F

OMPI

WCT-WPPT/IMP/2
ORIGINAL : français
DATE : 23 novembre 1999

ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE
GENÈVE

ATELIER SUR LA MISE EN OEUVRE 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)

Genève, 6 – 7 décembre 1999

LA PROTECTION LÉGALE DES SYSTÈMES TECHNIQUES

présenté par Alain Strowel[*]
et Séverine Dusollier[**]

[*] Professeur aux Facultés universitaires Saint-Louis, Bruxelles, et à l'Université de Liège; avocat, Cabinet Dutilh.

[**] Chargée de recherche et responsable de la section "propriété intellectuelle" au Centre de recherche informatique et droit, Facultés universitaires Notre-Dame de la Paix, Namur.

TABLE DES MATIERES

Page

Introduction et champ de l'étude 1

A. TYPOLOGIE DES MESURES TECHNIQUES DE PROTECTION 1

1. Mesures techniques protégeant les droits des auteurs 2
2. Systèmes d'accès 2
3. Outils de marquage et de tatouage 3
4. Systèmes de gestion électronique 4

B. DISPOSITIFS LÉGAUX DE PROTECTION DES SYSTÈMES TECHNIQUES 6

1. Protection spécifique à la propriété intellectuelle 6

1.1. Critères de comparaison des dispositifs légaux 6

1.2. Protection des mesures techniques dans l'Union européenne : 9

a) La directive sur la protection des programmes d'ordinateur et sa transposition dans les États membres 9

b) Proposition de directive sur le droit d'auteur et les droits voisins dans la société de l'information 10

Actes prohibés 11
Objet de la protection 11
Type d'activités illicites et responsabilité 12
Appareils illicites 13
Limites du droit d'auteur et protection. 13
Exceptions à l'interdiction de la neutralisation. 14
Clause de no mandate 14

1.3. Protection des mesures techniques aux États-Unis : 14

a) Section 1002 du *Copyright Act* : La protection des *Serial Copy Management Systems* 14

b) *Digital Millenium Copyright Act* 15

i) La protection des systèmes de contrôle d'accès 16

Objet de la protection 16
Type d'activités illicites 17
Appareils illicites 18
Exceptions à la prohibition de la neutralisation des systèmes d'accès et de la fabrication de dispositifs 18
Limites du droit d'auteur et protection 19

ii) La protection des mesures techniques protégeant les droits d'auteur 19

Objet de la protection *19*
Exceptions et mesures techniques de protection des droits *20*
Exceptions à la fabrication de dispositifs illicites *20*
Clause de no mandate *20*

1.4. Australie : *Copyright amendment (Digital Agenda) Bill of 1999* 20

Objet de la protection *21*
Actes prohibés et appareils illicites *21*
Limites du droit d'auteur et exceptions *22*
Exceptions à l'interdiction de neutralisation *22*

1.5. Autres pays 22

2. Protection des mesures techniques contrôlant l'accès à des services 23

3. Dispositions en matière de criminalité informatique 25

C. CONSIDÉRATIONS FINALES 27

1. Éléments d'une protection adéquate et efficace 27

1.1. Quant à l'objet de la protection 27
1.2. Quant aux types d'actes illicites 28
1.3. Quant au type d'appareils illicites 28

2. Limitations du droit d'auteur et exceptions 29

2.1. Exceptions et fabrication de dispositifs de contournement 29
2.2. Exceptions et acte de neutralisation 30

Introduction et champ de l'étude

En décembre 1996, la communauté internationale négociait et adoptait au sein de l'Organisation Mondiale de la Propriété Intellectuelle deux traités majeurs dont l'objectif premier était d'adapter le cadre juridique du droit d'auteur et des droits voisins aux nouvelles technologies.[1] Deux dispositions de ces traités ont instauré un nouveau type de protection visant les mesures techniques protégeant les œuvres. Plusieurs États ont déjà transposé ces dispositions particulières dans leur loi nationale, d'autres sont en train de le faire.

L'objet de la présente étude est d'analyser de manière comparative ces différentes dispositions nationales ou régionales, leur étendue et leur champ d'application, ainsi que de présenter d'autres textes érigeant une protection similaire pour les mesures techniques.

Une attention particulière sera accordée à la question de l'interaction des limitations du droit d'auteur et de la protection juridique des ces technologies, ainsi qu'à la définition des éléments nécessaires à une protection adéquate et efficace à l'encontre de leur neutralisation.

A. TYPOLOGIE DES MESURES TECHNIQUES DE PROTECTION

Les technologies susceptibles d'être utilisées par les auteurs et autres titulaires de droit pour protéger leurs œuvres et prestations[2] dans la société de l'information sont extrêmement diverses. Certaines ont été conçues spécifiquement pour répondre à la menace que le numérique apportait au droit d'auteur, d'autres ont été développées pour protéger indifféremment tout type de contenu numérique, qu'il soit soumis au droit d'auteur ou non.

Il est difficile de dresser une liste précise des mesures technologiques existantes ou en cours de développement, de même qu'il est impossible de prédire l'avenir de ces technologies dans le domaine de la protection des œuvres soumises au droit d'auteur.[3]

Pour cette raison, nous avons choisi de présenter et de regrouper les mesures techniques de protection du droit d'auteur et des droits voisins en quatre grandes catégories selon le type de fonction principalement poursuivie par ces dispositifs. On peut ainsi distinguer les mesures qui protègent effectivement un acte soumis au droit exclusif de l'auteur, les systèmes d'accès conditionnel, les outils de marquage et d'identification et les systèmes de gestion électronique des droits. Dans chaque catégorie, des exemples précis de technologies seront brièvement présentés.

---

1 J. REINBOTHE, M. MARTIN-PRATT, S. VON LEWINSKI : *The New WIPO Treaties : a First Résumé, E.I.P.R.* 1997/4, p. 173; A. LUCAS, *Droit d'auteur et numérique*, Droit@Litec, 1998, p. 270 et suiv.

2 Par la suite, pour des raisons de commodité, nous parlerons uniquement de la protection des droits d'auteur sur les œuvres, sans mentionner nécessairement celle des droits connexes portant sur diverses prestations ou objets.

3 D. GERVAIS, *Gestion Électronique des Droits et Systèmes d'Identificateurs Numériques*, Comité consultatif de l'OMPI sur la gestion du droit d'auteur et des droits connexes dans le cadre des réseaux mondiaux d'information, Première session, Genève, 14 et 15 décembre 1998.

1. Mesures techniques protégeant les droits des auteurs

Il s'agit des outils techniques qui empêchent l'accomplissement de tout acte ou usage soumis aux droits exclusifs des ayants droit, tels que l'impression, la communication au public, la copie digitale, l'altération de l'œuvre, etc. On parle surtout des systèmes anti-copie dont la fonction principale est d'empêcher l'accomplissement d'une copie de l'œuvre ou de l'objet protégé, soit uniquement digitale, soit toute copie numérique ou analogique. Par exemple, le **dongle**, utilisé principalement dans le secteur du logiciel, consiste généralement en un élément du hardware,[4] une sorte de clé, qui se branche sur le port série (*serial port*) de l'ordinateur. Tout logiciel protégé par ce système se connecte alors à cette clé pour vérifier quelle est l'étendue des droits de l'utilisateur. Le principe des dongles apparaît comme un précurseur de la technologie des **cartes à puces** ou ***smart cards*** qui autorisent le stockage d'un plus grand nombre d'informations. En outre ces cartes à puces peuvent contenir des unités de paiement pré-acquittées. Contrairement aux dongles dont l'utilisation s'est jusqu'ici limitée aux logiciels d'un coût élevé, les cartes à puces seront sans doute plus fréquemment utilisées pour les logiciels, ainsi que pour d'autres œuvres offertes au grand public. Ces deux technologies poursuivent à la fois un but d'accès et de contrôle des utilisations, notamment de la copie.

Le ***Serial Copy Management System*** est un système principalement utilisé aux États-Unis sur les dispositifs d'enregistrement audio digitaux tels le DAT et les mini-disques. Cette technologie permet à l'appareil de décoder les signaux audio intégrés dans le support et de décoder notamment les données relatives à la protection de celui-ci. Le système autorise la réalisation d'une seule copie digitale à partir de l'original mais empêche toute copie ultérieure. Un système similaire, le *Content Scrambling System*,[5] basé sur la technique de la cryptographie, a été apposé sur les DVD afin d'en empêcher toute reproduction.

2. Systèmes d'accès

L'un des enjeux majeurs des réseaux numériques est de sécuriser l'accès à l'information et aux contenus protégés, à la fois dans le but de garantir le paiement d'une rémunération et pour protéger les droits d'auteur sur l'œuvre ainsi "cadenassée". De nombreux systèmes ont donc été mis au point en vue de garantir et sécuriser l'accès soit à une œuvre, soit à un ensemble d'œuvres, soit à un service comprenant notamment des œuvres protégées. Désactiver le mécanisme de contrôle d'accès se réalise soit par paiement, soit lorsque les autres conditions de la licence conclue avec les titulaires de droit auront été remplies. Le dispositif d'accès peut ne contrôler qu'un accès initial et ensuite laisser l'œuvre libre de toute utilisation ou vérifier, à chaque nouvel accès, le respect des conditions. L'accès peut également être facilement différencié selon le type d'utilisateurs, ce qui constitue un grand avantage de ces systèmes. Par exemple, une université peut avoir obtenu un accès contre un prix forfaitaire annuel à une œuvre ou une collection d'œuvres pour un certain nombre d'étudiants et pour une durée d'une année. Le système vérifiera dans ce cas l'existence de la clé de décryptage sur les ordinateurs de l'université ou l'utilisation du mot de passe convenu contractuellement, voire l'identité de l'étudiant. A l'inverse, la même technologie peut

---

[4] Il peut également s'agir d'une disquette que l'on insère dans l'ordinateur lorsque l'utilisateur souhaite utiliser le logiciel. Le logiciel ne fonctionnera alors qu'à condition que cette disquette soit en possession de l'utilisateur.

