou l'autre des moyens suivants, ou les deux" :

– en s'assurant que "l'accès à une œuvre" est possible "uniquement au moyen d'un code d'accès ou d'un procédé (y compris le décryptage, le désembrouillage ou toute autre transformation de l'œuvre...) avec l'autorisation du titulaire du droit d'auteur ou de son preneur de licence;

– par un mécanisme de contrôle de la copie[177].

En limitant la protection des mesures techniques de protection à celles qui sont "conçues pour empêcher ou entraver les atteintes aux droits", le DAA suit les traités de l'OMPI et les principes retenus aux États-Unis d'Amérique et dans l'Union européenne : l'objectif de l'utilisation de telles mesures est de renforcer la capacité des titulaires de droits d'empêcher les utilisations non autorisées de leurs œuvres.

Tout comme la directive sur le droit d'auteur, cependant, l'utilisation de l'expression "mécanisme de contrôle de la copie" suggère que le DAA n'interdit pas le contournement des mesures techniques qui sont utilisées par les titulaires de droits pour empêcher d'autres types d'utilisations non autorisées qui tombent sous le coup de leurs droits exclusifs (telles que les interprétations ou exécutions publiques). L'histoire législative du DAA fait des techniques de contrôle de la copie en série un exemple de mesure de "contrôle de la copie". Dans l'affaire *Sony* c. *Stevens* décrite ci-dessous, le tribunal fédéral a considéré que cette disposition se rapportait à un mécanisme qui limite la copie d'une œuvre.

Le DAA définit les dispositifs et les services de contournement par rapport à deux critères : si le dispositif ou le service n'a 1) qu'un "but ou usage commercialement limité

---

174 Loi de 1968 sur droit d'auteur (Cth), article 116A.1)b)i) à vi).
175 Article 116A.1)b)vii).
176 Article 116.A)1)c).
177 Article 10.1) (définition de la "mesure technique de protection").

en dehors du contournement" ou 2) aucun but ou usage autre que le contournement[178]. Le premier de ces deux critères est semblable à celui retenu dans le DMCA et dans la directive sur le droit d'auteur. Le second – celui de l'objectif unique - a été rejeté dans d'autres ressorts juridiques (mais pas dans la loi japonaise sur la prévention de la concurrence déloyale), parce qu'il autoriserait le trafic de dispositifs ou de services ayant peut-être un but légitime mineur ou marginal, mais ayant été conçus pour le contournement. La prise en considération du premier critère semble toutefois répondre aux préoccupations des titulaires de droits et d'autres personnes qui considéraient qu'il serait trop facile de contourner le critère de l'objet unique. L'une des distinctions importantes entre le DAA et les principes retenus aux États-Unis d'Amérique et dans l'Union européenne réside donc dans le fait que, selon la législation australienne, un dispositif ou un service qui a un but commercialement significatif autre que le contournement serait légal.

La conception australienne peut donc être récapitulée comme suit :

	Acte de contournement	**Instruments de contournement**
Mesure technique de contrôle d'accès	Non interdit	Interdits (article 10.1); article 116A)
Mesure technique de gestion du droit d'auteur	Non interdit	Interdits (article 10.1); article 116A)

3.4.1.1.c) Limitations et exceptions

Le DAA établit trois exceptions de base à l'interdiction du trafic de dispositifs ou de services de contournement.

Utilisation à des fins autorisées : lorsqu'un dispositif ou un service de contournement est fourni à une "personne qualifiée" à des "fins autorisées", celui-ci n'est pas interdit, si la personne qualifiée remet au fournisseur une déclaration signée. Les "fins autorisées" sont définies par référence aux exceptions aux atteintes au droit d'auteur prévues dans la loi sur le droit d'auteur. Les "fins autorisées" doivent entrer au moins dans l'une des exceptions statutaires aux atteintes au droit d'auteur, qui sont les suivantes[179] :

– reproduction de programmes d'ordinateur aux fins d'interfonctionnement, de correction des erreurs ou d'essais de sécurité;

– copie licite par des bibliothèques, des services d'archives, des établissements d'enseignement et autres, y compris les institutions d'aide aux handicapés mentaux; et

– utilisation licite de matériel protégé par le droit d'auteur par les services du Commonwealth ou d'un État.

Il importe de noter que les "fins autorisées" ne couvrent pas les "utilisations loyales" telles que la copie à des fins privées. Compte tenu de l'ampleur que pourrait prendre une telle

178 Article 10.1) (définitions des "dispositif de contournement" et des "services de contournement").

179 Article 116.A)7).

exemption et de l'incapacité de contrôler les dispositifs de contournement qui pourraient être licitement fournis aux personnes qui se cantonnent à un "usage loyal", il aurait été difficile de limiter la portée et l'effet d'une telle exemption aux seules personnes "qualifiées" et remettant des déclarations à cet effet.

Le terme "personne qualifiée" désigne une personne autorisée à utiliser le matériel aux fins d'une des exceptions mentionnées ci-dessus[180]. Enfin, la personne qualifiée doit remettre une déclaration signée confirmant que le dispositif ou le service sera utilisé seulement aux fins autorisées et que le matériel protégé n'est pas aisément disponible autrement que sous une forme protégée par une mesure technique[181]. Pour empêcher les pirates et d'autres personnes mal intentionnées d'utiliser cette procédure pour avoir accès aux dispositifs de contournement des mesures techniques, le DAA prévoit que les déclarations fausses ou fallacieuses faites en connaissance de cause constituent des infractions pénales[182].

La force de la solution australienne dépend donc dans une large mesure de l'intégrité du processus de déclaration. Il a été relevé, par exemple, que si une déclaration n'était pas fausse ou fallacieuse lorsqu'elle était faite, mais que le dispositif ou le service était utilisé plus tard à des fins non autorisées, aucune infraction ne pouvait être retenue. Dans ce cas, la responsabilité du fournisseur ne serait pas engagée parce qu'il aurait fourni le dispositif ou le service de contournement au vu d'une déclaration valide. Les utilisateurs de ces dispositifs ne pourraient non plus être poursuivis étant donné que les actes de contournement ne sont pas interdits par le DAA.

Fabrication ou importation à des fins autorisées : une disposition semblable s'applique à la fabrication ou à l'importation d'un dispositif de contournement. Pour que l'exception soit applicable, il doit être établi que le dispositif est fabriqué ou importé à une fin autorisée – comme indiqué ci-dessus – et que le matériel protégé par le droit d'auteur n'est pas aisément disponible sous une autre forme non protégée par une mesure technique[183].

En outre, un dispositif peut être fabriqué ou importé s'il permet à une personne de fournir un dispositif ou un service de contournement, mais seulement à des "fins autorisées"[184].

Application de la loi ou sécurité nationale : tout acte accompli licitement aux fins de l'application de la loi ou de la sécurité nationale est couvert par une exception générale[185].

3.4.1.1.d) Information électronique sur le régime des droits

Le DAA met également en œuvre les dispositions des traités de l'OMPI relatives à l'information sur le régime des droits. Il interdit la suppression ou l'altération non autorisée et en connaissance de cause de l'information électronique sur le régime des droits en vue

---

180 Article 116A.8).
181 Article 116A.3)b).
182 Articles 203G.1) et 2).
183 Article 116A.4)a).
184 Article 116A.4)b).
185 Article 116A.2).

d'induire, de permettre, de faciliter ou de dissimuler une atteinte aux droits[186]. Il interdit également la distribution, l'importation ou la communication au public d'une copie d'une œuvre protégée lorsque l'information électronique sur le régime des droits a été supprimée et que la personne sait ou a des raisons de penser qu'elle contribue ce faisant à une atteinte aux droits[187]. Pour ces deux infractions, les dispositions législatives présument que les défendeurs ont agi en connaissance de cause : il appartient à ces derniers de prouver qu'ils n'ont pas modifié ni supprimé l'information en connaissance de cause et qu'ils ne savaient pas que leur trafic de copies modifiées faciliterait les atteintes aux droits.

3.4.1.1.e) Voies de droit

Les sanctions prévues en cas d'infraction aux dispositions comprennent une procédure en référé donnant lieu à des dommages-intérêts ou une saisie sur les bénéfices[188]. Des dommages-intérêts punitifs sont également prévus pour les infractions flagrantes[189]. Les titulaires de droits peuvent également intenter une action pour la conversion ou la détention des dispositifs de contournement qui sont utilisés pour réaliser les copies illicites[190]. Les peines prévues pour les infractions pénales comprennent des amendes et des peines d'emprisonnement (jusqu'à cinq ans)[191].

3.4.1.2 Autres lois

D'autres dispositions de la législation australienne interdisent l'accès non autorisé aux ordinateurs et au contenu crypté. En particulier, les services de radiodiffusion cryptée sont protégés par la partie VAA insérée dans la loi de 1968 sur le droit d'auteur par l'effet du DAA. Le DAA s'inspire en partie de la directive sur l'accès conditionnel, mais sa portée est plus restreinte, puisqu'il s'applique seulement aux "émissions cryptées" définies dans la loi.

La partie VAA interdit la fabrication, divers types de trafic (y compris la mise à disposition en ligne) et l'utilisation commerciale des "dispositifs de décryptage d'émissions"[192]. Ces dispositifs sont définis comme des dispositifs "(y compris les programmes d'ordinateur) conçus ou adaptés pour permettre à une personne d'accéder à une émission cryptée sans l'autorisation du radiodiffuseur par le contournement, ou la facilitation du contournement, des moyens ou arrangements techniques qui protègent l'accès sous une forme intelligible à l'émission"[193]. Les "émissions codées" comprennent 1) les émissions de télévision ou de radio rendues accessibles uniquement aux personnes autorisées et sur paiement de redevances et 2) les émissions de télévision diffusées par des services de radiodiffusion, dont l'accès sous une forme intelligible est protégé par des mesures techniques[194]. Selon la législation et la jurisprudence, les services vidéo et audio sur

---

186 Article 116B.
187 Article 116C.
188 Article 116D)1).
189 Article 116D)2).
190 Article 116.
191 Article 132.6)A).
192 Article 135AN.1)b).
193 Article 135AL (définition d'un "dispositif de décryptage").
194 Article 135AL (définitions du terme "émission cryptée" a) et b)).

demande, le télétexte et la diffusion en continu sur l'Internet ne relèvent pas de la définition des services de radiodiffusion, et ne sont donc pas protégés contre l'accès non autorisé par la partie VAA[195].

Les radiodiffuseurs peuvent engager des poursuites pour l'usage commercial non autorisé de dispositifs de décryptage lorsqu'ils diffusent des émissions cryptées et que les personnes utilisent ces dispositifs pour accéder sans autorisation à ces émissions, en sachant (ou en ayant des raisons de penser) que l'accès n'est pas autorisé[196]. Les radiodiffuseurs peuvent obtenir une ordonnance en référé et soit des dommages-intérêts, soit une saisie sur les bénéfices[197]. La distribution commerciale d'un dispositif de décryptage d'émissions peut également constituer une infraction pénale[198].

Deux éléments du régime juridique australien méritent d'être mentionnés. Tout d'abord, la loi sur le droit d'auteur confère le droit d'agir au civil au radiodiffuseur, non au titulaire du droit d'auteur. Ensuite, la détention privée ou l'utilisation non commerciale non autorisée de dispositifs de décryptage d'émissions n'est pas interdite.

3.4.2 Jurisprudence

Autodesk, Inc. c. Dyson[199] : avant l'adoption du DAA, la Haute Cour australienne appliquait les principes existants de la loi australienne sur le droit d'auteur pour interdire tout dispositif utilisé pour contourner une mesure technique employée pour protéger un programme d'ordinateur. Dans cette affaire, Autodesk possédait un programme de conception assistée par ordinateur protégé par le droit d'auteur; les utilisateurs ne pouvaient y accéder de manière autorisée que par l'intermédiaire d'une protection matérielle (un "dongle"), qui était vendue avec le programme et devait être branchée sur l'ordinateur pour permettre au programme de fonctionner. Une partie distincte et importante du programme invitait le dongle à s'authentifier; ce module comparait les réponses à l'aide d'une "table de correspondance". Il fallait que la réponse reçue soit correcte pour que le programme puisse fonctionner.

Le défendeur a fabriqué un dispositif de contournement par ingénierie inverse du dongle. La Haute Cour a considéré que la production de ce dispositif de contournement portait atteinte au droit d'auteur sur le programme d'Autodesk parce que, au cours de la reproduction de la "table de correspondance" dans le dongle, une partie substantielle du programme était nécessairement copiée. En conséquence, la responsabilité du défendeur pour la fabrication du dispositif de contournement a été reconnue dans l'atteinte au droit d'auteur d'Autodesk.

---

195 Loi de 1992 sur les services de radiodiffusion (Cth) article 6 (définition des "services de radiodiffusion"); détermination à l'alinéa c) de la définition du "service de radiodiffusion" (n° 1 de 2000), dans *Gaz GN38* du 27 septembre 2000 (la diffusion en continu sur l'Internet de programmes de télévision ou de radio n'entre pas dans le cadre de la définition du "service de radiodiffusion").

196 *Id.*, article 135ANA.1).

197 *Id,* article 135ANA.4).

198 *Id,* article 135AS.1).

199 173 CLR 330 (1992).

Kabushiki Kaisha Sony Computer Entertainment c. Stevens[200] : en interprétant et en appliquant l'article 116A du DAA, en juillet 2003, la Cour d'appel fédérale a autorisé le recours intenté par Sony Computer Entertainment contre la décision du tribunal de première instance, qui s'était prononcé en faveur d'un défendeur qui avait vendu et installé des puces pour contourner le codage des jeux pour la console PlayStation 2 (ainsi que des copies contrefaites de ces jeux). Les mesures de protection mises en place par Sony comprenaient une mémoire de démarrage située sur la carte mère de ses consoles, qui était conçue pour vérifier les codes d'accès stockés sur la piste d'amorçage des disques et les codes régionaux destinés à faire en sorte que seuls les disques codés pour l'Australie puissent être lus sur les consoles vendues dans ce pays. La Commission australienne pour la concurrence et la défense des consommateurs, qui avait participé en tant qu'*amicus curiae* aux procédures de première instance, était intervenue en faveur du défendeur au motif que le codage régional était préjudiciable au bien-être des consommateurs et qu'il limitait leur choix.

Le juge de première instance avait soigneusement passé en revue l'examen par l'Australie des traités de l'OMPI et les divers projets du DAA, ainsi que la directive sur le droit d'auteur, pour interpréter l'expression "mesure technique de protection" au sens du DAA. Il était parvenu à la conclusion que les mesures de Sony n'étaient pas des "mesures techniques de protection" selon l'article 116.A) : bien qu'elles dissuadent ou découragent l'accès à l'œuvre, elles ne le faisaient pas au moyen d'un code d'accès ou d'un procédé décrit à l'article 10.1) de la loi de 1968 sur le droit d'auteur. En appel, le juge Lindgren a analysé de manière approfondie tant le texte que l'histoire législative du DAA.