[5] D. MC CULLAGH, *Blame US Regs for DVD Hack*, *Wired News*, 11 novembre 1999.

accorder des accès répétés à un particulier en échange d'un paiement renouvelé, notamment proportionnel à la fréquence d'utilisation.

Les technologies remplissant cette fonction sont nombreuses : cryptographie, mots de passe *set-top-boxes*, *black-boxes*, signatures digitales, enveloppe numérique.[6] Le procédé de **cryptographie** est bien connu. Il peut être défini, à l'instar de la loi française sur la réglementation des télécommunications comme "*la transformation à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse grâce à des moyens conçus à cet effet*".[7] Dans le monde numérique le cryptage et décryptage se réalise au moyen d'algorithmes de degré de complexité variable. Les **signatures digitales** sont une application particulière de la cryptographie réalisée pour certifier et identifier un document.[8] Dans le cadre de la protection du droit d'auteur, cette technologie est principalement utilisée pour sécuriser les transmissions sur les réseaux des œuvres et pour empêcher l'accès à l'œuvre à toute personne non autorisée. La fourniture de la clé de décryptage se réalise moyennant paiement du prix ou respect des autres conditions auxquelles est subordonnée l'utilisation de l'œuvre.

L'enveloppe digitale ou **container numérique** est une application de la cryptographie par laquelle une œuvre est "insérée" dans une enveloppe numérique qui contient les informations relatives à l'œuvre et les conditions d'utilisation de celle-ci. Ce n'est qu'en répondant à ces conditions (telles que paiement d'une rémunération, utilisation d'un mot de passe, etc.) que l'enveloppe s'ouvre et que l'utilisateur peut accéder à l'œuvre.

3. Outils de marquage et de tatouage

De nombreuses techniques sont susceptibles de jouer une fonction d'identification et de marquage des œuvres.[9] Les objectifs de ces techniques sont variés : la principale est de servir de support, de manière visible ou invisible, à l'insertion de données relatives à l'œuvre, qu'il s'agisse du titre de l'œuvre, de l'identité de son créateur et du titulaire de droits, ainsi que des conditions d'utilisation. Cette fonction sera particulièrement protégée dans le cadre de l'article 12 du Traité de l'OMPI sur le droit d'auteur, article relatif à la protection de l'information sur le régime des droits. On parle ici surtout du procédé de ***watermarking*** ou **tatouage** qui permet d'insérer en filigrane certaines informations dans le code digital de l'œuvre. Ce marquage est en général invisible et inaudible. Cette inscription invisible est réalisée par la technique de la stéganographie qui peut être définie comme "*l'art et la science de communiquer de manière à masquer l'existence même de la communication*".[10] L'utilisation d'encre invisible constitue un exemple de cette science millénaire empruntée au monde analogique. Dans un environnement numérique, le *watermarking* modifie certains bits

---

6 Les dongles et cartes à puces (voir supra) peuvent également avoir une fonction de contrôle d'accès.

7 Loi 90-1170 du 29 décembre 1990, J.O., 30 décembre 1990, p. 16439.

8 J. HUBIN, Y. POULLET, avec la collaboration de B. LEJEUNE et P. VAN HOUTTE, *La Sécurité informatique, entre technique et droit*, Cahier du CRID no 14, Bruxelles, Story-Scientia, 1998.

9 S. DUSOLLIER, *Le droit d'auteur et son empreinte digitale, Ubiquité*, n° 2, Mai 1999, p. 31-47.

10 R. LEYMONERIE, *Cryptage et Droit d'auteur, Les Cahiers de la Propriété Intellectuelle*, 1998, Vol. 10, n°2, p. 423; voir également D. GUINIER, *La stéganographie, De l'invisibilité des communications digitales à la protection du patrimoine multimédia, Expertises*, juin 1998, p. 186-190.

dits "inutiles"[11] d'une image ou d'un son. A l'aide d'un logiciel approprié, ce code numérique peut être extrait et déchiffré. Le marquage est généralement indélébile et se retrouve, même après une altération ou un découpage de l'œuvre, dans chaque partie de celle-ci.

Cependant, d'autres caractéristiques de ces technologies permettent de protéger plus ou moins directement le droit d'auteur. Tout d'abord, le marquage est dans certains cas parfaitement visible, une "marque" est alors clairement apposée sur la représentation de l'œuvre, de manière quelque peu similaire à l'apposition du terme "SPECIMEN" sur des faux billets de banque ou autres papiers officiels. Cette pratique, également appelée "*fingerprinting*", est assez répandue dans les agences de photos qui appliquent ainsi leur nom ou leur logo sur un exemplaire d'une photo aux seules fins de promotion et ne communiquent l'image débarrassée de ce marquage que lorsque le paiement de la rémunération prévue a été effectué. C'est le cas également dans certains musées ou archives en ligne dont les reproductions des collections s'ornent du sceau du musée.[12] Ce *watermarking* visible remplit dans ce cas une fonction de protection contre la copie dans la mesure où ce marquage nettement apparent implique une diminution de la valeur de ce qui est gratuitement accessible sur les réseaux.

Chaque exemplaire différent de l'œuvre distribué aux utilisateurs peut en outre intégrer un numéro de série numérique distinct. Dans ce cas, une copie pirate retrouvée par la suite sur le marché peut révéler l'exemplaire originel à partir duquel cette contrefaçon a été réalisée. Cet estampillage de chaque image permet donc de remonter à la source de copies non autorisées de l'image à l'aide d'un fichier reprenant ces numéros de série et les utilisateurs auxquels ces images estampillées ont été licenciées. Ici la fonction essentielle de la technique de protection est d'apporter des éléments de preuve quant à la contrefaçon. Enfin, une dernière fonction utile du *watermarking* est d'authentifier le contenu marqué, notamment en assurant que l'œuvre a conservé son intégrité.

4. Systèmes de gestion électronique

Les outils de gestion électronique sont toutes les technologies qui assurent la gestion des droits sur les réseaux en permettant la conclusion de licences d'utilisation *on-line* et en contrôlant l'utilisation des œuvres. D'autres fonctions peuvent également être prises en charge par ces outils : la répartition des droits perçus, la perception des paiements, l'envoi de factures, la réalisation de données de profilage des utilisateurs, etc. A titre d'exemple, les **agents électroniques** ont récemment fait leur apparition sur le marché.[13] Développés pour accomplir de nombreuses fonctions sur les réseaux, certains d'entre eux sont programmés

---

11 Ces bits sont inutiles en ce sens que les images et les sons comprennent un grand nombre de bits dont la suppression ou la modification n'entraînent aucune conséquence perceptible pour l'auditeur ou le spectateur. Par exemple dans le cas d'une oeuvre sonore, la ligne de code numérique permettant le marquage est insérée dans les bits de fréquence inaudibles pour une oreille humaine.

12 Un exemple en est la Bibliothèque du Vatican dont les documents précieux ont été numérisés et mis à la disposition du public *on-line*, toutefois recouverts du sceau du Vatican, ce qui empêche toute forme de réutilisation commerciale.

13 R. JULIA-BARCELO, *Electronic contracts = A new legal framework for electronic contracts : the EU electronic commerce proposal*, *C.L.S.R.*, 06/1999, n° 15/3, pp. 147-158.

pour négocier et conclure des contrats électroniques.[14] Cette technologie commence à s'appliquer également au droit d'auteur dans la mesure où de tels *contracting agents* accompagnent la diffusion de contenu protégé sur Internet à la fois pour afficher les termes et conditions des licences d'utilisation et pour recevoir et gérer l'acceptation ou le *clic* des utilisateurs. D'autres agents plus performants gèrent complètement de manière automatisée la distribution et l'utilisation de l'œuvre, notamment en intégrant un système de paiement électronique, en renouvelant les licences d'utilisation, ou en réalisant un compte rendu précis de l'utilisation (quelles œuvres ont-elles été copiées, imprimées, agrandies, téléchargées? combien de fois?), à la fois dans un but de facturation adéquate et proportionnelle à l'utilisation réelle et dans un but de marketing ultérieur (quel utilisateur apprécie tel type de musique?). On peut également imaginer que la répartition des droits à destination des auteurs et artistes interprètes et autres titulaires de droits puisse être effectuée en ligne par de tels agents. Lorsque ces agents se contentent de contrôler l'utilisation des œuvres et de dresser la fréquence de consultation des œuvres et des sites web, voire d'établir des profils précis des utilisateurs, on parle souvent de ***metering systems***.

Enfin, les ***Electronic Right Management Systems*** ou ***ERMS*** sont sans doute les mesures de protection dont on parle le plus, bien qu'il faut se garder d'y voir une technologie spécifique. Les ERMS (dénommés également ***ECMS*** pour *Electronic Copyright Management Systems*) consistent plutôt en une combinaison de nombreux outils et technologies dans le but d'exercer plusieurs fonctions.[15] Ainsi, un outil de cryptographie bloquant l'accès à l'œuvre peut être associé à un système anti-copie empêchant la reproduction de l'œuvre même par un utilisateur légitime. La technique du *watermarking* (voir supra) et un système de licence et de paiement électroniques peuvent également être intégrés dans le même programme informatique. Généralement, la fonction principale des ERMS est de gérer les utilisations et licences des œuvres *on-line*. C'est à ce titre que nous les rangeons dans la catégorie des outils de gestion.

En outre, les technologies développées actuellement et auxquelles sont susceptibles de recourir les titulaires de droits pour protéger leurs œuvres, remplissent de nombreuses fonctions plus marginales dont certaines sont encore plus éloignées du champ strict de la propriété intellectuelle. Celles-ci sont notamment :

– la mention des termes et conditions d'utilisation de l'œuvre;
– la transmission sécurisée du contenu;
– la preuve de la réception du contenu et de l'identité de la personne ayant reçu légitimement ce contenu;
– le paiement;
– l'enregistrement et le suivi des utilisations, notamment dans un but de paiement adéquat ou de marketing.

---

14 S. GAUTHRONET ET F. NATHAN, *On-line services and data protection and the protection of privacy*, Étude réalisée pour le compte de la Commission européenne, DG XV, p. 31.

15 M. LEDGER ET J.P. TRIAILLE, *Dispositions contre le contournement des dispositifs techniques de protection*, in *Copyright in Cyberspace*, ALAI Study Days, Amsterdam, June 1996, Ed. ALAI, 1997. <http://www.droit.fundp.ac.be/espacedroit/textes>; D. GERVAIS, *Electronic Right Management Systems (ERMS), The next logical step in the evolution of rights management*, (1997), voir http://www.copyright.com/stuff/ecms_network.htm.

Ces fonctions sont essentielles au contrôle et à la rémunération des titulaires des droits. Toutefois les technologies qui assurent le bon déroulement de ces autres facettes de la transaction entre un auteur et un utilisateur ne seront pas forcément couvertes par les dispositions légales protégeant les mesures techniques. Il faudra donc trouver une autre base juridique pour poursuivre d'éventuels contrefacteurs de ces systèmes complémentaires. Ce point dépasse le cadre de la présente étude.

B. DISPOSITIFS LÉGAUX DE PROTECTION DES SYSTÈMES TECHNIQUES

Nous avons vu combien la technologie dont se serviront les auteurs et autres titulaires de droit pour protéger leurs œuvres sert généralement différentes fonctions et est susceptible de sécuriser et de gérer électroniquement une multitude de contenus et d'informations numériques éventuellement non protégés par un droit intellectuel. Le même système de contrôle d'accès peut être utilisé pour des sites web contenant de la musique, de simples informations financières ou pour la diffusion sur Internet de programmes de télévision. La conséquence en est double.

D'une part, les technologies sont et seront utilisées par différents opérateurs dans des buts variés. Dès lors, la protection légale de ces techniques peut être consacrée par d'autres textes que ceux relatifs à la propriété intellectuelle.

D'autre part, les systèmes et mécanismes de neutralisation de ces technologies apparaissent sur le marché pour contourner un type de technologie qui peut être indifféremment utilisée dans des buts variés. L'objectif premier de ces dispositifs illicites n'est donc pas forcément de porter atteinte à un contenu protégé par le droit d'auteur ou les droits voisins; par conséquent, l'arsenal juridique devrait prévoir des sanctions hors du cadre strict de la propriété intellectuelle. Par exemple, un *hacker* peut chercher à défaire une protection spécifique à des contenus protégés par le droit d'auteur (songeons par exemple aux personnes qui ont révélé récemment sur Internet comment neutraliser la protection anti-copie des DVD), mais il peut aussi développer un dispositif de contournement d'une mesure de sécurité, dispositif qui pourrait par la suite être repris dans un but d'infraction au droit d'auteur. Afin d'interdire de tels dispositifs, les titulaires de droit pourraient se référer à d'autres textes légaux que ceux qui transposent les Traités OMPI.

C'est la raison pour laquelle nous nous proposons, après avoir étudié en droit comparé les dispositions légales qui protègent spécifiquement les droits intellectuels (point 1), de donner un aperçu d'autres dispositions légales qui seraient susceptibles de sanctionner la neutralisation de technologies protégeant le droit d'auteur, telles que la directive européenne sur la protection des services à accès conditionnel (point 2), ou encore certaines dispositions nationales en matière de criminalité informatique (point 3).

1. Protection spécifique à la propriété intellectuelle

1.1. Critères de comparaison des dispositifs légaux

Lors de la Conférence diplomatique de 1996, les pays membres de l'OMPI n'ont pu s'accorder sur un régime de protection très détaillé des mesures techniques de protection du droit d'auteur et droits voisins. Le texte du Traité demande aux États d'adopter une protection juridique "*contre la neutralisation des mesures techniques efficaces qui sont mises*

en œuvre par les auteurs dans le cadre de l'exercice de leurs droits et qui restreignent l'accomplissement d'actes qui ne sont pas autorisés par les auteurs concernés ou permis par la loi". L'article 11 du Traité OMPI sur le droit d'auteur et l'article 18 du Traité sur les Phonogrammes, ne précisent en aucune manière comment cette protection doit être organisée,[16] ni quels sont les actes précis qui devraient être prohibés. Entière liberté est laissée aux États sur ce point, ce qui implique que les dispositions nationales risquent d'être peu harmonisées, même si, à l'analyse, les modèles américain et européen semblent avoir inspiré les autres législateurs.

Plusieurs pays ont achevé ou entamé la transposition en droit interne des obligations relatives à la protection légale des mesures techniques résultant des Traités OMPI de 1996. La complexité de ces dispositions nationales nouvelles ou de ces projets est grande. Nous analyserons les dispositifs légaux déjà adoptés selon différents critères qui sont :

- **l'objet de la protection et la définition des mesures techniques** : toutes les mesures techniques ne sont pas forcément protégées dans tous les textes. Si le Traité OMPI parle en général des "*mesures techniques efficaces qui sont mises en œuvre par les auteurs dans le cadre de l'exercice de leurs droits"*, les dispositions nationales sont souvent plus précises et limitent la protection en définissant soit les mesures techniques visées, soit le critère d'efficacité qui justifie la protection. Nous verrons également que les législateurs ont souvent institué une protection double à la fois pour les systèmes contrôlant l'accès aux œuvres et pour les systèmes protégeant directement les droits exclusifs de l'auteur.

- **l'étendue de la prohibition (acte de neutralisation et/ou actes préparatoires à la neutralisation)** : les textes de l'OMPI semblent ne concerner que l'acte de neutralisation même de la mesure technique de protection. Or, les titulaires de droit et les législateurs insistent sur la nécessité d'une interdiction des activités dites préparatoires à la neutralisation que constituent la fabrication et la mise à la disposition du public de dispositifs de contournement. Il est en effet évident que le préjudice causé aux titulaires de droit sera d'autant plus grand si les moyens techniques de neutralisation sont facilement et largement disponibles sur le marché. Dès lors, la plupart des dispositions ou projets nationaux instituent une double incrimination, d'une part à l'égard des personnes qui neutralisent la mesure technique, d'autre part à l'égard de la commercialisation des dispositifs susceptibles de permettre ou de faciliter cette neutralisation.

- **le type d'activités préparatoires illicites :** les législateurs déterminent généralement strictement les activités susceptibles d'entraîner la responsabilité des fabricants de dispositifs de neutralisation. Dès lors, les activités illicites sont énumérées, de la fabrication à toutes les sortes de distribution au public des dispositifs illicites. Dans ce cadre, nous examinerons si la prestation de services de neutralisation est également incriminée.

- **les conditions d'illicéité des appareils :** une question essentielle est de déterminer à partir de quel moment un dispositif *a priori* licite peut être considéré comme illégitime. Un grand nombre de dispositifs électroniques ou informatiques sont spécifiquement conçus pour contourner la mesure technique et explicitement

---

16 J. REINBOTHE, M. MARTIN-PRATT, S. VON LEWINSKI, op.cit., p. 173.

commercialisés dans ce but. D'autres peuvent être détournés de leur fonction *a priori* légitime afin de servir des objectifs moins licites. Il est donc essentiel de tracer une ligne nette entre les dispositifs licites et ceux qui ne le sont pas.[17] La définition précise et claire de l'illicéité est d'ailleurs une préoccupation majeure de l'industrie des équipements électroniques qui réclame à cet égard une certaine sécurité juridique. Par exemple, un magnétoscope dont la fonction première est la lecture et l'enregistrement de programmes audiovisuels mais dont une fonction accessoire permet de neutraliser la protection technique apposée sur les cassettes vidéos est-il illicite? Qu'en est-il d'un logiciel de cryptage que les utilisateurs usent surtout pour décrypter sans autorisation certains signaux? En bref, la fonction de neutralisation doit-elle être principale, unique, prédominante ou simplement accessoire?

- **la connaissance de l'atteinte en tant que condition de la responsabilité :** certains textes exigent de l'auteur des agissements illégitimes une certaine connaissance de l'atteinte au droit d'auteur. Dans certaines législations, l'auteur d'un acte de contournement ne sera responsable que s'il savait ou devait savoir qu'il commet ainsi une infraction au droit d'auteur.