En autorisant le recours, la Cour fédérale a adopté une interprétation plus large de la définition des "mesures techniques de protection". Elle a considéré que cette définition s'appliquait aux dispositifs ayant pour objectif de dissuader ou de décourager les atteintes aux droits et pas seulement, comme le juge de première instance l'avait affirmé, aux mesures empêchant ou entravant matériellement les actes susceptibles de porter atteinte aux droits. À cet égard, la Cour a estimé que l'article 116 s'appliquait non seulement à la reproduction non autorisée, mais également à la vente des articles dont la fabrication portait atteinte au droit d'auteur. Étant donné que les mesures de protection de Sony rendent les copies des jeux inutiles, la Cour a considéré qu'elles empêchaient l'infraction au sens où elles rendaient la vente des copies irréaliste ou impossible. Le juge de première instance n'avait pas estimé nécessaire de statuer sur la question de savoir si les puces étaient elles-mêmes des dispositifs de contournement. Il a néanmoins considéré que, compte tenu la l'utilité commercialement significative limitée des puces de modification en dehors du contournement, si les codes d'accès avaient pu être considérés comme des "mesures techniques de protection", les puces auraient été des dispositifs de contournement illicites.

La décision sur le recours est en grande partie conforme à la décision rendue dans l'affaire *Owen* décrite à la section 3.3.3, selon laquelle une puce semblable contournait de manière illicite les techniques de protection contre la copie de la PlayStation 2 de Sony en vertu de la loi du Royaume-Uni sur le droit d'auteur, les dessins et modèles et les brevets.

3.5 Japon

[200] [2003] FCA FC 157.

Au Japon, les dispositions anticontournement des traités de l'OMPI ont été mises en œuvres dans le cadre d'amendements apportés en 1999 à la loi sur le droit d'auteur et à la loi sur la concurrence déloyale. Les amendements apportés à la loi sur le droit d'auteur traitent du contournement des techniques de protection contre les atteintes au droit d'auteur. Les amendements apportés à la loi sur la concurrence déloyale interdisent à la fois le contournement des mesures techniques de contrôle de la copie et de contrôle d'accès. Au Japon, l'examen des possibilités juridiques de protection des mesures techniques précède la conférence diplomatique de l'OMPI, avec la publication, par le Groupe de travail de la sous-commission multimédias du Conseil du droit d'auteur, de deux rapport intérimaires, parus l'un en février 1995 et l'autre en février 1997. Ce groupe de travail avait lancé un processus de consultations et étudié l'évolution aux États-Unis d'Amérique et dans l'Union européenne. En décembre 1998, il a publié son rapport sur les mesures techniques et la gestion des droits[201].

3.5.1 Cadre juridique

3.5.1.1 Dispositions anticontournement

3.5.1.1.a) Loi sur le droit d'auteur

La loi n° 77 de 1999 a modifié la loi sur le droit d'auteur pour interdire diverses formes de trafic d'instruments de contournement, ainsi que l'offre au public de services de contournement. Elle n'interdit pas expressément l'acte de contournement.

La loi sur le droit d'auteur définit les "mesures techniques de protection" comme des "mesures visant à empêcher ou à dissuader des actes qui constituent des atteintes au droit moral, au droit d'auteur … ou aux droits voisins"[202]. Comme en Australie, les "mesures" sont définies par rapport à leur but.

La loi sur le droit d'auteur ne définit pas le terme "empêcher", mais un commentaire accompagnant les modifications de 1999 de la loi sur le droit d'auteur indique que le terme "empêcher" signifie stopper[203]. Le terme "dissuader" est défini dans la loi sur le droit d'auteur comme le fait de causer une "entrave considérable aux résultats de tels actes". Comme en Australie, le fait d'"empêcher" ou de "dissuader" suppose des moyens matériels ou techniques (plutôt que la simple dissuasion ou l'effet concret de la dissuasion). Il est précisé dans le commentaire qu'une mesure doit mettre en œuvre des moyens électromagnétiques pour donner effet à l'empêchement ou à la dissuasion[204].

Les dispositifs et les programmes de contournement sont interdits par les dispositions pénales de la loi sur le droit d'auteur. Un dispositif ou programme de contournement est défini comme tout dispositif ou programme qui a pour "fonction principale" le contournement

---

201 Les rapports intérimaires de 1995 et 1997 et le rapport final de décembre 1998 sont cités dans Koshida, note 204.

202 Article 2.xx) de la loi du Japon sur le droit d'auteur.

203 T. Koshida, *On the Law to Partially Amend the Copyright Law (Part 1): Technological advances and new steps in copyright protection* (1999), disponible à l'adresse *http://www.cric.or.jp/cric_e/cuj/cuj.html*. ["Koshida"].

204 *Id.*

de la protection technique[205]. La loi sur le droit d'auteur ne définit pas le terme "fonction principale". Le commentaire indique toutefois que seuls les dispositifs qui ont une "fonction pratique significative limitée autre que le contournement" sont interdits[206]. En cela, la loi japonaise est conforme aux autres solutions visant à interdire les dispositifs de contournement.

Bien que l'acte de contournement ne soit pas interdit, la loi sur le droit d'auteur prévoit qu'une personne ne peut contourner une mesure technique de protection afin de reproduire une œuvre à des fins privées et non commerciales[207]. D'ordinaire, la loi sur le droit d'auteur autorise de telles reproductions. Toutefois, lorsque la reproduction est faite par une personne qui sait que cet acte est rendu possible par le contournement ou parce que la mesure n'empêche plus la copie, l'exemption au titre de la copie privée n'est plus applicable. Cependant, une telle personne n'est pas soumise aux dispositions pénales de la loi sur le droit d'auteur.

Cette disposition définit le "contournement" comme le fait de permettre à une personne d'effectuer "des actes empêchés par les mesures techniques de protection" (c'est-à-dire, l'empêchement) ou de stopper les "obstacles" aux résultats des actes "dissuadés par de telles mesures" (dissuasion)[208]. Elle couvre également la suppression de l'information sur le régime des droits. La suppression ou l'altération de mesures ou d'informations qui sont essentielles à la conversion ou à la compression n'est pas considérée comme un acte de contournement.

3.5.1.1.b) Loi sur la concurrence déloyale

La loi sur la concurrence déloyale, comme la loi sur le droit d'auteur, interdit seulement le trafic des dispositifs et non l'acte de contournement lui-même. Elle protège les "moyens techniques de restriction". Ceux-ci sont définis comme comprenant "les moyens de limiter la lecture d'images et de matériel audio, l'exécution de programmes ou leur enregistrement par méthode électromagnétique, c'est-à-dire une méthode d'enregistrement et de transmission des signaux auxquels les dispositifs de lecture réagissent de manière spécifique … ou une méthode d'enregistrement et de transmission sur supports d'enregistrement par conversion des images, du matériel audio ou des programmes…"[209].

La définition s'applique à la fois aux mesures de contrôle d'accès et de contrôle de la copie, dans la mesure où elles limitent l'"enregistrement". Comme dans le cas de la directive sur le droit d'auteur, la mention de "l'enregistrement" suggère que les moyens techniques qui limitent l'exercice non autorisé des droits d'auteur autres que le droit de reproduction ne sont sans doute pas couverts par la loi sur la concurrence déloyale. Comme indiqué

---

205 Article 120bis de la loi du Japon sur le droit d'auteur.

206 Koshida, note 203

207 Article 30.1) de la loi du Japon sur le droit d'auteur.

208 Article 30.1)ii).

209 Article 2.5) de la loi sur la concurrence déloyale. Voir Office des brevets du Japon, Centre Asie-Pacifique pour la propriété industrielle et Institut japonais de l'innovation et de l'invention, *Outline and Practices of Japanese Unfair Competition Law* 22 (1999) (traduction commentée de la loi), disponible à l'adresse *http://www.apic.jiii.or.jp/facility/text/2-10.pdf* ["JPO/APIC Outline"].

précédemment, la loi sur le droit d'auteur envisage toutefois la protection des mesures techniques susceptibles d'être utilisées pour protéger d'autres droits d'auteur.

Aux termes de l'article 2.1)x) de la loi sur la concurrence déloyale, constituent des actes de concurrence déloyale "la transmission, la fourniture ou l'exposition de matériel dont la seule fonction consiste à empêcher l'effet des moyens techniques de restriction et à permettre de regarder des images et d'écouter du matériel audio … ou d'enregistrer des images [etc.] … limités par des moyens techniques de restriction utilisés à des fins commerciales", ainsi que les dispositifs intégrant de tels dispositifs[210]. La distribution de tels programmes en ligne est aussi interdite. Dans son commentaire, l'Office des brevets du Japon indique que cet article s'applique aux actes de contournement des techniques de "restriction de la copie", alors que l'article 2.1)xi) s'applique aux actes visant les techniques de contrôle d'accès[211]. Le système de gestion de la copie en série est mentionné comme exemple de techniques de restriction de la copie alors que le CSS est décrit comme une technique de contrôle d'accès[212]. Les puces utilisées pour la lecture non autorisée de jeux vidéo sont considérées comme des dispositifs de contournement[213].

Comme indiqué précédemment, l'article 2.1)xi) s'applique pour protéger les techniques de contrôle d'accès contre les dispositifs de contournement. En résumé, il interdit le trafic (y compris la distribution en ligne) de dispositifs (y compris les produits incorporés dans d'autres dispositifs) qui neutralisent les moyens techniques utilisés commercialement pour empêcher les personnes (autres que les personnes indiquées) de regarder des images et d'écouter des œuvres audio, si et dans la mesure où ces produits ont pour seule fonction de permettre à des personnes de lire des œuvres vidéo ou audio, d'exécuter des programmes ou d'enregistrer des images, des œuvres sonores ou des programmes dont l'utilisation est restreinte[214].

Le texte de ces dispositions, comme le commentaire, souligne que seuls les dispositifs ayant pour fonction exclusive le contournement des moyens techniques sont interdits. Il s'agit de la seule loi, parmi celles examinées dans le présent document, qui limite l'interdiction aux produits ayant le contournement pour "unique objet".

La loi japonaise met en application les traités de l'OMPI de la manière suivante :

	Acte de contournement	**Instruments de contournement**
Mesure technique de contrôle d'accès	Non interdit	Interdits (article 2.1)xi) de la loi sur la concurrence déloyale)
Mesure technique de	Non interdit	Interdits (article 120bis de la loi sur le

210 Article 2.1)x) de la loi sur la concurrence déloyale.

211 JPO/APIC Outline, note 209, par. 21.

212 *Id,* par. 45.

213 *Id.* Voir également Ministère du commerce international et de l'industrie, *Amendment to the Unfair Competition Law (Draft)* (mars 1999) (décrivant les puces qui permettent la lecture de logiciels copiés comme exemple de dispositifs de contournement des mesures de contrôle de l'utilisation), disponible à l'adresse *http://www.meti.go.jp/english/report/data/gCD110e.html*.

214 Article 2.1)xi) de la loi sur la concurrence déloyale. Voir JPO/APIC Outlook, note 209, par. 23 et 24.

contrôle du droit d'auteur		droit d'auteur; art. 2.1)x) de la loi sur la concurrence déloyale)

3.5.1.1.c) Limitations et exceptions

La loi sur le droit d'auteur ne contient pas de clause d'exemption. Le commentaire indique toutefois que l'utilisation d'une "machine non réactive, qui ne réagit pas au signal utilisé pour les mesures techniques" n'est pas considérée comme un contournement[215].

La loi sur la concurrence déloyale prévoit une exception à l'interdiction générale, afin d'autoriser la distribution de dispositifs utilisés pour les essais ou la recherche sur les mesures techniques de protection[216]. L'objectif de l'exemption est de favoriser le perfectionnement des mesures.

3.5.1.2 Voies de droit

Seules des sanctions pénales sont prévues par la loi sur le droit d'auteur pour le trafic de techniques de contournement : une amende n'excédant pas un million de yens ou une peine d'emprisonnement n'excédant pas un an. Le commentaire indique que les recours civils ne sont pas prévus parce que, lors de l'introduction d'un dispositif de contournement, il ne serait pas évident de déterminer les œuvres auxquelles il pourrait s'appliquer ni, par conséquent, les titulaires de droits d'auteur qui seraient fondés à obtenir une ordonnance pour atteinte directe à leurs œuvres[217].

En vertu de la loi sur la concurrence déloyale, le trafic de dispositifs et de programmes de contournement est considéré comme un acte de "concurrence déloyale". Des mesures conservatoires sont prévues.

---

215 Koshida, note 203

216 Article 11.1)7) de la loi sur la concurrence déloyale.

217 Koshida, note 203

3.5.1.3 Information sur le régime des droits

La loi japonaise sur le droit d'auteur suit d'une manière générale les traités de l'OMPI et les autres lois de mise en œuvre en ce qui concerne la définition de "l'information sur le régime des droits". Elle définit de manière relativement précise l'information sur le régime des droits comme l'information concernant le droit moral ou le droit d'auteur qui est enregistrée dans une mémoire informatique ou transmise sous forme électromagnétique avec les œuvres, et qui est utilisée commercialement en rapport avec l'autorisation d'utilisation des œuvres aux fins de la gestion du droit d'auteur. L'information sur le régime des droits comprend les informations identifiant les œuvres et les titulaires et d'autres informations qui seront précisées par décret ministériel, qui se rapportent aux modalités d'exploitation et qui permettent celle-ci "par comparaison avec d'autres informations"[218]. La définition semble plus restrictive que celle utilisée ailleurs, dans la mesure où, par exemple, elle ne s'applique pas aux mentions de réserve du droit d'auteur ni aux autres mentions incorporées dans les œuvres.

La loi sur le droit d'auteur n'établit pas en tant que droit distinct du droit d'auteur l'insertion, la suppression ou la modification de l'information sur le régime des droits. Ces actes sont considérés comme des atteintes au droit moral, au droit d'auteur et aux droits voisins des auteurs et des artistes interprètes ou exécutants. Plus précisément, la loi sur le droit d'auteur interdit l'adjonction intentionnelle d'informations fausses, la suppression ou l'altération intentionnelle d'informations (sauf en cas d'impossibilité de procéder autrement) et la distribution de copies des travaux en sachant qu'il y a eu adjonction, suppression ou altération illicite de l'information sur le régime des droits[219]. À la différence d'autres pays, cependant, il n'y a aucune condition supplémentaire selon laquelle la personne, pour voir sa responsabilité engagée, doit avoir fourni, supprimé ou modifié sciemment l'information sur le régime des droits pour contribuer à l'infraction. En outre, lorsque la suppression s'inscrit dans un processus technique de conversion ou de compression, il n'y a pas atteinte aux droits. Les sanctions pénales en cas de violation de ces dispositions sont les mêmes que celles prévues pour les infractions aux dispositions anticontournement.

3.5.2 Autres lois

D'autres lois au Japon assurent une protection juridique aux systèmes de gestion numérique des droits ou à d'autres techniques d'accès conditionnel. Par exemple, la loi sur la radiodiffusion interdit à toute personne de recevoir un service de radiodiffusion à péage sans avoir conclu un accord avec le radiodiffuseur[220].

4. PARTIES PRENANTES AUX SYSTÈMES DE GESTION NUMÉRIQUES DES DROITS ET RÉALISATIONS EN LA MATIÈRE

4.1 Introduction

218 Article 2.xxi) de la loi sur le droit d'auteur.
219 Article 113.3) de la loi sur le droit d'auteur.
220 Article 52-5 de la loi sur la radiodiffusion.

Les fonctions nécessaires pour la gestion numérique des droits ont été expliquées en détail ci-dessus. Les utilisateurs des techniques – les parties prenantes – participent à la chaîne de valeur des droits de propriété intellectuelle, qui associe tous ceux qui ont un intérêt, moral ou financier, dans la création, la distribution et la consommation de contenu protégé. Ce sont ces parties prenantes qui tireront parti des fonctions de gestion numérique des droits pour créer des conditions favorables à la distribution et à la consommation de la propriété intellectuelle dans l'environnement numérique. De nombreux points de vue ont été exprimés, certains convergents, d'autres résolument opposés.

La présente section recense les diverses parties prenantes et leur position dans la chaîne de valeurs, et décrit leurs conceptions de l'élaboration, de la mise en place et de l'utilisation de systèmes de gestion numérique des droits pour la distribution, la protection et l'exploitation de contenu protégé.

4.1.1 Titulaires de droits

Selon la Convention de Berne, un droit d'auteur prend naissance lors de la création d'une œuvre. Les titulaires du droit d'auteur peuvent être des créateurs (personnes physiques), des sociétés (personnes morales) ou des cotitulaires. En outre, un droit peut être cédé sous licence par le créateur à un tiers qui, aux fins de la présente cette section, sera considéré comme le titulaire des droits.

Les titulaires de droits s'attendent légitimement à pouvoir autoriser, généralement contre paiement, l'exploitation des actifs de propriété intellectuelle qu'ils possèdent. Dans le domaine analogique (secteur de l'édition, etc.), ils sont habitués à utiliser un certain nombre de méthodes leur permettant d'obtenir une rémunération pour l'usage des œuvres. Cette rémunération peut prendre la forme d'un paiement direct par les utilisateurs, de paiements dans le cadre de conventions collectives qui sont administrées par les sociétés de gestion collective ou d'un paiement effectué par des intermédiaires qui revendent l'œuvre aux consommateurs.

L'avènement de la gestion numérique des droits peut offrir aux titulaires de nouvelles possibilités de gérer leurs droits. Par exemple, un créateur peut conclure un contrat avec un prestataire de services de gestion numérique des droits (tel que Overdrive ou DWS) et proposer directement ses œuvres au public. Les sociétés d'enregistrement et les maisons d'édition pourraient également conclure de tels arrangements, raccourcissant ainsi la chaîne de distribution en supprimant les grossistes et détaillants intermédiaires traditionnels. Les incidences de telles évolutions sur la chaîne de valeurs commencent seulement à se manifester et appellent un complément d'étude et de négociation entre les participants.

4.1.2 Sociétés de gestion collective

Les sociétés de gestion collective, qui gèrent et administrent les droits de groupes d'auteurs, jouent traditionnellement un rôle central dans la cession sous licence et la distribution de contenu protégé par le droit d'auteur, ainsi que dans la collecte de redevances pour l'utilisation de ce contenu. Compte tenu de leur vaste expérience en matière de gestion de droits, elles s'intéressent naturellement aux possibilités offertes par les techniques numériques dans ce domaine. La gestion des droits est devenue de plus en plus complexe, en raison à la fois de la nature mondiale de l'exploitation et de la cession sous licence des œuvres

et de la myriade de supports et de formats sous lesquels des droits peuvent être cédés. Il n'est donc pas étonnant que les sociétés de gestion collective considèrent que les systèmes de gestion numérique des droits ont un rôle important à jouer dans l'exercice de leurs fonctions. Certaines d'entre elles utilisent déjà des techniques numériques pour gérer de manière rapide et efficace certains droits.

Cela étant, certaines parties prenantes peuvent estimer que le rôle des sociétés de gestion collective devrait être plus limité dans un monde numérique, notamment dans la mesure où les titulaires de droits peuvent concéder des licences directement aux utilisateurs. Elles peuvent également penser que la nature collective des activités des sociétés de gestion collective empêche effectivement les titulaires d'exercer leurs droits de manière individuelle. Les sociétés de gestion collective rejettent ces arguments, faisant valoir que les titulaires peuvent toujours, en théorie du moins, choisir entre la gestion collective et la gestion individuelle de leurs droits. Et les sociétés de gestion collective considèrent que, compte tenu de leur rôle fondamental dans la diffusion numérique du contenu, leurs besoins et fonctions doivent être pleinement compris et assimilés dans la conception et la mise en œuvre de tout système de gestion numérique des droits.

Craignant peut-être que les systèmes de gestion numérique des droits ne viennent à les remplacer, les sociétés de gestion collective ont également argué du fait que ces systèmes ne pourraient effectuer toutes les tâches qu'elles exécutent, en particulier les plus concrètes. Ainsi, même dans un monde modelé par la gestion numérique des droits, les sociétés de gestion collective se voient continuer à effectuer la vérification des comptes de paiement des redevances, ainsi qu'à exécuter toutes les activités d'une organisation mutuelle, telles que la négociation collective avec d'autres titulaires et utilisateurs de droits, et à participer pleinement à l'élaboration de normes et aux débats de politique publique sur le droit d'auteur et son application.

Les sociétés de gestion collective ont souligné qu'elles participaient elles-mêmes activement à l'élaboration de certains éléments des systèmes de gestion numérique des droits, notamment en contribuant à l'établissement de normes pour les identificateurs (par exemple, le code ISWC) et en prenant part aux instances internationales visant à promouvoir l'utilisation de normes communes (par exemple, le format MPEG 21).

4.1.3 Intermédiaires

S'agissant de supports matériels, lorsque l'on parle d'intermédiaires, on a tendance à penser aux grossistes et aux détaillants, qui forment la filière de distribution entre les "sociétés de contenu" et leurs clients. Or, l'examen des rôles à remplir dans la chaîne de valeur numérique mène rapidement à la conclusion selon laquelle toute organisation placée entre le créateur et le consommateur doit être considérée comme un "intermédiaire". Cela vaut tant pour les organismes commerciaux tels que les compagnies d'enregistrement et les éditeurs que pour les organismes "d'intérêt public" tels que les bibliothèques, qui jouent traditionnellement un rôle très important dans la centralisation et la diffusion de l'information.

La répartition traditionnelle des rôles dans la chaîne de distribution matérielle semble avoir une application à long terme limitée dans l'environnement de réseau. Les tâches qui doivent être accomplies dans cette chaîne peuvent être arbitrairement désagrégées – voir réagrégées - de manière complètement différente.

Toutefois, la mesure dans laquelle la chaîne peut être remodelée dépend très largement de l'efficacité des communications. Le réseau lui-même fournit l'infrastructure *matérielle* nécessaire à ces communications et (par "l'effet de réseau") entraîne simultanément la mise en œuvre de l'infrastructure *normative* qui permet une communication efficace d'ordinateur à ordinateur.

Pour que le remodelage de la chaîne de valeur soit réellement efficace, il est essentiel que cette infrastructure normative soit aussi ouverte et peu arbitraire que possible. Il importe, par exemple, de n'avoir aucun a priori sur la répartition des fonctions dans la chaîne de valeur. Cela pourrait entraîner des difficultés considérables pour les organismes concernés, dans la mesure où ceux-ci sont naturellement enclins à conserver les modèles et les pratiques de gestion existants (même s'ils sont inadaptés à l'environnement de réseau).

Les intermédiaires peuvent donc avoir des intérêts divergents (et probablement contraires également aux intérêts des consommateurs). Ils peuvent avoir beaucoup de mal à faire la part entre leur intérêt à court terme et leur intérêt à long terme. Néanmoins, il est dans l'intérêt à long terme de tous que les systèmes et l'infrastructure de gestion numérique des droits soient conçus de manière à ménager la plus grande souplesse en termes d'appui aux modèles de gestion et aux chaînes de distribution numériques, au lieu de prévoir simplement des mécanismes qui imitent les modèles physiques existants.

4.1.4 Intermédiaires de télécommunications

Les opérateurs de réseau n'ont pas été traditionnellement impliqués dans la chaîne de valeur de la propriété intellectuelle. En tant que "transporteurs", ils mettaient à disposition les câbles sur lesquels l'information – qu'il s'agisse d'appels téléphoniques ou de données – était transmise d'un endroit à l'autre. Cependant, avec l'avènement de l'économie numérique, les opérateurs de réseau se sont empressés d'entrer dans la chaîne de valeur en tant que fournisseurs d'accès à l'Internet afin de proposer à leurs clients des services de contenu rémunérateurs.

Les fournisseurs d'accès sont de plus en plus préoccupés par le risque de voir leur responsabilité engagée pour toute atteinte aux droits liés au contenu qu'ils diffusent. Les opérateurs de télécommunications traditionnels n'ont jamais été inquiétés pour la transmission de contenu portant atteinte à des droits. En revanche, en tant que fournisseurs d'accès à l'Internet ("FAI"), ces opérateurs et les nouveaux arrivants peuvent voir leur responsabilité directement ou indirectement engagée en cas de transmission ou de stockage temporaire ou permanent de contenu illicite. Les États-Unis d'Amérique, en vertu du DMCA, et l'Union européenne, dans la directive sur le commerce électronique, ont considéré que la responsabilité du FAI ne pouvait être retenue lorsqu'il se livrait de bonne foi à ces activités. Pour cette raison, les régimes juridiques aux États-Unis d'Amérique et dans l'Union européenne limitent la responsabilité potentielle du FAI lorsque celui-ci, après notification, supprime ou rend inaccessible le contenu illicite (voir les sections 3.2.1.2 et 3.3.1.2.c) ci-dessus).

Les FAI sont extrêmement intéressés par la mise en œuvre d'instruments de gestion numérique susceptibles de les prémunir contre les risques juridiques. D'autre part, ils ne souhaitent pas compromettre leurs relations avec la clientèle en établissant des obstacles apparents (si la gestion numérique des droits est perçue comme un obstacle) à l'utilisation du contenu qu'ils distribuent.

4.1.5 Vendeurs de logiciels

La contribution de l'industrie du logiciel à la gestion numérique des droits a connu différentes phases. Pour comprendre comment les fournisseurs de logiciels de gestion numérique des droits se rattachent au reste de la chaîne de valeur, il faut connaître l'histoire récente du marché du logiciel. À l'origine, le secteur était presque exclusivement occupé par de petites entreprises de haute technologie, implantées pour la plupart aux États-Unis d'Amérique. Si certaines d'entre elles ont commencé leurs travaux de recherche-développement à la fin des années 80, la majorité a éclos pendant la première moitié des années 90. Plus l'intérêt pour les techniques de gestion numérique des droits se développait, plus ces sociétés ont prospéré. Sans parvenir à s'assurer une large clientèle, nombre d'entre elles ont mis à profit cette période pour déposer des brevets. Ces portefeuilles de brevets croissants ont alimenté des sommes importantes de capital-risque et le secteur s'est montré particulièrement florissant jusqu'à la fin des années 90. Cette situation a poussé plusieurs de ces sociétés à proposer des services en plus des logiciels. À l'époque, elles espéraient tirer des bénéfices des droits sur les transactions dérivant de l'utilisation de leurs logiciels et services. Si cette perspective n'était guère attrayante pour les titulaires de droits, elle semblait alors à la portée de ces entreprises.

Cependant, au tout début du nouveau millénaire, la situation du marché a radicalement changé. Avec l'effondrement de la confiance dans le secteur entier du logiciel, les sociétés les plus petites sont devenues insolvables, certaines d'entre elles manquant totalement des clients. Celles qui sont restées ont continué à lutter avant de s'effondrer ou se sont consolidées au moyen de fusions ou ont été rachetées, avec leurs portefeuilles de brevets, par de plus grandes compagnies.

Cela a donné un secteur du logiciel de gestion numérique qui est en grande partie dominé par quelques acteurs mondiaux, tels que Microsoft, IBM et Adobe. Il semble que ce soient ces sociétés qui fixent les priorités pour les logiciels de gestion numérique des droits, les entreprises de plus petite taille se contentant d'ajouter des fonctions supplémentaires aux technologies commerciales de base. Toutefois, et cette réserve est importante, les titulaires de droits sont devenus récemment très actifs s'agissant de faire valoir leurs conditions pour la gestion des droits dans l'environnement numérique moyennant leur participation aux initiatives en faveur de l'établissement de normes. C'est là, au cœur des débats sur le point de savoir dans quelle mesure l'environnement en ligne et hors ligne de gestion des droits dans l'environnement numérique sera normalisé, ce qui aura un effet considérable sur l'interfonctionnement, que se jouent l'avenir des société de logiciels et les recettes qu'elles pourront tirer de la gestion numérique des droits. Il faut dire également que l'issue du débat sur les normes déterminera dans une large mesure les rapports entre les titulaires de droits et les entreprises de technologie. Ces questions seront examinées dans les sections 2.5.2 (normes) et 4.2.7 (interfonctionnement).

4.1.6 Vendeurs de matériel

Les fabricants de matériel, notamment les entreprises d'informatique et d'électronique grand public, figurent parmi les principaux promoteurs des techniques de protection du contenu. Au début des années 80 (et avant), l'industrie de la technologie était quelque peu réticente devant les limitations juridiques frappant les dispositifs de copie tels que magnétoscopes et magnétophones.

Avec l'arrivée des techniques numériques, des arrangements ont été trouvés avec les titulaires de droits. Le rapprochement était principalement motivé par la prise de conscience du fait que les nouveaux formats numériques, du point de vue tant du contenu que de la technologie, exigeaient la coopération et l'appui de tous les secteurs industriels concernés. Sans l'appui des titulaires de droits, les nouveaux produits d'enregistrement et de traitement numériques pourraient être mort-nés. Pour obtenir un tel appui, il fallait que des techniques de protection du contenu soient mises au point et appliquées dans les produits numériques.

Vers la fin des années 80 et le début des années 90, les sociétés de technologie ont proposé des systèmes de protection du contenu assez simples. Comme indiqué ci-dessus, il s'agissait notamment du système de gestion de la copie en série ("SCMS") pour limiter la copie en série de contenu audionumérique. Le système CGMS-A ("Copy Generation Management System-Analog") a été proposé pour limiter la copie, par des dispositifs d'enregistrement numériques, de contenu audiovisuel analogique marqué. Depuis le milieu des années 90 jusqu'à l'heure actuelle, les principales sociétés de technologie s'attachent à mettre au point rapidement des systèmes commerciaux de protection du contenu plus sophistiqués, comme ceux décrits dans la section 3.2.1.

Pour protéger le contenu audiovisuel des DVD, par exemple, Matsushita Electric Industrial Co. et Toshiba ont mis au point le CSS, qui, comme indiqué précédemment, est à présent vendu sous licence par la DVD Copy Control Association, Inc ("DVD CCA"). Le système DTCP ("Digital Transmission Content Protection"), qui est utilisé pour protéger le contenu dans la sphère du domicile, a été mis au point par Hitachi, Intel, Matsushita, Sony et Toshiba. Intel est le principal promoteur du système HDCP ("High-bandwidth Digital Content Protection"), qui est utilisé pour protéger le contenu vidéo numérique des bus d'ordinateurs aux moniteurs et à d'autres dispositifs d'affichage. Matsushita, Toshiba, Intel et IBM ont mis au point diverses techniques de protection du contenu pour les DVD audio et les techniques d'enregistrement connexes, notamment les systèmes intitulés Content Protection for Prerecorded Media ("CPPM") et Content Protection for Recordable Media ("CPRM").