- **le sort des limitations du droit d'auteur :** une des questions les plus controversées en matière de protection légale des mesures techniques est celle du sort réservé aux limitations et exceptions du droit d'auteur et particulièrement la question de savoir s'il est admissible de contourner la protection technique pour exercer un acte non soumis à l'autorisation de l'auteur. Cette question des exceptions présente en réalité deux aspects. D'une part, faut-il tolérer la neutralisation des mesures techniques contrôlant l'accès et l'utilisation d'une œuvre tombée dans le domaine public ou dont l'usage est exempté sur le pied d'une exception légale? D'autre part, doit-on considérer comme illicites la fabrication et la commercialisation de systèmes de neutralisation ne visant qu'à la suppression des technologies apposées sur des éléments du domaine public ou permettant l'exercice d'exceptions?

- **l'existence d'exceptions à l'interdiction de neutralisation :** dans certains cas, la protection légale des systèmes techniques s'accompagne d'une série d'exceptions. Dans ce cas, l'acte de neutralisation et/ou la fabrication et distribution de dispositifs illicites échappent à la prohibition de principe.

- **l'existence d'une clause de *no mandate* :** certains systèmes exigent une reconnaissance par l'appareil de lecture, de téléchargement ou de reproduction. La protection est dans ce cas intégrée au support ou dans le code numérique de l'œuvre qui envoie un signal (*control flag*) à l'appareil pour l'empêcher d'accomplir certaines fonctions (copier, imprimer, accéder par ex.). L'industrie des équipements électroniques ou informatiques craint d'être tenue d'inclure dans ceux-ci des mécanismes permettant l'interaction avec ces signaux. L'industrie électronique plaide en conséquence pour l'insertion claire dans la loi d'une disposition qui les dispense d'adapter leurs produits aux mesures techniques. Une telle disposition est généralement qualifiée de clause de "*no mandate*".

---

17 Th. VINJE, *A brave new world of technical protection systems : Will there still be room for copyrigh?*, *EIPR*, 1996, n°8, p. 431.

1.2. Protection des mesures techniques dans l'Union européenne :

a) La directive sur la protection des programmes d'ordinateur et sa transposition dans les États membres

Le législateur européen s'est pour la première fois penché sur la protection légale des mesures techniques lors de la rédaction de la directive du 19 mai 1991 sur les logiciels. Son article 7 (1) (c) impose aux États membres d'incriminer les personnes qui "*mettent en circulation ou détiennent 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"*.[18]

Les mesures techniques ici protégées ne sont pas réellement définies dans le texte européen. Seuls sont visés de manière vague les dispositifs techniques protégeant les programmes d'ordinateur. On pourrait donc considérer que, lorsqu'ils sont appliqués aux logiciels, la plupart des systèmes que nous avons énumérés ci-dessus peuvent rentrer dans cette définition, qu'ils concernent la protection de l'accès ou la copie du programme.

L'acte de contournement lui-même n'est pas visé par cette disposition. Seules les activités dites préparatoires, en l'occurrence, dans ce texte, la mise en circulation et la détention à des fins commerciales, sont illicites. La mise en circulation peut se réaliser par la vente, l'offre au public, la location, etc.

Les appareils et systèmes dont la mise en circulation est prohibée sont *tout moyen* dont le *seul but* est de faciliter la suppression ou la neutralisation du dispositif technique. Ce critère est la fois large et assez restreint. D'une part, le terme "tout moyen", semble indiquer qu'un large éventail de mécanismes, logiciels, éléments d'un système et appareils soient visés. D'autre part, le critère du "seul but" réduit largement le champ des dispositifs considérés comme illicites. Par exemple, un logiciel poursuivant un but parfaitement licite mais permettant accessoirement de neutraliser la mesure technique ne sera pas couvert par l'interdiction, même s'il est clair que le succès de ce programme auprès des utilisateurs repose surtout sur cette fonction accessoire. Ce critère du but unique entraîne par conséquent l'exemption d'un grand nombre de systèmes de la prohibition.[19]

L'Allemagne a toutefois interprété ce critère très largement,[20] le seul but de l'application et non du programme dans son ensemble ayant été considéré comme suffisant pour interdire la distribution du logiciel permettant ainsi la neutralisation. En conséquence, cette interprétation large du texte permettrait de prohiber des programmes dont une application a pour seul but le contournement, même si le programme poursuit également d'autres objectifs.

Pour le reste, les transpositions dans les États membres de cette disposition s'écartent peu du texte de la directive. Par exemple, l'Allemagne a introduit dans sa loi sur le droit d'auteur une disposition interdisant les moyens qui facilitent le retrait ou le contournement non autorisés des mesures techniques protégeant les programmes.[21] La loi belge punit "*ceux*

---

18 Directive sur la protection juridique des programmes d'ordinateur du 14 mai 1991, J.O. L 122, 17.5.1991.

19 Th. VINJE, op. cit., p. 431.

20 A. RAUBENHEIMER, *Softwareschutz nach den Vorschriften des UWG*, *CR*, 1994, p. 264.

21 Sec. 69 f *Gesetz über Urheberrecht und verwandte Schutzrechte*.

qui mettent en circulation ou détiennent à des fins commerciales tout moyen ayant pour seul but de faciliter la suppression non autorisée ou la neutralisation des dispositifs techniques qui protègent le programme".[22]

La proposition de directive européenne sur le droit d'auteur dans la société de l'information, qui sera présentée ci-après, prévoit que la protection juridique qu'elle édicte n'affecte en aucune façon les dispositions spécifiques de protection prévues par la directive sur la protection juridique des programmes d'ordinateur. Toutefois, il serait illogique de conserver ce régime qui instaure une protection limitée aux dispositifs dont le seul but est la neutralisation des programmes d'ordinateur alors que la future directive sur le droit d'auteur introduira une protection plus large pour tous les autres types d'œuvres.

b) Proposition de directive sur le droit d'auteur et les droits voisins dans la société de l'information

L'article 6 de la proposition révisée de directive sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information[23] est rédigé comme suit :

"1. Les États membres prévoient une protection juridique appropriée contre la neutralisation non autorisée de toute mesure technique efficace destinée à protéger tout droit d'auteur ou droit voisin du droit d'auteur tel que prévu par la loi ou le droit sui generis, prévu au chapitre III de la directive 96/9/CE du Parlement européen et du Conseil [directive sur les bases de données] que la personne exécute en sachant ou en ayant des raisons valables de penser qu'elle poursuit cet objectif.

2. Les États membres prévoient une protection juridique appropriée contre les activités, y compris la fabrication ou la distribution de dispositifs, produits, éléments ou la prestation de services, non autorisées, qui :

a) font l'objet d'une promotion, d'une publicité ou d'une commercialisation dans le but de neutraliser la protection ou

b) n'ont qu'une raison commerciale ou qu'une utilisation limitée autre que de neutraliser la protection ou

c) sont principalement conçues, produites, adaptées ou réalisées en vue de permettre ou de faciliter la neutralisation de la protection

de mesures techniques efficaces destinées à protéger tout droit d'auteur ou droit voisin (...) ou le droit sui generis (...)".

---

22 Article 10 de la loi belge du 30 juin 1994 transposant en droit belge la directive européenne du 14 mai 1991.

23 Proposition modifiée de directive sur l'harmonisation du droit d'auteur et des droits voisins dans la société de l'information, COM(1999) 250 final du 21 mai 1999.

Actes prohibés

Le texte de la proposition de directive, après un détour par le Parlement européen, a décidé d'incriminer à la fois l'acte de contournement, ainsi que les activités préparatoires. La proposition initiale entretenait un certain flou sur ce point dans la mesure où "toutes les activités" étaient visées. A présent, l'article se subdivise en deux paragraphes distincts, l'un incriminant l'acte de neutralisation non autorisée, l'autre incriminant les activités de fabrication et de distribution de dispositifs non autorisés.

Objet de la protection

Qu'il s'agisse de la neutralisation ou de la distribution de dispositifs de neutralisation, les mesures techniques protégées sont définies comme "toute technique, dispositif ou élément qui, dans le cadre normal de leur fonctionnement, sont destinés à prévenir ou à empêcher la violation de tout droit d'auteur ou droit voisin (...) ou droit *sui generis* (...)". A première vue, cette définition ne couvrirait que les mesures établissant une protection directe des droits de l'auteur, telles que les systèmes anti-copie.

Toutefois, et suivant en cela les traités OMPI, les mesures techniques devront être efficaces pour pouvoir bénéficier de la protection. Le législateur européen a introduit une définition de ce critère d'efficacité : "*les mesures techniques ne sont réputées efficaces que lorsque l'accessibilité à l'œuvre ou son utilisation ou celle d'un autre objet protégé sont contrôlées grâce à l'application d'un code d'accès ou de tout autre type de procédé de protection qui atteint cet objectif de protection de manière opérationnelle et fiable avec l'autorisation des ayants droit. Ces mesures incluent le décryptage ou la désactivation de brouillage ou de toute autre transformation de l'œuvre*."

Cette définition de l'efficacité des mesures techniques appelle plusieurs commentaires. Tout d'abord, les critères de l'efficacité sont, soit le fait que l'accès à l'œuvre soit contrôlé techniquement, soit que son utilisation le soit. Or, l'accès à une œuvre ou à tout autre objet protégé n'est *a priori* pas en soi un acte soumis aux droits exclusifs de l'auteur ou du titulaire de droits voisins.