Les fabricants de matériel ont également été au premier rang des activités de conception et de promotion des techniques de tatouage. La DVD CCA examine actuellement la possibilité d'adopter une technique pour le marquage des DVD vidéo. Deux techniques sont à l'étude depuis un certain temps. L'une a été mise au point par le groupe "VWM", qui comprend de grandes sociétés de technologie telles que Hitachi, NEC, Philips, Pioneer et Sony, ainsi que deux acteurs plus petits, mais essentiels dans le domaine de la protection du contenu, à savoir Macrovision Corp. et Digimarc. Toshiba a mis au point l'autre technique de tatouage.

Le principal moteur de ces initiatives est la nécessité commerciale d'utiliser ces techniques pour tenir compte de la prolifération des produits numériques, notamment les appareils d'enregistrement et les lecteurs, les ordinateurs individuels et les processeurs qui s'y rapportent. Pour comprendre les différentes techniques décrites ci-dessus, qui sont censées se compléter les unes les autres dans une architecture liée au domicile, il faut savoir qu'elles sont appuyées par des systèmes complets de protection imposés dans le cadre de licences. Les modalités de ces licences font quant à elles l'objet d'un processus long et intense de collaboration, de consultation et de négociation avec les titulaires de droits. Étant donné qu'ils confient leur précieux contenu à la protection offerte par ces techniques, les titulaires de droits insistent pour qu'aucun changement essentiel ne soit apporté aux techniques ou aux conditions de licence connexes sans qu'ils aient un droit de regard ou d'approbation.

4.1.7 Utilisateurs professionnels et commerciaux

Les besoins des utilisateurs de contenu (principalement l'information) dans un contexte professionnel ou commercial ne sont pas fondamentalement différents de ceux d'un particulier. Toutefois, les priorités peuvent être légèrement différentes. Trois questions méritent une attention particulière.

Tout d'abord, la question de *l'autorité* et de *l'authenticité* est susceptible d'occuper une place plus centrale : ce document est-il bien ce qu'il prétend être? Provient-il d'une source digne de confiance? Ces questions peuvent être particulièrement pressantes lorsqu'une responsabilité ou une réputation professionnelle est en cause.

Deuxièmement, la question de la *confidentialité*, le "droit de lire de manière anonyme", peut revêtir une signification tout à fait différente. Pour prendre un exemple simple, un concurrent à même de détecter ce que lit un chercheur en pharmacie devrait pouvoir tirer des conclusions assez précises au sujet de l'orientation et des résultats possibles de ses recherches.

Troisièmement, il existe un besoin en faveur de l'accès au contenu moyennant l'identification de *l'appartenance à une catégorie*, par exemple, le fait d'être salarié d'une corporation ou membre d'une association. À l'heure actuelle, ces mécanismes sont relativement peu raffinés, étant fondés sur l'emplacement physique et l'authentification de l'adresse IP. On a rapidement pris conscience de la nécessité d'une gestion beaucoup plus sophistiquée de l'identité numérique; toutefois, les incidences sur la vie privée sont potentiellement importantes. Dans la mesure où une personne peut également appartenir à un groupe privilégié par la législation sur le droit d'auteur, l'identification du contexte dans lequel le matériel protégé est utilisé peut soulever des questions délicates quant à l'application des exceptions légales aux droits exclusifs des titulaires. Par exemple, en tant qu'enseignant et dans le cadre d'activités pédagogiques, une personne peut se servir de tel ou tel matériel protégé en vertu des "exceptions en faveur de l'enseignement" ou des exceptions au titre de l'usage loyal prévues dans certains ressorts juridiques; or, ces exceptions peuvent ne pas être applicables au même matériel lorsque la personne l'utilise dans sa capacité privée.

Lorsqu'on examine l'application des systèmes de gestion numérique des droits, il est essentiel de tenir compte de ces difficultés, même si la solution semble actuellement impossible à trouver.

4.1.8 Consommateurs

Les consommateurs ont des attentes au sujet de la façon dont ils peuvent accéder au contenu et utiliser celui-ci. Ces attentes sont fondées sur des pratiques de longue date, en ce qui concerne tant le contenu qu'ils acquièrent légalement que celui qu'ils peuvent de plus en plus obtenir sans autorisation, notamment au moyen du partage de fichiers point à point.

D'une part, les consommateurs se sentent autorisés à copier le contenu qu'ils acquièrent licitement, qu'il s'agisse d'émissions radiodiffusées par voie hertzienne ou de CD qu'ils achètent. Ils se sont également habitués à pouvoir copier les émissions de télévision sur des appareils d'enregistrement, même si le contenu est diffusé sur la base d'un accès conditionnel

(télévision à péage) ou d'un service à paiement sélectif. Aux États-Unis d'Amérique du moins, des mesures ont été prises en vue de tenir compte de ces attentes et de ces pratiques dans les "règles de codage" qui font partie des systèmes de protection du contenu décrits ci-dessus dans les sections 3.2.1 et 4.1.6 et dans le Digital Millennium Copyright Act[221].

D'autre part, les consommateurs peuvent franchement reconnaître que certains comportements – le piratage commercial et la distribution à grande échelle de contenu protégé par le droit d'auteur même dans un contexte non commercial – sont inopportuns. Beaucoup de consommateurs aiment ne rien payer pour contenu – d'où le succès du partage de fichiers -, mais la plupart seraient disposés à verser quelque chose dans les circonstances et pour le produit appropriés.

Il n'est donc pas étonnant que les techniques utilisées pour limiter les comportements habituels des consommateurs ne soient pas bien accueillies par ceux-ci ou les organisations qui les représentent. Dans de nombreux pays, des groupes bien organisés représentent les intérêts des consommateurs ou du public en matière de techniques numériques, y compris les systèmes de gestion numérique des droits. Aux États-Unis d'Amérique, par exemple, la Home Recording Rights Coalition est impliquée dans les questions liées aux consommateurs et l'enregistrement privé depuis 1981. Plus récemment, l'Electronic Frontier Foundation et Public Knowledge, entre autres, ont participé aux débats publics sur les négociations sectorielles concernant les normes de protection du contenu et les questions relatives à la gestion numérique des droits et sont intervenus au cours des discussions devant le Congrès et la Commission fédérale des communications concernant le rôle du gouvernement dans l'imposition d'accords négociés par l'industrie. En Europe, l'Organisation des consommateurs européens représente les intérêts des utilisateurs sur les questions de gestion numérique des droits et en ce qui concerne les initiatives de la Communauté européenne sur le droit d'auteur.

Outre l'examen des incidences potentielles de la mise en œuvre des systèmes de gestion numérique des droits sur les pratiques des consommateurs, des préoccupations ont également été exprimées concernant l'impact de ces techniques sur la vie privée, dans la mesure notamment où les systèmes de gestion numérique des droits pourraient permettre aux titulaires et aux distributeurs de recueillir et d'utiliser des données personnelles sur les habitudes d'achat des consommateurs et l'utilisation qu'ils font du matériel protégé par le droit d'auteur. Ces questions liées au respect de la vie privée sont examinées dans la section 5.2.1.

4.2 Systèmes actuels de gestion numérique des droits

4.2.1 Introduction

Si le présent document expose le cadre juridique et technique pour l'utilisation et le fonctionnement des techniques de gestion numérique des droits, les utilisateurs qui se trouvent tout au long de la chaîne de valeur sont principalement intéressés par leur mise en œuvre. À cet égard, il importe de souligner que la mise en œuvre de ces techniques en est encore à ses balbutiements. Cela tient à de nombreuses de raisons, juridiques, techniques et commerciales. Premièrement, les divers instruments juridiques censés protéger la mise en

[221] Voir la note 56 concernant les règles de codage prévues à l'article 1201.k) du DMCA.

œuvre et le fonctionnement des mesures techniques de protection ne sont pas encore en place sur le plan universel. Deuxièmement, les modèles commerciaux qui permettront aux titulaires de concéder l'exploitation de leur contenu sont encore loin d'être définitivement élaborés. Et troisièmement, les techniques nécessaires pour créer ces modèles, et les normes sur lesquelles elles s'appuieront, sont toujours en cours de développement.

On peut toutefois faire quelques observations sur les systèmes actuellement en service.

a) La plupart des systèmes de gestion numérique des droits actuellement en fonction sont limités à des secteurs de contenu spécifiques (tels que les industries de l'édition ou de la musique). La gestion numérique des droits ne s'applique pas encore aux riches contenus multimédias associant musique, contenu audiovisuel et texte. Une telle séparation verticale entre les secteurs reflète la distribution du contenu analogique, où il est techniquement et matériellement difficile de combiner différents types de supports. Au fur et à mesure que la gestion numérique des droits s'assouplira, permettant de combiner à la volée différents types de contenu, la séparation verticale entre les flux de contenu deviendra de plus en plus poreuse, avant de s'estomper.

b) Les modèles de gestion étayant la distribution du contenu sont encore assez peu élaborés. Les systèmes d'abonnement, les services à la carte et l'achat pur et simple dominent toujours le marché. On prévoit pour l'avenir une prolifération des modèles de gestion, dont bon nombre seront fondés sur l'achat de produits hybrides; les modèles de distribution point à point dans lesquels les titulaires de droits sont rémunérés restent rares. La majorité de ces systèmes sont consacrés à l'échange de contenu non autorisé.

c) Les systèmes de paiement sont toujours primitifs, la plupart des paiements s'effectuant par carte de crédit.

4.2.2 Services de gestion numérique des droits sur les œuvres sonores

Un certain nombre de services de musique en ligne sont apparus ces deux dernières années, sous l'impulsion de grandes sociétés d'enregistrement et de sociétés de diffusion de contenu en ligne telles que RealNetworks, dans le cadre de son service Rhapsody. Ces services légitimes de téléchargement de musique ont été mis en place afin de proposer une solution de remplacement aux services point à point illégitimes. Il est encore trop tôt pour évaluer le succès des services légitimes de musique en ligne.

MusicNet a été fondé par BMG, Warner Music et EMI. L'entreprise a passé des accords avec Sony et Universal. Par conséquent, le service de musique en ligne propose dorénavant du contenu des cinq plus grandes maisons de disques. Les utilisateurs ont accès au contenu de MusicNet par l'intermédiaire de partenaires de distribution tels que Rand AOL. Le système permet aux utilisateurs de télécharger et d'écouter en continu du contenu musical protégé par des techniques de gestion numérique des droits. Selon le type d'abonnement choisi, les utilisateurs peuvent sauvegarder la musique sur leur disque dur et la graver sur CD. Il en coûte environ 10 dollars É.-U. par mois pour écouter une quantité illimitée de morceaux du catalogue en ligne de MusicNet.

iTunes a été lancé aux États-Unis d'Amérique au printemps de 2003 par Apple. Le service utilise le dispositif iPod d'Apple comme lecteur, qui sauvegarde les pistes musicales protégées par des techniques de gestion numérique des droits qui sont téléchargées sur le

service iTunes par l'intermédiaire d'un ordinateur. Ce service s'est révélé extrêmement populaire et Apple a annoncé en juin 2003 qu'il avait vendu plus de cinq millions de morceaux par l'intermédiaire de son site musical iTunes.

Pressplay a été lancé par Vivendi Universal et Sony. Ce service est semblable dans son principe au modèle de distribution de MusicNet. Tous les morceaux distribués sur le réseau sont protégés par des techniques de gestion numérique des droits . Pressplay a été acheté récemment par la société de gravure de CD Roxio, qui avait également racheté Napster vers la fin de 2002.

Plus récemment, une nouvelle entreprise de musique en ligne, appelée Echo, a été fondée par plusieurs grands détaillants de musique aux États-Unis d'Amérique, dont Best Buy, Tower Records, Virgin Entertainment Group, Wherehouse Music, Hastings Entertainment et Trans World Entertainment.

OD2 est un service européen de téléchargement de musique cofondé par le compositeur et interprète Peter Gabriel. OD2 fournit des services de distribution à de grandes maisons de disques, telles que Sony et BMG.

4.2.3 Services de gestion numérique des droits sur les œuvres audiovisuelles

De grands studios de cinéma ont commencé récemment à assurer des services de films à la demande sur l'Internet public. La mise en œuvre des techniques de gestion numérique des droits constitue une partie essentielle de leurs stratégies. Les initiatives les plus réussies ont été jusqu'ici dans l'industrie pornographique. Du côté du marché des consommateurs, le nouveau portail de films sur demande MovieLink a été lancé en 2002. MovieLink est une coentreprise associant MGM, la Paramount, Sony Pictures Entertainment, Universal Studios et Warner Bros. Studios. Ce service, qui est accessible uniquement aux personnes domiciliées aux États-Unis d'Amérique, a été lancé comme projet pilote en novembre 2002. Il propose une collection de 200 films des principaux studios cinématographiques.

Ce service permet aux utilisateurs d'acheter le contenu au moyen de leur carte de crédit et de télécharger les films sur leur disque dur. Chaque titre incorpore des techniques commerciales de gestion numérique des droits, comme celles contenues dans le lecteur Windows Media Player de Microsoft. Une fois téléchargé, le film reste sur le disque dur de l'utilisateur pendant 30 jours. Si le fichier n'a pas été lu au cours de cette période, il expire. Une fois que le fichier a été lu, un compte à rebours automatique de 24 heures est activé. Après la période de 24 heures, le fichier devient inutilisable.

4.2.4 Services de gestion numérique des droits sur les œuvres textuelles

Des initiatives en matière de gestion numérique des droits ont aussi été lancées dans l'industrie du texte. Microsoft a mis au point un système de gestion numérique des droits pour les publications électroniques adaptées, appelé Digital Asset Server. Son principal concurrent, Adobe, commercialise quant à lui Adobe Content Server. La division logiciels de Palm, Palm Digital Media, a également élaboré un système personnalisé de gestion numérique des droits pour distribuer ses livres électroniques. La plupart des grandes librairies électroniques en ligne ont adopté les dernières techniques. Les intégrateurs de systèmes de gestion numérique des droits tels Overdrive utilisent les techniques de plusieurs fournisseurs pour établir des systèmes personnalisés pour l'industrie de l'édition en ligne.

4.2.5 Services de gestion numérique des droits sur les logiciels

Les consoles de jeux et les systèmes de jeux en ligne sont de plus en plus protégés au moyen de systèmes de gestion numérique des droits. La console de jeux Xbox de Microsoft, par exemple, comprend un système de cryptage matériel 128 bits, qui empêche des utilisateurs de lire les jeux piratés et d'utiliser la console à d'autres buts. Sony a également incorporé des techniques de gestion numérique des droits dans sa PlayStation 2 et Nintendo dans sa GameCube.

Cela étant, il existe des "mod chips", qui sont des circuits qui peuvent être ajoutés sur la carte mère d'une console, permettant aux utilisateurs de contourner la protection contre la copie des consoles. Bien que les problèmes posés par ces puces de modification ne soient pas encore aussi pressants que ceux posés par les utilisations non autorisées d'œuvres musicales, cinématographiques et textuelles, les sociétés de jeux vidéo et de logiciels sont de plus en plus préoccupées par leur diffusion. Pour cette raison, comme indiqué dans la section 3, Sony a poursuivi des distributeurs de mod chips avec succès aux États-Unis d'Amérique, au Royaume-Uni et (en appel) en Australie.