Le texte initial de la Commission limitait par ailleurs la définition de l'efficacité à l'accès.[24] L'intervention du Parlement européen a ajouté le critère de l'utilisation, ce qui permet de couvrir plus largement les actes accomplis par l'utilisateur, en ce compris les actes de reproduction et de communication au public soumis aux autorisations des titulaires de droit. Cette modification s'associe à l'alinéa premier qui insiste plus clairement sur le fait que la protection vise les mesures techniques protégeant tout droit d'auteur ou droit voisin. Ainsi, si sous l'empire de premier texte, on pouvait douter que les systèmes anti-copie bénéficiaient d'une protection, il nous semble à présent que la nouvelle définition permet d'établir plus facilement leur protection. Néanmoins, la protection finalement instaurée est étonnamment large puisqu'elle permet d'englober tous les actes effectués par l'utilisateur (allant de l'accès initial à l'œuvre à tous les actes ultérieurs d'utilisation). Nous reviendrons sur ce point dans la dernière partie de cette étude.

---

[24] S. DUSOLLIER, *Electrifying the Fence : The legal protection of technological measures for protecting copyright, E.I.P.R.*, 1999, n° 21/6, p. 285-297.

La définition précise en outre que les mesures techniques doivent avoir été appliquées à l'œuvre ou à l'objet protégé avec l'accord des titulaires de droit, qu'ils soient auteurs, artistes-interprètes, producteurs ou exploitants. Toutefois, l'étendue de cette autorisation n'est pas claire. L'exploitant qui souhaite sécuriser la distribution des œuvres par un système technique de protection devra-t-il obtenir l'autorisation de tous les titulaires de droit? Imaginons une médiathèque qui souhaite sécuriser les médias qu'elle loue ou prête avec l'autorisation des ayants droit ou la permission de la loi. Devra-t-elle obtenir une autorisation spécifique de chaque titulaire de droit? Si elle ne l'obtient pas, cela signifie-t-il qu'elle ne pourra poursuivre les personnes contournant la protection? De manière générale, cela implique-t-il que seules les technologies employées par les titulaires de droit seront protégées? Ce serait faire preuve d'une protection quelque peu incomplète dans la mesure où des œuvres sur certains réseaux de distribution licites, pourtant dûment protégées techniquement, pourraient dès lors être copiées et utilisées, en dépit de cette protection. Il faut toutefois signaler que dans ce cas, d'autres textes pourraient apporter une protection à ces systèmes tels que la directive sur l'accès conditionnel bien que nous verrons que, dans ce cas, l'acte de neutralisation ne sera pas en lui-même sanctionnable.

Enfin, il est précisé que les procédés de protection incluent le décryptage ou la désactivation de brouillage[25] ainsi que toute autre transformation de l'œuvre. La transformation de l'œuvre pourrait selon nous inclure les techniques de watermarking ou tatouage de l'œuvre qui pourtant, ainsi que nous l'avons vu plus haut, ne constituent qu'un mécanisme de protection indirecte de l'œuvre. Ces trois types de procédés ne sont cependant cités qu'à titre d'exemples, ce qui n'exclut pas que des systèmes tels les dongles ou autres systèmes empêchant la reproduction de l'œuvre soient également susceptibles d'être visés.

Type d'activités illicites et responsabilité

Nous avons vu que l'alinéa 1er de l'article 6 inclut désormais explicitement l'acte même de neutralisation des mesures techniques dans le champ des activités illicites. Dans ce cas, un élément moral a cependant été ajouté dans le but de ne poursuivre que les personnes qui ont effectué un tel contournement du mécanisme technique en connaissance de cause. Le texte parle de "*en sachant ou en ayant des raisons valables de penser qu'elle [la personne] poursuit cet objectif [la neutralisation non autorisée]"*. Il s'agit là d'une condition de connaissance qui n'apparaît pas dans l'infraction parallèle de fabrication d'appareils de neutralisation.

Dans le cas des activités préparatoires, le texte européen est très large puisqu'il vise de manière assez vague "les activités". La fabrication, la distribution de dispositifs illicites, ainsi que la prestation de services ne sont cités qu'à titre d'exemple. En conséquence, il nous semble que toute activité de commercialisation de ces dispositifs non autorisés est couverte. De même, il nous semble que les activités non commerciales d'offre de systèmes de contournement sont également visées. Ainsi, la distribution de clés de décryptage sur Internet, même dans un but non lucratif, à l'instar de ce qui se produit actuellement pour le décryptage de la protection technique du DVD, serait également considérée comme illicite.

---

[25] Ce qui montre bien ici que ce texte envisage principalement les systèmes de cryptage et d'accès.

Appareils illicites

L'illicéité des dispositifs et services est quant à elle conditionnée par trois critères alternatifs. Soit le système ou service fait l'objet d'une promotion, d'une publicité ou d'une commercialisation, dans le but de neutraliser la protection technique; soit la raison commerciale ou l'utilisation de tels dispositifs est principalement la neutralisation; ou enfin, le système ou service est principalement conçu, produit, adapté ou réalisé en vue de permettre ou de faciliter la neutralisation.

En quelque sorte, sont visés les services et dispositifs qui poursuivent clairement une fonction de neutralisation des mesures techniques afférentes, que celle-ci se révèle dès sa conception, par la publicité qui se réalise autour de ce produit, par sa fonction principale ou par l'utilisation qui en est faite.

Ici aussi, et cela est bien normal, la frontière entre systèmes licites et illicites restera floue et sujette à l'appréciation des tribunaux. A titre d'exemple, le logiciel de cryptage principalement utilisé pour décrypter des œuvres protégées sera interdit. Quant au magnétoscope, même si la fonction de neutralisation n'est qu'accessoire, le fait de promouvoir l'appareil dans ce but suffira à le rendre illicite.

Limites du droit d'auteur et protection.

Dans le texte révisé de la proposition, la Commission européenne réitère que les protections techniques doivent être établies dans le but de protéger un droit d'auteur ou droit voisin et donc dans les limites de ceux-ci.

En outre, un considérant énonce clairement que la neutralisation, pour être jugée illicite, ne doit pas avoir été autorisée par les ayants droit, ni permise par la loi.[26] Toutefois, ceci ne règle en rien le sort des actes de contournement effectués dans le but d'exercer une exception. Les systèmes techniques n'empêchent l'accomplissement des actes soumis au droit d'auteur (par ex. reproduction, communication, modification de l'œuvre) qu'en aveugle sans être capable de déterminer si l'acte empêché par la protection technique ressort de l'exercice légitime d'une exception. De plus, les mêmes mesures techniques protégeront de manière équivalente les œuvres protégées par le droit d'auteur et celles tombées dans le domaine public.

De plus, le considérant n° 30 ne détermine pas que le contournement est licite si effectué dans le cadre d'une exception. Il faudrait que le texte précise que l'acte de reproduction ou d'utilisation postérieur au contournement doit avoir été autorisé par l'auteur ou permis par la loi.

Seule la copie privée hérite d'un sort définitif, à la fois dans l'article 5, alinéa 2, b) *bis*, qui n'autorise la copie privée digitale qu'en cas d'absence de mesures techniques l'empêchant, et par le considérant 27 qui ajoute à ce premier principe que l'exception de copie privée ne peut justifier un acte de neutralisation non autorisé. En conséquence, contourner une protection anti-copie pour réaliser une copie privée d'une œuvre sera interdit.

---

[26] Considérant 30, *in fine*.

Le fait que la Commission n'ait pas, sur ce point, suivi les amendements du Parlement qui proposait de généraliser cette solution à l'ensemble des exceptions, pourrait indiquer que dans l'état actuel de ce texte, les autres exceptions ne s'effacent pas devant les protections techniques, voire que le contournement de celles-ci serait autorisé dans ce cadre.

Même si la Commission précise dans son exposé des motifs que cette question du rapport aux exceptions est réglée par le texte même de l'article 6 sur les mesures techniques, notamment à travers la définition de celles-ci laquelle requiert une violation du droit d'auteur, la question est loin d'être définitivement résolue.

Exceptions à l'interdiction de la neutralisation

Contrairement au texte américain, la proposition de directive n'énumère pas une série d'exceptions à l'interdiction de principe du contournement. Toutefois, les considérants de la directive nous apprennent que la protection ainsi instaurée ne pourra faire obstacle à la recherche sur la cryptographie,[27] ainsi qu'à la décompilation des logiciels autorisée par la directive de 1991 en la matière.[28] Resteront donc permis les actes de neutralisation des mesures techniques pour tester l'efficacité de l'algorithme de cryptage ainsi que le fait d'outrepasser une protection pour décompiler le logiciel. Dans ce dernier cas toutefois, il faudra que la décompilation s'effectue dans les conditions strictes posées par la directive sur la protection des programmes d'ordinateur, notamment le fait que la personne soit un utilisateur légitime du programme et que les informations nécessaires à l'inter-opérabilité ne soient pas disponibles d'une autre manière. Enfin, cette décompilation ne pourra s'exercer, de même que le contournement de la mesure technique effectué à cet effet, que dans le seul but d'arriver à l'inter-opérabilité du programme.

Clause de no mandate

Suite aux discussions au sein du Parlement européen, la proposition révisée intègre désormais une clause de no mandate dans ses considérants. Il est ainsi écrit au considérant 30 que la protection ne peut "*empêcher le fonctionnement normal des équipements électroniques et leur développement technique; qu'une telle protection juridique n'implique aucune obligation de mise en conformité des produits, composants ou services à ces mesures techniques*". L'objectif principal de la Commission est ici d'encourager les négociations entre les titulaires de droit et l'industrie électronique afin de parvenir à une intégration des mesures techniques dans les équipements électroniques et informatiques.

1.3. Protection des mesures techniques aux États-Unis :

a) Section 1002 du *Copyright Act* : la protection des *Serial Copy Management Systems*

Lors des premiers développements d'appareils permettant l'enregistrement et la copie de fichiers audio digitaux, communément appelés *Digital Audio Tape* ou DAT, l'industrie du

---

[27] Considérant 30bis, *in fine*.

[28] Considérant 31, *in fine*.

disque américaine et les titulaires de droit se sont émus que de tels systèmes puissent permettre des copies massives d'œuvres musicales sans aucune perte de qualité et à un moindre coût.

Une modification du *Copyright Act* a alors été adoptée pour imposer l'insertion dans les DAT d'un mécanisme anti-copie empêchant la réalisation de plus d'une copie digitale de l'œuvre (il s'agit des *Serial Copy Management Systems*). En l'espèce, l'industrie a été obligée de conformer sa production aux systèmes techniques alors en cours, et l'on a donc affaire à une disposition qui ne respecte pas la condition de *no mandate*.

Cette modification législative comprend également une interdiction d'importer, fabriquer, distribuer, offrir ou prester un service dont le premier effet ou but est de neutraliser la mesure technique anti-copie.[29] Il est utile de signaler que dans une décision récente,[30] un juge américain a estimé que ces dispositions étaient de stricte interprétation et ne pouvaient par conséquent être étendues à d'autres systèmes que les DAT. L'industrie phonographique essayait de contraindre les fabricants de lecteurs de fichiers MP3, tels la société Diamond, à insérer dans leurs appareils un système empêchant la copie des fichiers ainsi que la lecture de fichiers pirates.

b) *Digital Millenium Copyright Act*

En octobre 1998, le Congrès américain votait le *Digital Millenium Copyright Act*, long texte législatif révisant le *Copyright Act*. Conçue à la fois pour transposer les traités de l'OMPI et pour réaliser certains points de l'agenda numérique américain,[31] cette réforme législative traite de la protection des mesures techniques.

La nouvelle section 1201 du *Copyright Act* américain prévoit :

> *(a) VIOLATIONS REGARDING CIRCUMVENTION OF TECHNOLOGICAL MEASURES*
>
> > *(1) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.(...)*
> >
> > *(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that:*
> >
> > > *(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;*

---

29 Sec. 1002 (c) *: "No person shall import, manufacture, or distribute any device, or offer or perform any service, the primary purpose or effect of which is to avoid, bypass, remove, deactivate, or otherwise circumvent any program or circuit which implements, in whole or in part, a system described in subsection (a)."*

30 *RIAA v. Diamond Multimedia Systems, Inc.*, N° 98-56727 (9th Cir., juin 1999).

31 J. GINSBURG, *Chronique des États-Unis*, *R.I.D.A.*, janvier 1999, p.147 et suiv.

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(b) ADDITIONAL VIOLATIONS-

(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof that

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological protection measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

Une double protection est ainsi instaurée, l'une à l'égard des systèmes techniques qui contrôlent l'accès aux œuvres protégées, l'autre à l'égard des mesures techniques qui protègent effectivement un droit exclusif de l'auteur. En réalité trois infractions sont instaurées par le texte américain : (1) la *neutralisation des mesures techniques* de protection qui *contrôlent l'accès* aux œuvres protégées; (2) *la fabrication et diffusion* de mesures de dispositifs ou la *prestation de services* visant à neutraliser les systèmes de *contrôle d'accès*; et enfin, (3) la *fabrication et diffusion* de dispositifs ou la *prestation de services* permettant la neutralisation de *mesures techniques de protection des droits* des auteurs. Ces trois aspects méritent d'être traités séparément.

i) La protection des systèmes de contrôle d'accès

Objet de la protection

Les mesures technologiques visées sont celles qui "*dans le cadre normal de leur fonctionnement, requièrent l'application d'information, d'un procédé ou d'un traitement,*

avec l'autorisation des titulaires de droit, afin d'obtenir l'accès à l'œuvre".[32] Ceci implique certainement les mécanismes de cryptage, d'enveloppe digitale, de dongle, de mots clés.

L'objectif et la fonction principale des technologies dont il est question est de contrôler l'accès à une œuvre, non à un exemplaire ou une copie de l'œuvre.[33] En conséquence, seront protégés par cet article les mécanismes permettant de soumettre à l'autorisation du titulaire de droit, notamment contre paiement renouvelé, chaque nouvel accès ou nouvelle utilisation d'une œuvre sur un support licitement acquis (par exemple un logiciel sur CD ROM). Dès lors, l'utilisateur ne pourrait, sous peine de sanctions pénales, neutraliser la protection technique attachée à l'œuvre, même s'il a dûment payé en vue d'y avoir accès. Cette extension de la protection au-delà des droits traditionnels de l'auteur a déjà suscité des commentaires aux États-Unis.[34] Nous reviendrons dans la dernière partie sur cette controverse dont les termes et enjeux ne diffèrent pas substantiellement de la situation européenne que nous avons déjà esquissée plus haut.

Type d'activités illicites

Ces nouvelles dispositions sanctionnent tant la neutralisation de la mesure technique que la fabrication et la commercialisation de dispositifs neutralisant cette protection.

S'agissant de la neutralisation, le texte ne sera applicable qu'au terme d'une période de deux ans à dater de l'entrée en vigueur des nouvelles dispositions. Durant ces deux années, le *Register of Copyright* et le *Librarian of Congress* examineront dans quelle mesure cette interdiction du contournement des protections techniques est susceptible de porter préjudice aux utilisateurs d'œuvres protégées, ainsi qu'aux exceptions au droit d'auteur généralement admises au titre du *fair use*, telles que la citation, l'enseignement, la recherche, le compte rendu d'actualités, etc. Au terme de ces deux années, certains types d'œuvres pourront être exemptées de l'interdiction de neutralisation de systèmes d'accès les protégeant, afin d'en permettre une utilisation légitime. Ce serait le cas par exemple des articles scientifiques si l'on estimait que leur emploi fréquent dans la recherche nécessite que les utilisateurs puissent les consulter, même en dépit des protections techniques qui leur seraient attachées.

Ce processus d'évaluation de l'effet de la prohibition sera répété tous les deux ans.

L'autre branche de la protection des systèmes d'accès est, quant à elle, effective immédiatement. Elle vise la fabrication, l'importation, l'offre au public, la fourniture ou tout autre type de commercialisation de technologies, produits, services, appareils ou éléments illicites. Tant la prestation de services que l'offre de produits sont donc couverts.

---

32 Traduction non officielle de " *if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work*".

33 J. GINSBURG, op. cit., p. 159.

34 J. LITMAN, *New Copyright Paradigms*, http://www.msen.com/~litman/paradigm.htm; D. NIMMER, *Brains and other paraphernalia of the digital age*, *Harvard Journal of Law and Technology*, vol. 10, nr. 1, 1996, p. 1-46; J. GINSBURG, op. cit.

Par contre, aucun élément de connaissance ne vient conditionner la responsabilité ni de la personne qui commet un acte de neutralisation, ni de celle qui fabrique et distribue des dispositifs illicites.

Appareils illicites

Les produits ou services seront jugés illicites lorsqu'ils seront principalement conçus ou fabriqués dans le but de neutraliser une mesure technique, qu'il s'agisse d'un contrôle d'accès ou d'une protection d'un droit exclusif, lorsqu'ils n'ont qu'une raison commerciale ou une utilisation limitée autre que la neutralisation ou lorsqu'ils auront fait l'objet d'une promotion commerciale centrée autour de l'idée de neutralisation.

Exceptions à la prohibition de la neutralisation des systèmes d'accès et de la fabrication de dispositifs

Le texte américain ayant fait l'objet d'un intense lobbying de diverses industries et milieux intéressés, de l'industrie informatique et électronique aux bibliothèques, l'interdiction de principe de neutraliser les systèmes techniques de contrôle d'accès connaît certaines exceptions dont le régime est souvent complexe. Nous nous bornerons à en indiquer ici les principales :

- ***exception en faveur des bibliothèques sans but lucratif*** : le §1201 (d) prévoit une exception à l'interdiction de neutralisation au profit non seulement des bibliothèques, mais également au profit des archives et institutions d'éducation qui ne poursuivent pas un but lucratif. Cette exception est limitée à la possibilité de contrevenir à une protection technique dans le seul but de se renseigner sur l'intérêt d'une éventuelle acquisition de l'œuvre protégée. Encore faut-il en outre qu'une copie de cette œuvre ne soit pas autrement disponible et que la bibliothèque se débarrasse de l'exemplaire de l'œuvre à laquelle elle a accédé, une fois sa décision prise;

- ***exception pour les autorités et contrôles de sécurité*** : les autorités officielles ou de police qui contournent les protections techniques dans un but d'investigation ne seront pas soumis au régime de l'infraction. Cela va de soi, de même que l'exception dans le cadre de la vérification de sécurité d'un système effectuée avec l'autorisation du propriétaire du système ou réseau informatique;

- ***décompilation*** : à l'instar de la directive européenne sur la protection des logiciels, le droit américain reconnaît à l'utilisateur légitime d'une copie d'un programme la possibilité de procéder à la décompilation du programme afin d'en assurer l'inter-opérabilité. Or, les systèmes de contrôle d'accès pourraient anéantir de facto cette possibilité. En conséquence la loi prévoit une exception à la criminalisation de la neutralisation de telles mesures techniques dans ce cadre;

- ***activités de recherche en matière de cryptage*** : le § 1201 (g) introduit une stricte exception lorsque la neutralisation est nécessaire pour faire avancer la recherche en matière de cryptage, notamment en traquant et vérifiant les points faibles de la technologie. Dans le cadre de cette exception, la neutralisation des mesures

d'accès ainsi que le développement de dispositifs llicites sont exemptés;

- ***exceptions pour les mineurs*** : le législateur américain est très préoccupé par le fait que des mineurs d'âge puissent accéder à des contenus pornographiques ou violents sur Internet. L'industrie a dès lors développé de nombreux systèmes de filtrage, tels que les PICS,[35] pour répondre à ces inquiétudes. Lors des discussions du DMCA, il est apparu que ces systèmes pourraient contenir des composants aptes à neutraliser la protection technique d'accès, précisément pour vérifier la nature du contenu du site visité. Le § 1201 (h) prévoit que de tels systèmes ne pourraient être interdits de commercialisation pour ce seul motif;

- ***protection des données à caractère personnel*** : dans la mesure où la technologie d'accès ou le contenu ainsi protégé contient des données personnelles relatives à l'utilisateur – songeons aux *cookies* par exemple – ce dernier est habilité à contourner de telles mesures techniques afin de découvrir et d'effacer l'élément réunissant ces informations personnelles à l'insu de la personne concernée. L'exception est toutefois limitée à ce seul objectif et ne s'appliquera pas si l'opérateur du système technique informe l'utilisateur de la collecte de données.