4.2.6 Extension de la gestion numérique des droits à d'autres secteurs de l'industrie

On prend peu à peu conscience du fait que les techniques de gestion numérique des droits peuvent s'appliquer dans d'autres secteurs que les industries du droit d'auteur. Bien que la gestion sécurisée de l'information commerciale ait toujours été une préoccupation dans le commerce et l'industrie, il est de plus en plus admis que les connaissances constituent le bien le plus important (et le plus précieux) d'une organisation. Dans ce contexte, la définition de la valeur des connaissances va au-delà des définitions traditionnelles de la propriété intellectuelle découlant des brevets, du droit d'auteur et des bases de données exclusives. De plus en plus, les membres du conseil d'administration et les cadres supérieurs d'une société sont poussés par les autorités réglementaires et leurs propres actionnaires à démontrer qu'ils s'attachent à préserver la sécurité d'informations qui, dans de nombreux cas, représentent la majorité du capital.

C'est pourquoi les techniques décrites dans le présent document commence à soulever un certain intérêt. En utilisant des techniques de gestion numérique des droits, les sociétés espèrent pouvoir gérer l'utilisation de l'information, là où avant elles pouvaient seulement en contrôler l'accès. Ce faisant, elles protégeront plus efficacement leurs actifs et pourront également contrôler où leur information est utilisée. Cela renforcera considérablement la sécurité de l'information.

4.2.7 Interfonctionnement

Le thème de l'interfonctionnement traverse toutes les discussions sur la gestion numérique des droits et a déjà été abordé dans la section sur les normes (section 2.5). Son importance pour l'avenir de la distribution de contenu sécurisé ne peut pas être sous-estimée. La meilleure manière de définir l'interfonctionnement est sans doute de dire qu'il s'agit de la possibilité de maintenir les règles d'utilisation du contenu des droits, de les interpréter sans ambiguïté et de les imposer dans de multiples systèmes *commerciaux* de gestion des droits dans l'environnement numérique et dispositifs d'utilisateurs. Ce terme désigne également la possibilité d'utiliser des séries de données d'origines différentes comme si elles répondaient à

une norme commune (ce qui est essentiel pour utiliser des métadonnées émanant de différentes communautés).

Actuellement, l'interfonctionnement n'est pas accessible aux titulaires de droits ni aux utilisateurs puisque la plupart des systèmes de gestion numérique des droits en service sont fondés sur des solutions isolées de tel ou tel fournisseur et non sur des normes largement adoptées. En outre, ils sont pour la plupart limités à un type de support simple. Cela tient peut-être à la segmentation traditionnelle des industries des médias autant qu'à la disponibilité de la technologie.

Bien que les normes soient essentielles pour la mise en œuvre de l'interfonctionnement, la demande des consommateurs jouera également un rôle moteur. En l'absence d'une mesure suffisante d'interfonctionnement permettant à différents systèmes de fonctionner de concert sans inconvénient pour l'utilisateur (qu'il s'agisse du titulaire des droits ou du consommateur), il est peu probable que la gestion numérique des droits soit une véritable réussite. Étant donné l'importance de l'interfonctionnement, il n'est pas étonnant que la question de savoir si les pouvoirs publics devaient intervenir pour le rendre obligatoire dans les systèmes de gestion numérique des droits ait été posée. Cette question est examinée dans la section 5.2.3.

5. QUESTIONS DE POLITIQUE GÉNÉRALE SOULEVÉES PAR LES TECHNIQUES DE GESTION NUMÉRIQUE DES DROITS

L'élaboration, la mise en œuvre, la protection et l'utilisation des techniques de gestion numérique des droits soulèvent de nombreuses questions de politique générale pour les gouvernements nationaux et les organisations internationales, dont la Commission européenne et l'OMPI. Nombre d'entre elles ont été évoquées et recensées dans la discussion précédente. La présente section regroupe et passe en revue certains de ces thèmes.

5.1 Questions de propriété intellectuelle

5.1.1 Mise en œuvre des traités de l'OMPI

Le WCT est entré en vigueur le 6 mars 2002, lorsque 30 États l'eurent ratifié ou y eurent adhéré. Le WPPT est entré en vigueur le 20 mai 2002. Quelque 42 États sont actuellement (au mois d'août 2003) parties au WCT, et autant au WPPT.

La mise en œuvre des traités de l'OMPI a été relativement rapide aux États-Unis d'Amérique, au Japon et en Australie[222]. Elle a été plus lente dans l'Union européenne, car la procédure d'adoption de la directive sur le droit d'auteur a pris un certain temps. En outre, au sein de l'Union européenne, deux États membres seulement ont observé la date limite pour la transposition en droit interne de la directive sur le droit d'auteur et, au début du mois d'août 2003, ils n'étaient que cinq à l'avoir fait. Plusieurs grands pays n'ont pas encore mis en œuvre les traités de l'OMPI.

En ce qui concerne les pays qui ont mis en œuvre les traités de l'OMPI, et l'Union européenne, les démarches varient légèrement. Cette variation a été envisagée par les parties

---

[222] Il faut noter que, bien que l'Australie ait mis en œuvre les traités de l'OMPI (voir la section 3.4), elle ne les a pas encore ratifiés.

contractantes et est autorisée par le texte des traités de l'OMPI eux-mêmes. Plusieurs types de variations ont été recensés.

Dans la plupart des pays, les dispositions anticontournement semblent être mises en œuvre dans les lois sur le droit d'auteur ou parallèlement à celles-ci. Dans quelques pays, elles sont incorporées dans les lois sur la concurrence déloyale. En outre, quelques pays sont devenus parties aux traités de l'OMPI sans apporter aucun changement fondamental à leur régime juridique national; ces pays considèrent que leur cadre juridique existant est suffisant pour remplir les obligations qui leur incombent en vertu des traités.

Chaque ressort juridique mettant en œuvre les traités a dû déterminer les types de mesures techniques à protéger, c'est-à-dire celles qui contrôlent l'accès aux œuvres comme celles qui limitent les droits exclusifs du titulaire. La plupart des ressorts juridiques semblent protéger les deux types de mesures techniques.

De plus, les dispositions qui donnent effet aux traités de l'OMPI restreignent généralement les actes en amont du contournement. Ces actes comprennent la fabrication et le trafic d'instruments de contournement. Certaines législations de mise en œuvre vont toutefois plus loin et interdisent divers types d'actes de contournement. Dans ces cas, elles peuvent exclure de la responsabilité certaines catégories d'actes de contournement. Ou, comme aux États-Unis d'Amérique, les actes de contournement peuvent ne pas être interdits en rapport avec les mesures techniques qui protègent le droit d'auteur, dans la mesure où un acte de contournement devrait être assimilé à une atteinte au droit d'auteur proprement dit.

Les différences sont évidentes en ce qui concerne les exceptions ou limitations applicables aux actes ou aux produits de contournement. En ce qui concerne les dispositions interdisant le trafic, les lois diffèrent sur la question de savoir si un dispositif doit être interdit ou autorisé, selon qu'il a pour "seul" ou pour "principal" but le contournement.

Jusqu'ici, il ne semble pas que la rapidité avec laquelle les traités de l'OMPI ont été mis en œuvre ni que les variations dans les textes d'application aient eu des effets mesurables sur l'élaboration ou l'utilisation des systèmes de gestion numérique des droits. Avec le temps, toutes les parties contractantes devraient respecter les obligations qui leur incombent en vertu des traités. Il restera alors à voir si les différences dans la mise en œuvre auront un effet significatif sur la mise en service des systèmes des gestion numérique des droits ou sur la protection du contenu assurée par ces systèmes.

5.1.2 Effet des techniques de gestion numérique des droits sur les exceptions et limitations au droit d'auteur

En employant les techniques de gestion numérique des droits, les titulaires devront garder à l'esprit les exceptions et limitations dans les dispositions anticontournement, ainsi que les exceptions au droit d'auteur (dans l'Union européenne du moins). L'ajustement entre les possibilités techniques et commerciales des systèmes de gestion numérique des droits, d'une part, et les objectifs juridiques et politiques traduits dans les exceptions et limitations, de l'autre, risque d'être difficile.

Si, par exemple, dans l'Union européenne, les titulaires de droits emploient les mesures techniques qui privent des bénéficiaires d'une exception, ils pourront – à un point dans l'avenir –devoir s'inquiéter des mesures que les États membres pourraient prendre pour

s'assurer que ces personnes bénéficieront réellement de cet avantage. En effet, ainsi qu'il est envisagé dans le projet de loi en Allemagne, si les titulaires de droits ne s'assurent pas que les bénéficiaires peuvent bénéficier des exceptions, ils peuvent s'exposer à des sanctions. Les systèmes de gestion numérique des droits peuvent être mis au point et utilisés avec des règles rigoureusement compatibles avec les exceptions, mais ces règles ne pourront prévoir toutes les situations dans lesquelles une exception est (ou doit être) disponible mais où la technique de gestion numérique des droits n'est pas à même de s'adapter ou de vérifier la légitimité du droit du bénéficiaire.

En fait, aux États-Unis d'Amérique, le rapport entre l'utilisation des systèmes de gestion numérique des droits et les exceptions au droit d'auteur a été longuement discuté dans la perspective de l'incorporation de la notion de contournement légitime – sur la base de l'usage loyal – dans le DMCA. La doctrine de "l'usage loyal" est si malléable et si dépendante des faits et des circonstances que le Congrès a finalement décidé qu'il ne pourrait y avoir aucune exception générale aux dispositions anticontournement au titre de l'usage loyal; toutefois, cette question se présente de nouveau en liaison avec un projet de loi actuellement en instance aux États-Unis d'Amérique. De même, à moins que les systèmes de gestion numérique des droits soient conçus de manière à être capables d'autoriser l'utilisation au cas par cas, c'est-à-dire de déterminer quand une utilisation demandée est "loyale", il sera difficile pour les solutions de gestion numérique des droits de tenir compte de cette exception au droit d'auteur.

La question de savoir si une mesure technique peut s'adapter à la copie privée licite ou à des utilisations loyales s'est posée à de multiples occasions aux États-Unis d'Amérique. Dans chaque cas, on a noté que la loi ou la technologie faisait une certaine place aux préoccupations relatives aux utilisations loyales, tout en reconnaissant que certaines utilisations légitimes ne seraient plus possibles sur le plan technique.

En ce qui concerne la loi sur l'enregistrement audio à domicile, par exemple, la mise en œuvre nécessaire du système de gestion de la copie en série (ou d'un système équivalent) signifie que deux générations de copies audionumériques au maximum seraient techniquement possibles (même s'agissant des propres copies légitimes d'un utilisateur d'œuvres protégées); aucune copie numérique d'une copie numérique ne serait possible. En ce qui concerne la première de ces deux limitations, toutefois, une telle copie en série aurait vraisemblablement aurait été consentie par le titulaire du droit d'auteur. Quant à la seconde, la copie audionumérique en série pourrait dans certains cas constituer un usage loyal (aux fins de la réalisation de compilations et de sélections d'enregistrements) et devrait de ce fait être licite.

En outre, aux États-Unis d'Amérique, comme indiqué dans les sections 3.2.1 et 4.1.8, certaines "règles de codage" ont fait l'objet de négociations pendant plusieurs années[223]. Ces règles prévoient la copie en série illimitée du contenu dans certaines circonstances, mais uniquement pour une seule génération. Là aussi, on peut envisager des exemples de copie privée autorisée ou d'usage loyal qui seraient entravés par l'application de ces règles. Et, là encore, certains ont considéré que le compromis atteint dans ces règles de codage permettait des quantités de reproductions privées et non commerciales suffisantes, de sorte que les restrictions imposées par les règles sont tolérables.

---

[223] Voir Marks/Turnbull, note 42.

Dans la même veine, les traités de l'OMPI imposent aux parties contractantes l'obligation de prévoir une protection appropriée des mesures techniques qui sont utilisées pour protéger le droit d'auteur et les droits connexes. La législation d'application a généralement a suivi cette indication. Quel est alors le statut juridique des systèmes de gestion numérique des droits susceptibles d'être utilisés pour diffuser du contenu du domaine public sous une forme protégée? Les actes de contournement et les produits conçus pour le contournement d'un tel système sont-ils licites parce que le contenu protégé n'est pas soumis au droit d'auteur?

Les consommateurs, les établissements d'enseignement et les universitaires ont exprimé des préoccupations quant au fait que les systèmes de gestion numérique des droits pourraient être utilisés pour verrouiller du contenu sur lequel le droit d'auteur aurait expiré. À ce stade, on pense toutefois que les dispositions anticontournement ne seront plus applicables. Les titulaires de droits et les fournisseurs de services de gestion numérique des droits n'ont pas adopté uniformément la position selon laquelle les protections juridiques de ces services sont inapplicables lorsqu'ils sont utilisés pour protéger des œuvres du domaine public. À leurs yeux, dès lors qu'un système de gestion numérique des droits est utilisé pour protéger des œuvres soumises au droit d'auteur, il doit rester illicite de mettre au point des instruments pouvant être utilisés pour contourner ce système, même s'il s'agit de contourner des mesures techniques appliquées à une œuvre du domaine public. Ils feraient valoir que l'activité illégale découle du trafic d'un dispositif qui contourne un système de gestion numérique des droits qui est utilisé pour protéger une œuvre soumise au droit d'auteur. Par conséquent, les efforts visant à limiter les dispositions anticontournement aux systèmes de gestion numérique des droits lorsqu'ils sont utilisés pour protéger des œuvres soumises au droit d'auteur risquent d'être vains, étant donné que les dispositifs de contournement de ces systèmes (même lorsqu'ils sont utilisés pour protéger des œuvres non soumises au droit d'auteur) pourraient être illicites.

La question de savoir si les systèmes de gestion numérique des droits et les protections juridiques qui s'y rapportent tiendront suffisamment compte des exceptions et limitations légitimes prévues notamment dans les lois nationales sur le droit d'auteur se précisera au fur et à mesure que ces systèmes seront mis en œuvre. Il semble peu probable que tout cas de copie à usage privé, de copie aux fins d'ingénierie inverse ou de copie dans le cadre d'un usage loyal soit autorisé par un système de gestion numérique des droits ou un contrat spécifique. Il ne fait guère de doute non plus que la législation d'application des traités de l'OMPI n'autorisera pas le contournement dans toutes ces situations. Des utilisations légitimes seront inévitablement entravées par les systèmes de gestion numérique des droits, les contrats passés avec les titulaires et les distributeurs de contenu et les lois qui s'y rapportent. Les utilisateurs et les gouvernements ont craint que les contrats ne viennent finalement réduire à néant les exceptions ou limitations juridiques ou judiciaires aux droits[224]. On pourrait mentionner ici les préoccupations des utilisateurs selon lesquelles la limitation la plus importante des droits de l'auteur – la nature limitée de la durée du droit d'auteur – pourrait elle-même être annulée par le contrat : les titulaires de droits pourront-ils exercer un contrôle sur les œuvres du domaine public, bien après l'expiration du droit d'auteur, en imposant des conditions pour l'accès à ces œuvres (lorsque l'accès est contrôlé par un système de gestion numérique des droits) à l'intention des utilisateurs qui se conforment aux restrictions d'utilisation?[225]

Les précédents peuvent suggérer que même une prise en considération inexacte dans les systèmes de gestion numérique des droits et les contrats de distribution de telles utilisations légitimes peut être acceptable. Les titulaires de droits peuvent proposer certains types de licences à certaines catégories particulières de bénéficiaires des exceptions réglementaires ou fournir le contenu dans différents formats selon les catégories de personnes. Les titulaires de droits seront aussi probablement sensibilisés aux mécanismes de surveillance et d'exécution mis en place en ce qui concerne les incidences de l'utilisation des systèmes de gestion numérique des droits. En outre, s'ils ne prévoyaient pas des exceptions en faveur de la copie privée dans le cadre des solutions de gestion numérique des droits, dans l'Union européenne du moins, la directive sur le droit d'auteur indique tout à fait clairement que les États membres ont toujours la possibilité d'intervenir directement (ou d'imposer des sanctions), pour s'assurer que les pratiques autorisées en vertu des exceptions au droit d'auteur ne sont pas entravées par les mesures techniques.