Limites du droit d'auteur et protection

Le DMCA ne règle pas le statut des actes de contournement effectués pour exercer une exception permise dans le cadre du *fair use,* mais, comme on l'a déjà noté, le législateur a prévu une procédure d'évaluation de l'effet de la prohibition sur les exceptions et limites du copyright. Par ailleurs, l'éventuelle exemption de la protection pour certaines exceptions ne s'étendra qu'aux mesures techniques contrôlant l'accès et non aux mesures de protection des droits exclusifs. Toutefois, la neutralisation des mesures techniques n'étant pas interdite dans le cadre des protections des droits exclusifs, cette différence de régime n'a que peu d'incidence.

ii) La protection des mesures techniques protégeant les droits de l'auteur

Objet de la protection

L'alinéa (b) de la section 1201, dont le texte est cité plus haut, vise plus directement à transposer les traités OMPI dans la mesure où les mesures techniques ici considérées sont bien celles qui protègent les droits reconnus en vertu du droit d'auteur américain, soit les droits de reproduction, d'adaptation, de distribution, de représentation (*public performance)* ou présentation publique (*public display*) de l'œuvre. Dans ce cadre, la protection instaurée est unique et vise les fabricants et fournisseurs de dispositifs de neutralisation. L'acte de neutralisation lui-même n'est donc pas répréhensible, mais les actes postérieurement accomplis par l'utilisateur constitueront une atteinte au *copyright*. Sans doute a-t-on jugé que dans ce cas la justification d'une sanction supplémentaire ne se justifiait pas.

---

35 A. LIVORY, *CEE, contrôle du contenu circulant sur Internet : une approche particulière, le contrôle par l'usager et le système PICS, D.I.T.*, 06/1997, n° 97/2, pp. 52-54; Y. POULLET, *Quelques considérations sur le droit du cyberespace*, FUNDP, Faculté de droit, 1998, 27 p.

Les technologies visées sont celles qui protègent efficacement un droit reconnu au titulaire du droit d'auteur par le Copyright américain. Il s'agit notamment des SCMS et autres dispositifs anti-copie.

Les actes de commercialisation illicites sont identiques à ceux relatifs aux dispositifs de contrôle d'accès, soit la fabrication, l'importation, l'offre au public, la fourniture ou tout autre type de commercialisation de technologies, produits, services, appareils ou éléments illicites. Il en est de même pour la définition des dispositifs illicites qui s'applique *mutatis mutandis* aux deux types de technologie (d'accès et de protection des droits). Le critère essentiel est également la raison commerciale ou une utilisation limitée autre que la neutralisation.

Exceptions et mesures techniques de protection des droits

Le contournement n'étant pas interdit en lui-même, les utilisateurs pourront défaire la protection technique pour exercer un acte de *fair use*. D'autre part, rien n'indique qu'il soit autorisé de produire et distribuer des dispositifs de contournement dans le seul but d'outrepasser une protection pour utiliser une œuvre dans le cadre d'une exception.

Exceptions à la fabrication de dispositifs illicites

Seule l'exception pour les agissements de l'autorité et des services de police s'applique également dans le cadre des mesures techniques de protection des droits.

Clause de no mandate

Le DMCA prévoit que les industries électronique, de télécommunications et informatique ne devront pas adapter leurs produits de manière telle qu'ils puissent interagir avec les mesures techniques de protection ou de contrôle d'accès.[36]

1.4. Australie : *Copyright amendment* (*Digital Agenda*) Bill of 1999

Un projet de loi est également en cours en Australie dans un double objectif : adapter la loi australienne sur le copyright aux développements technologiques et transposer les Traités de l'OMPI. En matière de protection légale des mesures techniques, le projet énonce :

(5B) A person must not provide a circumvention service if the person knows, or is reckless as to whether, the service will be used to circumvent, or facilitate the circumvention of, an effective technological protection measure.

(5C) A person must not:
(a) make a circumvention device; or

(b) sell, let for hire, or by way of trade offer or expose for sale or hire, a circumvention device; or

[36] Art. 1201 (c) (3).

(c) distribute a circumvention device with the intention of trading, or engaging in any other activity that will affect prejudicially an owner of copyright; or

(d) by way of trade exhibit a circumvention device in public; or

(e) import a circumvention device into Australia with the intention of:

(i) selling, letting for hire, or by way of trade offering or exposing for sale or hire, the device; or

(ii) distributing the device for trading, or for engaging in any other activity that will affect prejudicially an owner of copyright; or

(iii) exhibiting the device in public by way of trade; or

(f) make a circumvention device available online to an extent that will affect prejudicially an owner of copyright;

if the person knows, or is reckless as to whether, the device will be used to circumvent, or facilitate the circumvention of, an effective technological protection measure.

Objet de la protection

Les mesures techniques efficaces qui font l'objet de cette protection sont définies comme "*a device or product, or a component incorporated into a process, that is designed to prevent or inhibit the infringement of copyright subsisting in a work or other subject-matter if, in the ordinary course of its operation access to the work or other subject matter protected by the measure is available solely by use of an access code or process (including decryption, unscrambling or other transformation of the work or other subject-matter) with the authority of the owner or licensee of the copyright in the work or other subject-matter*".

Ici aussi, l'élément clé de la définition est l'accès à l'œuvre et non la protection d'un droit spécifique de l'auteur. Contrairement au droit américain, voire au droit européen, aucune protection n'est prévue en parallèle pour les protections techniques empêchant la reproduction ou tout autre acte d'exploitation soumis au droit d'auteur. Se pose donc de nouveau la question de l'éventuelle application de ce texte aux systèmes anti-copie ou autres technologies dont la fonction première n'est pas la sécurisation et le contrôle de l'accès à l'œuvre.

Actes prohibés et appareils illicites

Seuls les actes préparatoires à la neutralisation seraient sanctionnés et non l'acte lui-même de contournement effectué par l'utilisateur. Au titre des actes préparatoires, seraient interdits la prestation de service de neutralisation, la fabrication, la vente, la location, l'exposition en vue de vente, la commercialisation, la distribution, l'importation ou la mise à disposition *on-line* d'un dispositif de neutralisation, ce dernier étant défini comme "*a device (including a computer program) having only a limited commercially significant purpose or use, or no such purpose or use, other than circumvention, or facilitating the circumvention of an effective technological measure*".

Le critère est similaire aux critères européen et américain.

Une condition supplémentaire de responsabilité est toutefois prévue dans la mesure où la personne en infraction devra avoir eu la connaissance de l'utilisation de l'appareil ou du dispositif à des fins de contournement.

Limites du droit d'auteur et exceptions

La proposition de loi australienne règle d'une manière inédite la délicate question du traitement des exceptions au droit d'auteur. Il est en effet prévu que la prohibition des actes de fabrication et distribution des dispositifs de contournement ou la prestation de service ne s'appliquera pas si la personne à laquelle est fourni ce service ou ce dispositif signe une déclaration selon laquelle elle s'engage à n'utiliser ceux-ci que dans un but permis par la loi, but qui doit également être expressément mentionné sur ladite déclaration. Le but permis par la loi est défini comme l'utilisation de l'appareil ou du service pour accomplir un acte relevant d'une exception au droit d'auteur ou effectué avec l'autorisation du titulaire du droit. Il nous semble que, dans ce cadre, une personne pourrait revendiquer l'usage d'un dispositif de neutralisation afin d'effectuer des actes hors du champ du droit d'auteur et par là même libérer le fournisseur de toute responsabilité à cet égard. On peut toutefois craindre qu'une telle déclaration ne devienne usage courant dans les contrats de fourniture de tels dispositifs électroniques rendant en conséquence la responsabilité des fabricants quasiment nulle.

En outre, en matière de fabrication et d'importation des mêmes dispositifs, aucune responsabilité du fabricant ou de l'importateur ne pourra être recherchée si leur utilisation se limite à un but permis par la loi.

Exceptions à l'interdiction de neutralisation

Outre l'exception générale prévue dans le cas où il s'agit de contourner la mesure technique pour exercer une exception au droit d'auteur, la proposition de loi prévoit une exception générale à l'interdiction pour les autorités ou services de police.