Les consommateurs, les enseignants, les bibliothécaires et d'autres utilisateurs de contenu protégé par le droit d'auteur peuvent tolérer une certaine imprécision dans la mesure dans laquelle les systèmes de gestion numérique des droits tiennent compte de leurs besoins. Leur bonne volonté à cet égard peut toutefois dépendre de la mesure dans laquelle les titulaires de droits n'abusent pas de l'utilisation des techniques de gestion numérique des droits et les avantages plus larges de la distribution de contenu dans cet environnement.

---

224 Voir, par exemple, Copyright Law Review Committee, *Copyright and Contract* (avril 2002) (rapport australien récapitulant les exposés sur la prévalence, les effets et les opportunités des contrats qui prétendent passer outre les exceptions au droit d'auteur), disponible à l'adresse *http://www.law.ecel.uwa.edu.au/ipcr339/CopyrightContractAct.pdf*.

225 Voir, par exemple, B. Hugenholtz, *Copyright, Contract and Code: What Will Remain of the Public Domain*, 26 Brook. J. Int'l L. 77, 78 (2000) (selon lequel "la combinaison des contrats et de la technologie fait peser une menace directe sur le système du droit d'auteur tel que nous le connaissons").

5.1.3 Systèmes de gestion numérique des droits et taxes pour la copie privée

Comme indiqué dans la section 3.3.2, au sujet de l'atelier de la Commission européenne sur la gestion numérique des droits, la relation entre les taxes pour la copie privée et la mise en œuvre des techniques de gestion numérique des droits a retenu une attention considérable en Europe (bien que les États-Unis d'Amérique appliquent des taxes sur les dispositifs et les supports d'enregistrement audionumériques en vertu de la loi sur l'enregistrement audio à domicile, la gamme des dispositifs et des supports frappés par ces taxes est relativement restreinte et la suppression de ces taxes n'a pas donné lieu à des débats importants ces derniers temps). La justification historique de ces taxes est qu'il convient d'indemniser les titulaires de droits pour la copie privée de leurs œuvres qui n'a pas été expressément autorisée et pour laquelle aucune autre rémunération n'est directement disponible. Les lois sur le droit d'auteur de la majorité des États membres de l'Union européenne prévoient des taxes sur les dispositifs ou les supports d'enregistrement.

En Europe, la directive sur le droit d'auteur indique expressément que, en ce qui concerne la copie privée à des fins non commerciales, les États membres prévoiront des exceptions au droit d'auteur "à condition que les titulaires de droits reçoivent une compensation équitable qui prend en compte l'application ou la non-application des mesures techniques"[226]. Il est donc reconnu que l'application des techniques de gestion numérique des droits aura une influence sur la "rémunération appropriée" des titulaires. Dans la mesure où des taxes pour la copie privée sont imposées sur les dispositifs et les supports, les consommateurs et l'industrie technologique ont souligné que le fait de permettre aux titulaires de droits d'obtenir une indemnité supplémentaire au moyen d'une technique de gestion numérique des droits pourrait se traduire par une double rémunération dont le montant dépasse ce qui est "équitable".

La directive sur le droit d'auteur traite directement du lien entre les systèmes nationaux de taxes et l'utilisation des systèmes de gestion numérique des droits uniquement dans son préambule. L'alinéa 38 indique que, en ce qui concerne l'utilisation privée, les États membres peuvent prévoir une exception accompagnée d'une "compensation équitable"; à cet égard, des "systèmes de rémunération" peuvent être introduits ou maintenus[227]. Cet alinéa prévoit le maintien de ces systèmes en ce qui concerne la reproduction privée sur support analogique, tout en reconnaissant que "la confection de copies privées sur support numérique est susceptible d'être plus répandue", qu'il y a des différences entre la copie privée numérique et analogique et qu'il convient "de faire une distinction entre elles à certains égards"[228].

L'alinéa 39 est essentiel dans l'examen du rapport entre les taxes et la gestion numérique des droits. Il est libellé de la manière suivante :

> *"Lorsqu'il s'agit d'appliquer l'exception ou la limitation pour copie privée, les États membres doivent tenir dûment compte de l'évolution technologique et économique, en particulier pour ce qui concerne la copie privée numérique et les systèmes de rémunération y afférents, lorsque des mesures techniques de protection efficaces sont disponibles. De telles exceptions ou limitations ne doivent faire obstacle ni à*

---

226 Article 5.2)b) de la directive sur le droit d'auteur.

227 Alinéa 38 du préambule de la directive sur le droit d'auteur.

228 *Id*.

l'utilisation de mesures techniques ni à la répression de tout acte de contournement."[229] *[italiques ajoutés]*

Cet alinéa reconnaît clairement le rapport entre, d'une part, la copie privée et les systèmes de taxes qui s'y rapportent et, d'autre part, les techniques de gestion numérique des droits. Lorsque des systèmes de gestion numérique des droits qui sont "efficaces" sont "disponibles", la directive sur le droit d'auteur suggère de modifier ou de supprimer les systèmes de taxes. Si les notions d'efficacité et de disponibilité peuvent être évidentes en théorie, ce qui est efficace ou disponible peut être extrêmement difficile à déterminer en pratique. Bien qu'il puisse être possible de déterminer à quel moment un système de gestion numérique des droits est "disponible", il est plus difficile d'établir les types de contenu à l'égard desquels ils doivent être suffisamment disponibles pour justifier une suppression des taxes pour la copie privée de ce contenu.

La notion d'efficacité soulève peut-être des questions encore plus complexes. Bien qu'un système de gestion numérique des droits puisse être "efficace" en termes de limitation de la copie non autorisée, que signifie être "efficace" aux fins de la modification ou de la suppression d'un système de taxes? Par exemple, si une mesure de gestion numérique des droits permet seulement la copie privée d'un certain contenu sur certaines classes de dispositifs et de supports d'enregistrement, la taxe doit-elle supprimée sur ces classes d'appareils et de supports? Mais qu'en est-il si ces mêmes dispositifs et supports peuvent également être utilisés pour réaliser des copies privées de contenu qui n'est pas protégé par un système de gestion numérique des droits et pour lequel le titulaire des droits n'obtient aucune autre rémunération? Les États membres devront-ils examiner chaque système de gestion numérique des droits en rapport avec chaque type de contenu et chaque classe de dispositifs ou de supports d'enregistrement numériques pour effectuer la transition? Étant donné qu'il apparaît que ces décisions seront prises au niveau national, ne risque-t-on pas d'aboutir à des solutions incompatibles dans le marché intérieur?

Là encore, il est improbable qu'il y ait une précision absolue entre la protection complète du contenu par les systèmes de gestion numérique des droits et la suppression des taxes sur les dispositifs et supports d'enregistrement utilisés pour la copie privée de ce contenu. Il peut donc être justifié d'adopter une solution "approximative" qui laisserait aux États membres le soin de conclure que l'utilisation réelle ou potentielle des systèmes de gestion numérique des droits permet d'assurer une rémunération appropriée aux titulaires de droits au titre de la copie privée. Après avoir étudié la situation, les États membres pourraient parvenir à la conclusion que les titulaires de droits sont, globalement parlant, suffisamment rémunérés pour de telles utilisations. Dans une telle situation, où des systèmes de gestion des droits efficaces sont effectivement "disponibles", les États membres pourraient envisager de supprimer tout système de taxes pour la rémunération des titulaires de droits.

5.2 Autres questions de politique générale

5.2.1 Confidentialité

L'utilisation des techniques de gestion numérique des droits soulève des questions qui vont au-delà de la protection de la propriété intellectuelle, concernant notamment le respect de

---

229 Alinéa 39.

la vie privée. Comme indiqué dans la section 2.4.9, l'utilisation de ces techniques peut être envisagée sous deux aspects différents, l'un renforçant la confidentialité et l'autre faisant planer des menaces sur la vie privée.

Les techniques de gestion numérique des droits se fondent généralement sur des communications et une authentification sécurisées entre deux dispositifs ou plus. Souvent, elles vérifient que le contenu est transmis à une personne qui a accepté les modalités auxquelles l'accès au matériel protégé par le droit d'auteur est consenti. Le paiement peut aussi être effectué de cette façon. Dans ces circonstances, la confidentialité de la transaction entre le titulaire et le consommateur est assurée. De même, dans la mesure où les techniques de gestion numérique des droits permettent à un consommateur de transférer légitimement une œuvre, ou l'autorisation d'utiliser une œuvre, à un tiers, elles préservent la confidentialité et l'intégrité de la transaction. Enfin, dans la mesure où ces techniques permettent aux titulaires de droits et aux distributeurs d'enregistrer les données relatives aux consommateurs et à l'historique de leurs transactions, le processus d'achat et de réception de contenu protégé par des mesures de gestion numérique des droits peut être plus rapide et plus efficace. À chacun de ces égards, les consommateurs peuvent considérer que les techniques de gestion numérique des droits sont bénéfiques.

Les organismes de défense des consommateurs et de la vie privée ont toutefois vu un côté potentiellement négatif à l'utilisation des systèmes de gestion numérique des droits. Pour eux, l'utilisation de ces techniques facilitera inévitablement la collecte et la synthèse de données personnelles sur les consommateurs par les titulaires de droits et les distributeurs de contenu. Les consommateurs se méfient de l'établissement de profils et des techniques qui combinent des données relatives à leur utilisation avec leur identité. Ils craignent que les tiers puissent accéder à l'ordinateur individuel d'une personne en vue d'identifier les dispositifs pour s'assurer qu'ils sont "de confiance".

Une autre préoccupation se rapporte au fait que les consommateurs peuvent perdre leur capacité de faire une utilisation légitime, mais anonyme, de contenu protégé par le droit d'auteur. Dans certains cas d'usage "loyal", par exemple, les utilisateurs de contenu protégé peuvent vouloir utiliser le matériel sans nécessairement s'associer personnellement à l'œuvre qu'ils ont consultée et utilisée. Or, les techniques de gestion numérique des droits exigent souvent une transaction bilatérale entre un titulaire de droits et un consommateur connu et les droits d'utilisation de l'œuvre peuvent voyager avec le contenu lui-même. Par conséquent, le consommateur n'aura plus la faculté d'utiliser le contenu de manière anonyme.

Bien entendu, les consommateurs qui craignent pour la confidentialité devraient pouvoir désactiver ces systèmes de gestion numérique des droits ou simplement s'abstenir d'acheter du contenu en ligne. Cela étant, des préoccupations ont été exprimées, selon lesquelles ce faisant, les consommateurs pourraient – quoique de leur propre choix – se priver de la possibilité d'accéder aux œuvres protégées par le droit d'auteur qui, de plus en plus, peuvent être obtenues uniquement par l'intermédiaire des techniques de gestion numérique des droits.

Différentes institutions gouvernementales se sont intéressées à des degrés variables au rapport entre l'utilisation des systèmes de gestion numérique des droits et les préoccupations relatives au respect de la vie privée. Dans la Communauté européenne, l'alinéa 57 du préambule de la directive sur le droit d'auteur met nettement en relief ces questions : les systèmes de gestion des droits, est-il indiqué, "traitent des données à caractère personnel

relatives aux habitudes de consommation des particuliers pour ce qui est des objets protégés et permettent l'observation des comportements en ligne"[230]. Cet alinéa précise que les mesures techniques devraient incorporer "les principes de protection de la vie privée" prévus dans la directive européenne sur la protection des données, qui protège les données personnelles[231]. La directive sur la protection des données établit un cadre détaillé qui s'applique à la collecte, à l'utilisation, au traitement, à la divulgation et à la sécurité des données personnelles dans les États membres, ainsi qu'au transfert de ces données à des pays tiers. La directive sur la protection des données s'applique directement aux systèmes de collecte et de traitement automatisés tels que ceux utilisés dans un système de gestion numérique des droits.

Aux termes de la directive sur la protection de données, les données personnelles ne peuvent être recueillies et utilisées qu'aux fins autorisées par le "sujet des données", c'est-à-dire la personne à laquelle se rapportent les données. En outre, la directive exige que le responsable du traitement des données mette en œuvre "les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre … la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau…"[232]. Étant donné la portée de la directive sur la protection des données et son application directe aux systèmes de gestion numérique des droits, les craintes de voir les titulaires de droits et les distributeurs utiliser de manière abusive les données qu'ils recueillent sur les consommateurs devraient être au moins légèrement apaisées.

Aux États-Unis d'Amérique, la protection des données personnelles a souvent été assimilée à un patchwork, mettant en œuvre différentes lois fédérales et étatiques. Ces dernières années, la Commission fédérale du commerce et les procureurs généraux des États ont veillé à ce que les sociétés qui emploient des moyens techniques de protection ou de collecte de données informent précisément les consommateurs de leurs pratiques en matière de sécurité, de confidentialité et de collecte de données. Ces organismes gouvernementaux peuvent saisir les tribunaux et faire prononcer des amendes administratives contre les sociétés qui ne prennent pas des mesures de sécurité suffisantes pour protéger les données figurant dans leurs systèmes[233].

---

230 Alinéa 57.

231 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, Journal officiel L 281/31, 23/11/1995 [ci-après dénommée "directive sur la protection des données"].

232 Article 17 de la directive sur la protection des données.

233 Voir *In the Matter of Microsoft Corp.*, FTC n° 012 3240 (2002) (voir *http://www.ftc.gov/os/2002/08/microsoftcmp.pdf* (plainte déposée) et *http://www.ftc.gov/opa/2002/08/microsoft/htm* (règlement) (transaction concernant la plainte relative au système d'authentification Passport, interdisant la presentation d'informations erronées sur les pratiques en matière d'utilisation des données et exigeant la mise en œuvre d'un système perfectionné de sécurité informatique)); *In the Matter of Eli Lilly and Co.*, FTC n° 012 3214 (2002) (voir *http://www.ftc.gov./opa/2002/01/elililly.htm*) (transaction en faveur de la mise en place d'un programme de supervision intensif suite à la divulgation par erreur d'adresses de courrier électronique) (suivie d'une transaction avec les procureurs généraux de huit États); *In the Matter of Ziff Davis Media, Inc.,* engagement à mettre fin aux pratiques incrimées (28 août 2002) (voir *http://www.oag.state.ny.us/press/2002/aug/aug28a_02_attach.pdf*) (après divulgation par erreur des informations personnelles des clients, engagement à mettre fin à cette pratique avec les procureurs généraux du Vermont, de New York et de la Californie supposant

[Footnote continued on next page]

Toujours aux États-Unis d'Amérique, les questions de confidentialité ont été débattues dans le cadre de l'adoption du DMCA, qui reconnaît expressément un certain lien entre l'utilisation des techniques numériques et les préoccupations relatives au respect de la vie privée. Comme indiqué dans la section 3.2.1.1.c), l'article 1201.i) du DMCA crée une exception aux dispositions anticontournement en faveur de la confidentialité : le contournement d'une mesure technique protégeant les cookies ou d'autres éléments protégés par le droit d'auteur – tels que les programmes d'ordinateur utilisés dans un système de gestion numérique des droits – qui recueillent ou divulguent des informations au sujet des activités en ligne de la personne sans information préalable ne constitue pas une violation de l'interdiction légale.

Il reste à déterminer si l'exception prévue à l'article 1201.i) aura un effet significatif sur l'harmonisation des préoccupations relatives à la confidentialité et à l'utilisation des systèmes de gestion numérique des droits. Quoi qu'il en soit, l'incidence de cette exception risque d'être tout à fait limitée. Elle ne permet le contournement que s'il a pour seul effet de détecter et de neutraliser la mesure – et non pas d'obtenir l'accès non autorisé à une œuvre. De plus, l'exception s'applique seulement si le contournement a pour unique but d'empêcher la collecte ou la diffusion d'informations personnelles.

5.2.2 Compétence et législation applicable

Les systèmes de gestion numérique des droits seront inévitablement utilisés pour protéger et distribuer du contenu sur une base transfrontalière. Par conséquent, la question la législation applicable tant à la protection de ces systèmes qu'à celle du contenu risque de se poser. Le choix du droit applicable et les questions de compétence dans l'environnement en ligne, y compris celles qui se posent en ce qui concerne les arrangements de propriété intellectuelle, sont examinés dans de nombreuses instances internationales et régionales.

Trois questions de compétence distinctes mais néanmoins liées se posent en ce qui concerne l'utilisation des techniques de gestion numérique des droits.

– Premièrement, la législation anticontournement de quel pays doit s'appliquer à la protection – au contournement ou au piratage – des techniques de gestion numérique des droits?

– Deuxièmement, quelle législation doit s'appliquer à l'utilisation, ou à l'utilisation abusive, de contenu protégé par un système de gestion numérique des droits?

– Troisièmement, quelle législation nationale doit s'appliquer aux accords relatifs à la distribution de contenu par l'intermédiaire de systèmes de gestion numérique des droits?

Premièrement, les lois contenant des dispositions anticontournement et d'accès conditionnel décrites ci-dessus ont une portée territoriale. Si un acte de contournement, y compris le trafic d'instruments de contournement, se produit à l'intérieur des frontières d'un pays, la législation de ce pays est applicable. La compétence de ce pays pourrait même s'exercer sur la distribution en ligne d'un programme de contournement dans un autre pays,

---

[Footnote continued from previous page]

l'étude, le suivi et la mise en œuvre de mesures relatives à la confidentialité, à la sécurité et à l'intégrité des données et le versement de dommages-intérêts aux clients lésés).

bien qu'il puisse s'avérer difficile d'obtenir la compétence personnelle sur le distributeur étranger.

Dans la l'affaire *États-Unis d'Amérique* c. *Elcom, Ltd.* dont il est question à la section 3.2.2, un ressortissant étranger et une société étrangère ont été inculpés de violation des dispositions antitrafic de l'article 1201.b) aux États-Unis d'Amérique pour avoir créé et distribué le logiciel de décryptage du logiciel de sécurité Adobe eBook. Le tribunal a toutefois expressément rejeté l'argument selon lequel il devait exercer sa compétence sur une base extraterritoriale. Il a constaté que le défendeur avait des liens suffisants avec les États-Unis d'Amérique pour que les actes puissent être considérés comme ayant eu lieu dans ce pays : le logiciel de contournement illicite était proposé et vendu par l'intermédiaire de l'Internet aux résidents des États-Unis d'Amérique, le serveur Internet sur lequel le logiciel était vendu était situé dans ce pays, de même que le service de paiement en ligne[234].

Deuxièmement, si une personne parvient à utiliser une œuvre protégée d'une autre manière que celle autorisée par un système de gestion numérique des droits, une telle utilisation constituera très probablement une atteinte au droit d'auteur en vertu de la législation nationale pertinente. En ce qui concerne l'accès en ligne et l'utilisation du contenu, la jurisprudence et les principes internationaux évoluent, s'agissant tant du pays dans lequel une personne peut être poursuivie pour une atteinte multijuridictionnelle que de la législation applicable. Les principes applicables peuvent être tirés de la législation nationale et de l'Accord sur les ADPIC; des travaux sur ces questions sont aussi en cours dans le contexte du projet de Convention de La Haye sur la compétence et les jugements étrangers en matière civile et commerciale[235]. En janvier 2001, l'OMPI a organisé un forum sur le droit international privé et la propriété intellectuelle pour passer en revue, parmi différents thèmes, les questions de compétence (sur les parties et la plainte) et le choix de la législation en rapport avec les œuvres transmises sur les réseaux numériques[236].

Troisièmement, le choix de la législation applicable à un accord en vertu duquel un consommateur obtient un contenu par l'intermédiaire d'un système de gestion numérique des droits suppose un pays de contrat et des principes régissant le choix de la législation. En général, c'est la législation indiquée dans le contrat qui est applicable. Lorsque les parties n'ont pas choisi de législation applicable, d'autres principes peuvent être mis en œuvre, tel que celui prévu dans la Convention de Rome de 1980 : le tribunal doit appliquer la législation du pays où la partie qui doit procéder à l'exécution caractéristique du contrat a son domicile ou son siège principal[237].

---

234 *États-Unis d'Amérique* c. *Elcom, Ltd.*, n° CR 01-20138 RMW (N.D. Cal. 27 mars 2002) (ordonnance de rejet de la pétition du défendeur pour incompétence quant au fond).

235 Voir *http://www.hcch.net/e/workprog/jdgm.html*.

236 Des exposés ont été rédigés par les professeurs André Lucas et Jane C. Ginsburg. Voir A. Lucas, *Private International Law Aspects of the Protection of Works and of the Subject Matter of Related Rights Transmitted Over Digital Networks*, Forum de l'OMPI sur le droit international privé et la propriété intellectuelle (WIPO/PIL/01/1 Prov., 17 décembre 2000); J. Ginsburg, *Private International Law Aspects of the Protection of Works and Objects of Related Rights Transmitted Through Digital Networks (2000 Update)*, Forum de l'OMPI sur le droit international privé et la propriété intellectuelle (WIPO/PIL/01/2, 18 décembre 2000), tous deux disponibles à l'adresse *http://www.wipo.int/pil-forum/en/index.html*.

237 Article 4.2) de la Convention de la CE sur la législation applicable aux obligations contractuelles (Rome, 1980) (il est présumé que le contrat est le plus étroitement lié au pays où la partie qui doit exécuter l'opération caractéristique du contrat a, au moment de la conclusion

[Footnote continued on next page]

D'autres directives quant aux principes juridiques applicables dans la Communauté européenne figurent dans la directive sur le commerce électronique, qui adopte une "règle du pays d'origine". Un prestataire de services est soumis aux lois des États membres dans lesquels il est établi, l'établissement désignant le lieu à partir duquel il exerce son activité économique ou assure son service[238]. Aux États-Unis d'Amérique, chaque État a adopté un principe de législation applicable qui indique au tribunal la législation à appliquer en l'absence d'accord entre les parties.

5.2.3 Rôle des pouvoirs publics dans la normalisation et l'interfonctionnement

Une question centrale qui traverse les discussions relatives à l'élaboration et à la mise en œuvre des techniques de gestion numérique des droits concerne le rôle approprié et nécessaire des gouvernements ou des institutions intergouvernementales. L'exemple le plus célèbre est celui de la loi sur la télévision numérique à haut débit, examinée dans la section 3.2.1.4, qui a été rédigée sous l'impulsion des titulaires de droits, considérant que le secteur privé n'avançait pas assez rapidement pour résoudre les problèmes de protection de contenu. Les partisans du projet ont argué que le gouvernement devrait intervenir si les industries ne trouvaient pas elles-mêmes de solution technique à une certaine date. Le processus d'ateliers sur la gestion numérique des droits de la Commission européenne examiné dans la section 3.3.2 a commencé et s'est achevé sur la question de savoir si la Commission devait faire plus pour accélérer la mise au point de solutions de gestion numérique des droits, avec un accent particulier sur la normalisation internationale et l'interfonctionnement.

Dans l'examen de cette question, plusieurs observations peuvent être pertinentes. Premièrement, alors que les titulaires de droits et les sociétés de gestion collective sont certainement devenus plus favorables à l'intervention des pouvoirs publics en dernier recours, les industries de technologie ont vigoureusement et presque uniformément résisté à toute suggestion en faveur de l'intervention directe du gouvernement dans le processus d'établissement de normes. En fait, les sociétés de technologie comme la plupart des titulaires de droits considèrent qu'une normalisation volontaire mise en œuvre par le secteur privé est de loin préférable à l'intervention du gouvernement. Avec le temps, à mesure que la collaboration sectorielle s'est intensifiée en ce qui concerne l'élaboration de systèmes de gestion numérique des droits et que les travaux visant à trouver des solutions à des questions telles que la protection des émissions numériques avançaient, la nécessité d'une intervention des pouvoirs publics dans ce secteur semble avoir considérablement diminué.

Deuxièmement, dans la mesure où les diverses solutions de gestion numérique des droits actuellement adoptées pourraient être exclusives et non entièrement interopérables, la question a été posée de savoir si les gouvernements devraient eux-mêmes lancer les processus de normalisation et s'assurer que les techniques évoluent vers l'interfonctionnement. La plupart des représentants du secteur privé, qu'il s'agisse des entreprises de technologie ou des concepteurs de solutions de gestion numérique des droits, restent convaincus que ces

---

[Footnote continued from previous page]

du contrat, son domicile habituel, ou, dans le cas d'un organisme constitué ou non en société, son siège administratif).

238 Alinéa 19 du préambule de la directive sur le commerce électronique.

questions devraient demeurer du ressort de l'industrie. À leurs yeux, les forces du marché et les besoins des consommateurs sont des vecteurs plus probables de compatibilité et d'interfonctionnement entre les systèmes de gestion numérique des droits. Les gouvernements, en revanche, ne sont pas à même d'assumer un rôle moteur dans l'élaboration de solutions orientées vers le marché.

Les gouvernements peuvent toutefois contribuer à cet effort de plusieurs manières. En particulier, ils peuvent continuer à mettre à disposition les tribunes nécessaires pour les discussions intersectorielles. Dans ces instances, les participants du secteur privé peuvent exprimer et consigner les progrès qu'ils réalisent vers l'élaboration de solutions et en profiter pour informer les tiers, y compris les décideurs. En outre, les gouvernements peuvent jouer un rôle plus actif en créant des environnements juridiques qui favorisent la normalisation et la coopération. Les gouvernements qui souhaitent consolider les industries de la gestion numérique des droits et les autres industries de technologie et encourager l'utilisation des techniques de gestion numérique des droits voudront sans doute reconnaître l'importance de ces techniques dans leurs lois sur le droit de la concurrence et leurs instruments d'application des lois relatives à la concurrence.

Troisièmement, la plupart des grands participants du secteur privé reconnaissent que le gouvernement a un rôle à jouer s'agissant d'assurer l'application des solutions agréées par les participants du secteur privé. L'exemple des traités de l'OMPI et de la législation d'application de ces traités démontre que les lois adoptées par les gouvernements sont nécessaires pour sauvegarder les protections techniques. Les antécédents législatifs interdisant le piratage des systèmes d'accès conditionnel vont dans le même sens. Les mesures prises par le secteur privé et les accords entre parties privées n'offrent que des perspectives très limitées de trouver et de sanctionner les personnes qui cherchent à tirer un bénéfice de l'accès à un contenu qu'elles ne paient pas. Les lois sont essentielles pour s'assurer que chacun – particuliers et fabricants de produits – est soumis aux mêmes règles en matière de protection du contenu. À cet égard, le décret de la FCC sur le broadcast flag illustre le rôle que doit jouer le gouvernement, à savoir celui d'imposer la conformité aux solutions agréées par l'industrie.

Quatrièmement, le pouvoir des gouvernements en matière d'imposition de normes et de contrôle de leur respect est nécessairement limité à l'étendue de leur souveraineté. Même les institutions de l'Union européenne, qui sont habilitées à élaborer et à imposer des normes juridiques pour de multiples États membres, n'ont aucune compétence en dehors de leurs frontières. Mais, comme l'illustrent les traités de l'OMPI, la nécessité d'une approche harmonisée en ce qui concerne les techniques de protection du contenu, y compris les systèmes de gestion numérique des droits, est évidente. Il est par exemple indiqué dans la section 3.2.1.3.b) que les titulaires de droits ne seraient guère avancés que le contenu de leurs émissions numériques diffusées par voie hertzienne soit techniquement et juridiquement protégé contre leur rediffusion dans un pays si le même signal de télévision peut être reçu d'une autre manière dans un pays limitrophe et redistribué sans entrave et en toute impunité. En conséquence, il importe que les gouvernements s'interrogent en permanence sur les moyens de faciliter une approche permettant de protéger de manière transparente à la fois le contenu et les systèmes de gestion numérique des droits qui s'y rapportent.

5.2.4 Pratiques de licences de technologie et obligations en la matière

Les pratiques de gestion et les lois en matière de concession de licences sur les systèmes de gestion numérique des droits et, plus généralement, de normes techniques, sont directement liées à la question du rôle des pouvoirs publics dans l'établissement de normes. Les techniques et les normes de gestion numérique des droits peuvent être protégées ou régies par les lois relatives aux brevets, au droit d'auteur et aux secrets d'affaires.

On distingue généralement les normes "ouvertes" des normes "exclusives". Les normes "ouvertes" peuvent être élaborées dans le cadre d'un organisme à composition non limitée, sous réserve du règlement intérieur de l'instance considérée. Au niveau international, l'UIT et la Commission électrotechnique internationale sont des exemples d'organismes de normalisation "ouverts". Au niveau européen, l'Institut européen des normes de télécommunications en est un autre exemple. Parmi les organismes nationaux figurent notamment l'American National Standards Institute aux États-Unis d'Amérique et la Japan Electronics and Information Technology Industries Association au Japon.

Des normes "commerciales" sont élaborées et les techniques correspondantes sont cédées sous licence par les sociétés ou groupes de sociétés titulaires des droits de propriété intellectuelle pertinents. Les différentes techniques de gestion numérique des droits, dont plusieurs de celles examinées ci-dessus, sont le fruit d'activités de développement individuelles ou conjointes et sont cédées sous licence exclusive, contre redevances.

La cession sous licence de techniques incorporées dans les normes établies dans le cadre de processus ouverts, de même que celles contenues dans des systèmes commerciaux, est régie par des prescription juridiques. Pour s'assurer que des normes ne sont pas adoptées sans tenir compte des droits de brevet qui peuvent être applicables, les participants à une procédure volontaire mise en œuvre par un organisme ouvert doivent s'engager à informer les autres participants de tout droit de propriété intellectuelle sur une norme proposée et, en outre, à céder sous licence un tel droit à des conditions raisonnables et non discriminatoires[239]. Aux États-Unis d'Amérique, la Commission fédérale du commerce a considéré qu'il était déloyal pour un participant à un organisme de normalisation ouvert de ne divulguer ses revendications de brevet qu'après que l'organisme eut adopté une norme et a réglé la question en interdisant au titulaire du brevet de faire valoir ses revendications contre ceux qui appliquent la norme[240].

Certains organismes vont plus loin et insistent pour que toute revendication de brevet essentielle soit cédée sous licence à titre gracieux. En mai 2003, par exemple, le W3C a publié des principes relatifs aux brevets pour s'assurer que ses recommandations pourraient

---

239 Voir, par exemple, ETSI Intellectual Property Rights Policy (avril 2003) (imposant aux participants l'obligation d'informer les autres participants de toute revendication essentielle de propriété intellectuelle; de concéder des licences à des conditions raisonnables et non discriminatoires; de chercher des solutions de rechange si elles ne sont pas concédées à de telles conditions; et de rendre publiques les revendications de propriété intellectuelle sur les normes adoptées), à l'adresse *http://portal.etsi.org/directives/directives_apr_2003.doc*; ANSI Essential Requirements: Due process requirements for American National Standards, Section 3.1 (mars 2003) (les participants doivent reconnaître qu'ils n'ont aucune revendication de propriété intellectuelle ou, s'ils en ont, s'engager à les céder sous licence gratuite ou à des conditions raisonnables qui sont manifestement exemptes de toute discrimination injuste), à l'adresse *http://public.ansi.org/*ansionline*/Documents/Standards%20Activities/American%20National%20Standards/Procedures, %20Guides,%20and%20Forms/ER2003.doc*.

240 *In the Matter of Dell Computer Corp.*, décision et ordonnance, n° C-3658 (20 mai 1996), disponibles à l'adresse *http://www.ftc.gov/opa/1995/11/dell.htm*.

être appliquées sans redevances[241]. Le W3C s'efforce de s'assurer qu'il n'adoptera pas une recommandation si un participant a une revendication de brevet essentielle qu'il ne cédera sous licence que contre redevance.

Les techniques exclusives (qu'elles soient fondées ou non sur des normes ouvertes) sont concédées dans le cadre de contrats de licence négociés, qui régissent généralement des questions telles que les redevances, l'étendue de l'exploitation, les droits sur les développements futurs, etc. Les techniques de protection contre la copie, en particulier nombre de celles qui sont mises au point par les fabricants de matériel, sont généralement cédées sous licence quasiment à "prix coûtant", les redevances prélevées couvrant les frais administratifs.

En ce qui concerne les normes tant ouvertes qu'exclusives, les licences sur les normes et techniques de gestion numérique des droits doivent être conformes à la législation applicable, y compris les lois sur la concurrence des divers ressorts juridiques dans lesquels ces licences produisent leurs effets. La loi sur la concurrence est pertinente parce que les lois de propriété intellectuelle confèrent des droits exclusifs au titulaire et parce qu'il importe d'empêcher les pratiques abusives ou illicites en matière de licences. Les principaux ressorts juridiques ont établi des directives ou des règlements régissant l'interface entre la propriété intellectuelle et les accords de licence de technologie[242], les lois applicables étant également complétées par des décisions judiciaires.

5.3 Questions de politique générale : le rôle de l'OMPI et des autres organisations internationales

Compte tenu des tendances commerciales, techniques et juridiques et des questions de politique générale décrites ci-dessus, les auteurs ont examiné les mesures ou les initiatives que l'OMPI et d'autres organisations internationales pourraient prendre, selon que de besoin, afin de favoriser l'exécution efficace des dispositions relatives à la gestion numérique des droits contenues dans les traités Internet de l'OMPI. Conformément au mandat de l'OMPI, qui consiste à "promouvoir la protection de la propriété intellectuelle à travers le monde"[243], les auteurs suggèrent que l'OMPI examine les recommandations suivantes.

5.3.1 Diverses conceptions de la mise en œuvre des traités Internet de l'OMPI

---

241 Voir W3C Patent Policy (20 mai 2003), à l'adresse *http://www.w3.org/Consortium/Patent-Policy-20030520.html*.

242 Voir, Ministère de la justice et Commission fédérale du commerce des États-Unis d'Amérique, Antitrust Guidelines for the Licensing of Intellectual Property (6 avril 1995), à l'adresse *http://www.usdoj.gov/atr/public/guidelines/ipguide.htm*; Règlement (CE) n° 240/96 de la Commission, du 31 janvier 1996, concernant l'application de l'article 85 paragraphe 3 du traité à des catégories d'accords de transfert de technologie, Journal officiel L 031, 09/02/1996; Commission du commerce équitable du Japon, directives concernant les contrats de licence de brevet et de savoir-faire en vertu de la loi antimonopole (30 juillet 1999), à l'adresse *http://www2.jftc.go.jp/e-page/guideli/patent99.htm*; Bureau de la concurrence du Canada, directives d'application de propriété intellectuelle (publiées le 21 septembre 2000), à l'adresse *http://strategis.ic.gc.ca/SSG/ct01992e.html*.

243 Article 3.i) de la Convention instituant l'Organisation mondiale de la propriété intellectuelle.

Les sections 3 et 5.1.1 décrivent plusieurs des solutions adoptées par les gouvernements nationaux et l'Union européenne pour donner effet aux obligations qui leur incombent en vertu des traités Internet de l'OMPI. Comme indiqué ci-dessus, les législations d'application divergent légèrement.

Recommandation n° 1 :

L'OMPI pourrait entreprendre une étude détaillée des différentes solutions existantes pour donner effet aux obligations découlant des traités Internet de l'OMPI. Cette étude pourrait récapituler les choix qui ont été faits par les législateurs et passer en revue les incidences probables de ces différentes solutions sur l'étendue de la protection juridique des systèmes de gestion numérique des droits et du contenu distribué par l'intermédiaire de ces systèmes.

5.3.2 Utilisation des systèmes de gestion numérique des droits et accès au contenu

Dans le débat en cours aux niveaux national et européen sur la mise en œuvre des traités de l'OMPI, parmi les questions les plus intensément discutées figure celle de savoir si les systèmes de gestion numérique des droits et leurs fondements juridiques limiteront l'accès légitime des consommateurs au contenu. Les craintes de voir les œuvres "verrouillées" et l'avènement de la société du "paiement à l'utilisation" sont largement répandues, y compris dans les ressorts juridiques qui n'ont pas encore mis en œuvre les traités de l'OMPI ni la directive sur le droit d'auteur.

Comme indiqué ci-dessus, tant les États-Unis d'Amérique que la Commission européenne ont élaboré des mécanismes réglementaires publics pour évaluer si et dans quelle mesure les techniques de contrôle d'accès entravent réellement certaines utilisations qui, sans être expressément autorisées par les titulaires de droits, sont considérées comme un "usage loyal" ou des "exceptions" légitimes et appropriées au droit d'auteur. Ces mécanismes prévoient notamment un réexamen périodique effectué par le Bureau du droit d'auteur des États-Unis d'Amérique, ainsi que des rapports et des contrôle périodiques par la Commission européenne. Néanmoins, les organismes de défenses des consommateurs, les bibliothèques, les services d'archives et les établissements d'enseignement ont exprimé des préoccupations quant à savoir si ces processus ont une portée et un poids suffisants pour permettre de procéder en temps utile aux ajustements qui pourraient s'avérer nécessaires.

Hormis les activités de surveillance périodique de la Commission européenne, il n'y a aucune proposition visant à examiner de manière systématique les incidences actuelles et futures des mesures de contrôle d'accès pour les consommateurs. Jusqu'ici, cependant, et à de rares exceptions près (notamment en ce qui concerne le CSS et les DVD), les mesures techniques ne semblent ne pas avoir eu un effet significatif sur le droit des utilisateurs légitimes d'accéder aux œuvres protégées par le droit d'auteur. Avec le temps, cela peut (ou non) changer, selon la façon dont les systèmes de gestion numérique des droits seront mis en œuvre par les titulaires. L'ampleur de ces effets ne peut pas être encore appréhendée compte tenu du caractère limité des processus qui ont été mis en place.

Recommandation n° 2 :

Sur une base périodique, l'OMPI pourrait collecter des données ou passer en revue d'une autre manière la mesure dans laquelle les systèmes de gestion numérique des droits sont déployés et l'effet des mesures techniques sur l'accès légitime aux œuvres protégées par le droit d'auteur. Cette activité ne devrait pas nécessairement reproduire les mécanismes adoptés aux niveaux national et européen : elle pourrait revêtir une portée plus large et examiner de manière plus détaillée la situation au niveau international.

5.3.3 Exceptions ou limitations réglementaires aux dispositions anticontournement

Les traités de l'OMPI sont muets sur la question de savoir si leur mise en œuvre exige – ou limite – l'adoption de toute exception ou limitation en rapport avec l'obligation d'assurer une "protection juridique appropriée" et des "sanctions juridiques efficaces" contre la neutralisation des mesures techniques. Toutefois, comme il a été indiqué précédemment, la législation d'application tend à prévoir certaines exceptions ou limitations. Celles-ci diffèrent les unes des autres, traduisant différents choix de politique générale et l'influence de différents groupes d'intérêt sur le processus législatif.

Certaines de ces exceptions et limitations sont mentionnées expressément, d'autres sont implicites. Certaines font l'objet de dispositions contraignantes, d'autres figurent dans les alinéas du préambule ou les commentaires du texte. Certaines exceptions s'appliquent uniquement aux utilisateurs – par exemple pour certaines formes de reproduction ou de copie privée. D'autres s'appliquent uniquement à certaines activités – telles que l'ingénierie inverse et les essais informatiques. D'autres exceptions ou limitations sont applicables uniquement aux produits et aux dispositifs, telles que les "clauses d'exemption" (pour les produits légitimes d'électronique grand public, d'informatique et de télécommunications) et les dispositions relatives à la répartition des moyens pour assurer l'interfonctionnement entre les programmes d'ordinateur.

En dernière analyse, il n'y a aucune uniformité ou harmonisation aux niveaux international ou régional entre les exceptions ou limitations. Deux types de conséquences peuvent en résulter. Premièrement, dans une certaine mesure du moins, les consommateurs de contenu identique (et dont le titulaires sont identiques) et protégé par des systèmes identiques de gestion numérique des droits peuvent être soumis à des modalités juridiques différentes en matière d'accès au contenu exempté des lois anticontournement et d'utilisation de ce contenu – selon qu'ils tombent ou non sous le coup d'une exception ou limitation applicable dans le pays dans lequel ils vivent.

Deuxièmement, les exceptions et limitations applicables aux actes et aux instruments de contournement ont bien entendu une incidence sur la mesure dans laquelle les systèmes de gestion numérique des droits peuvent protéger le contenu. À l'avenir, au fur et à mesure que les systèmes de gestion numérique seront déployés, si ces exceptions et limitations sont invoquées par les utilisateurs et les fabricants de produits d'électronique grand public et d'informatique, il faudra sans doute mieux appréhender ces incidences au niveau international. À titre d'exemple, dès lors qu'une personne aura accès au contenu ou utilisera celui-ci (malgré la gestion numérique des droits) sur la base d'un acte de contournement licite dans un pays, ce contenu pourra être diffusé plus largement sur l'Internet ou d'une autre manière.

De même, un produit ou un programme d'ordinateur qui est capable de contourner une mesure technique peut être licite dans un pays parce que, par exemple, il a des buts légitimes

autres que le contournement et parce que les lois de ce pays interdisent seulement les produits qui ont le contournement pour unique but ou fonction. Or, dès lors que ce produit est utilisé dans ce pays pour accéder à un contenu qui est protégé par des mesures techniques, ce contenu n'est en fait plus protégé dans ce pays et peut alors faire l'objet d'une redistribution au niveau mondial, ce qui peut donner lieu à des utilisations non autorisées ailleurs.

Ce qui précède donne à penser que les exceptions et limitations doivent être rédigées avec soin. Il est essentiel que seules certaines activités légitimes entrent dans le cadre des exceptions. Des directives sur la façon dont il convient de rédiger les exceptions et limitations, pour tenir compte non seulement des besoins légitimes en matière d'accès et d'utilisation mais aussi des préoccupations légitimes des titulaires de droits concernant le contenu qui (en vertu d'une exception) échappe à la protection des systèmes de gestion numérique des droits, peuvent se révéler utiles.

Recommandation n° 3 :

Plus les titulaires de droits utiliseront les systèmes de gestion numérique, plus les exceptions ou limitations adoptées par les ressorts juridiques dans la mise en œuvre des dispositions anticontournement prendront de l'importance. L'OMPI pourrait examiner les effets internationaux des disparités entre ces exceptions ou limitations sur 1) les personnes qui souhaitent utiliser de manière licite des œuvres protégées par le droit d'auteur en invoquant les exceptions et limitations, 2) les fabricants de produits légitimes et 3) les titulaires de droits.

5.3.4 Modification des taxes pour la copie privée dans le cadre de la transition vers la gestion numérique des droits

Comme indiqué dans la section 5.1.3, plusieurs ressorts juridiques ont mis en place des systèmes de taxes sur les dispositifs et les supports au titre de la copie privée. Depuis plusieurs années, les discussions se sont concentrées sur les questions de savoir 1) si ces taxes sont nécessaires, 2) dans l'affirmative, quels produits devraient être taxés, 3) quel doit être le montant de ces taxes et 4) à qui le produit des taxes doit être versé. Ainsi qu'il ressort clairement de la discussion concernant l'Union européenne, avec l'évolution de l'environnement numérique, l'extension potentielle des systèmes de taxes aux dispositifs et supports numériques, notamment multifonctionnels, suscite parmi les consommateurs et les industries de technologie des préoccupations quant au respect de l'équité. En particulier, les consommateurs ne devraient pas devoir payer deux fois – une fois au titre d'une taxe sur les dispositifs et supports numériques et une autre fois dans le cadre d'un système d'accès conditionnel – pour un usage unique du contenu. À l'inverse, le maintien ou l'augmentation des taxes pourrait réduire les incitations à la mise au point et à l'adoption de solutions de gestion numérique des droits.

Recommandation n° 4 :

L'OMPI pourrait évaluer l'effet des divers systèmes de taxes pour la copie privée compte tenu de l'adoption éventuellement largement répandue des techniques de gestion numérique des droits dans l'économie numérique mondiale. En Europe, la Commission européenne a été instamment priée d'aider les États membres à déterminer quand et comment il convient de modifier ces taxes dans le cadre de la transition vers la gestion numérique des droits. L'OMPI pourrait jouer un rôle d'intermédiaire neutre en permettant aux experts de

partager des informations pour renforcer au niveau international la compréhension collective du rapport entre les taxes et la gestion numérique des droits. Ce processus pourrait être utile pour évaluer l'opportunité de mettre au point des mécanismes de modification, selon que de besoin.

[Fin du document]