1.5. Autres pays

A notre connaissance, le Japon,[37] Singapour, la Hongrie et l'Irlande ont soit déjà transposé les Traités OMPI en matière de protection des mesures techniques ou s'apprêtent à le faire. Nous ne disposons toutefois pas des textes de ces États au moment où nous terminons ce rapport.

L'Allemagne avait également introduit un projet de loi dans le même but qui prévoyait de sanctionner la neutralisation, la suppression et la destruction des dispositifs et mesures techniques, en ce compris les programmes d'ordinateur, protégeant les droits des auteurs.[38] Ce projet paraît avoir été abandonné par le nouveau gouvernement allemand.

---

[37] Loi du 15 juin 1999.

[38] Proposition pour l'introduction d'un 5ème amendement à la loi allemande sur le droit d'auteur, du 7 juillet 1998, section 96a.

2. Protection des mesures techniques contrôlant l'accès à des services

Des législations situées hors du champ strict de la propriété intellectuelle apportent dans certains cas une protection aux systèmes techniques qui pourrait notamment être invoquée par les titulaires de droits pour protéger leurs œuvres, particulièrement pour en gérer l'accès.

L'objectif de ces dispositions est généralement de protéger les systèmes techniques empêchant et contrôlant l'accès à certains services. De telles dispositions autrefois prévues pour des services analogiques dans certains pays[39] pourraient être reprises et amplifiées pour le numérique et les services *on-line* en raison de la convergence de l'audiovisuel, de l'informatique et des télécommunications.

Nous nous limiterons à examiner une directive européenne qui nous paraît instaurer une protection supplémentaire des mesures techniques protégeant l'accès à des œuvres protégées. Il s'agit de la directive 98/84/CE du Parlement européen et du Conseil sur la protection juridique des services basés sur ou consistant en un accès conditionnel, directive datée du 20 novembre 1998.

L'objectif de la directive est de protéger les services dont l'accès est subordonné à certaines conditions, notamment au paiement d'une rémunération, ainsi que de sanctionner la commercialisation de mécanismes facilitant la neutralisation des systèmes d'accès conditionnel. Les services protégés sont notamment la radio et télévision, ainsi que les services de la société de l'information.

Ceci pourrait comprendre les services de vidéo ou d'audio sur demande, l'édition électronique, l'accès à une base de données *on-line*, un site de fichiers musicaux, etc. Par contre, les supports off-line dont l'accès serait régi par un système technique ne seront pas protégés sur base de ce texte.

Les titulaires de droit pourraient donc empêcher la commercialisation de dispositifs permettant le contournement des mesures d'accès auxquelles ils recourent. Il convient de préciser dès à présent que cette directive n'a pourtant pas pour objectif de protéger des contenus soumis à la propriété intellectuelle. La proposition initiale excluait d'ailleurs expressément les mesures techniques appliquées aux œuvres protégées par le droit d'auteur.[40] Dans sa version finale, la directive prévoit que son application se fera sans préjudice des dispositions communautaires en matière de propriété intellectuelle dans la directive sur le droit d'auteur dans la société de l'information (voir supra), ce qui ne suffit pas à lever toutes les questions sur le possible double emploi et sur l'articulation des deux textes et l'existence d'une double protection. Les deux directives visent en principe un objet différent : l'objet de la protection sera l'œuvre dans un cas, et un service dans l'autre, qu'il soit composé d'œuvres protégées ou non.

La directive accès conditionnel vise à protéger les services à accès conditionnel ainsi que les technologies qui garantissent et contrôlent cet accès. Dans la mesure où la proposition de directive sur le droit d'auteur définit les mesures techniques comme celles qui contrôlent

---

[39] En matière de cryptage des émissions de télévision, citons les articles 79-1 à 79-6 de la loi française du 30 septembre 1986 relative à la liberté de communication, les articles 297 à 299 de la loi anglaise sur le droit d'auteur, l'article 605 du *Communications Act* aux Etats-Unis.

[40] Considérant 15 de la proposition de directive.

l'accès aux œuvres, les deux textes sont susceptibles de protéger les mêmes technologies, ainsi que de sanctionner les mêmes types de systèmes pirates. Il faut bien se rendre à l'évidence que la grande majorité des services de la société de l'information comprendront des œuvres protégées par le droit d'auteur ou les droits voisins, ainsi que des bases de données protégées. Une base de données dont l'accès est sécurisé par une mesure technique constituera à la fois une œuvre (ou un objet protégé) et un service à accès conditionnel. La protection sera donc double.[41]

Le critère de la rémunération du service apparaît également comme essentiel à l'application de la directive sur l'accès conditionnel. Toutefois, ceci ne signifie pas que la rémunération doive être antérieure à la fourniture du service, ni être forfaitaire. Ainsi un service à accès conditionnel consistant en une collection on line de photographies, associé à un mécanisme de *metering*, pourrait être protégé, même si la facture comprenant un paiement en fonction de l'utilisation exacte de la photothèque est envoyée à intervalles réguliers après l'accès initial.

La directive sur l'accès conditionnel impose aux États membres d'interdire la fabrication, l'importation, la vente, la distribution, la location, la détention dans un but commercial, l'installation, la maintenance ou le remplacement d'un dispositif permettant l'accès non autorisé à un service protégé, ainsi que la promotion de tels dispositifs ou appareils. Le critère de l'illicéité des dispositifs d'accès non autorisé aux services protégés est plus strict que pour les mesures techniques en matière de droit d'auteur. Seuls les équipements ou logiciels conçus ou adaptés en vue de permettre cet accès seront prohibés.

Évidemment le fait que la protection des services à accès conditionnel soit étrangère aux droits d'auteur et droits voisins empêche que les exceptions et limitations du droit d'auteur puissent être invoquées pour défaire la protection technique. Ainsi, un service d'accès conditionnel comportant des œuvres du domaine public pourrait être protégé par un mécanisme de cryptographie. Les exploitants de ce service pourraient interdire la fabrication de clés de décryptage pirates, probablement pas sur base de la future directive sur le droit d'auteur, mais bien sur la base des transpositions de la directive accès conditionnel. Que les œuvres visées ne fassent plus l'objet d'une protection par le droit d'auteur importerait finalement assez peu.

En conséquence, les titulaires de droit auront parfois intérêt à invoquer ce texte afin d'empêcher la vente de systèmes de neutralisation : les exceptions et limites du droit d'auteur ne pourront lui être opposées. En outre, dans le cadre de la directive accès conditionnel, certaines activités telles que la maintenance, l'installation ou le remplacement d'un tel dispositif sont explicitement sanctionnés, ce que ne prévoit pas la proposition de directive sur le droit d'auteur.

---

41 S. DUSOLLIER *Electrifying the fence* …, op. cit., p. 290.

3. Dispositions en matière de criminalité informatique

L'accès non autorisé à des œuvres ou autres objets protégés peut dans certains cas être assimilé à une infraction portant atteinte aux systèmes informatiques. Ces infractions se retrouvent dans le Code pénal de nombreux pays au titre de la répression de la criminalité informatique, notamment suite aux inquiétudes qui ont vu le jour dans les années 80 face aux *hackers* et autres pirates de l'informatique.

Le Conseil de l'Europe préconisait de réprimer pénalement par des dispositions spécifiques une série d'agissements à l'encontre des systèmes et des données informatiques.

Cette liste comportait notamment les agissements suivants :

- la fraude informatique, définie comme "*l'entrée, l'altération, l'effacement ou la suppression de données ou de programmes informatiques, ou toute autre ingérence dans un traitement informatique, qui en influence le résultat en causant par là-même un préjudice économique ou matériel à une autre personne dans l'intention d'obtenir un avantage économique illégitime pour soi-même ou pour autrui ou dans l'intention de priver illicitement cette personne de son patrimoine*";

- le faux en informatique, qui consiste en l'infraction traditionnelle du faux par le biais d'une ingérence dans un système informatique;

- les dommages affectant les données ou les programmes qui consistent en *l'effacement, l'endommagement, la détérioration ou la suppression sans droit de données ou de programmes informatiques*, dont le cas le plus répandu est bien entendu le virus ou autres bombes informatiques;

- le sabotage informatique, que constitue l'entrée ou l'ingérence dans des systèmes informatiques dans l'intention d'en entraver le fonctionnement;

- l'accès non autorisé à des systèmes informatiques qui se réalise par la violation des règles de sécurité;

- l'interception non autorisée de communications informatiques;

- la reproduction non autorisée de programmes d'ordinateur ou de topographies;

- l'altération sans droit de données ou de programmes d'ordinateur;

- l'espionnage informatique;

- l'utilisation non autorisée d'un ordinateur, d'un système ou d'un réseau informatique, dont la criminalisation n'est suggérée que dans certains cas;

- l'utilisation sans droit d'un programme informatique.

Si certaines de ces infractions sont totalement étrangères à l'hypothèse de la protection technique des œuvres, d'autres pourraient servir, à titre subsidiaire, de base à une action contre des actes de neutralisation de la barrière technologique.

Par exemple, une personne qui contreviendrait au système de cryptographie qui sécurise l'accès à une base de données d'œuvres protégées pourrait être poursuivie pour fraude informatique (le préjudice causé aux titulaires de droit par l'entrée dans son système consistant en la perte de la rémunération leur étant due, l'intention frauduleuse devant toutefois être prouvée), ainsi que sur base de l'infraction résultant d'un accès non autorisé à la base de données.

La neutralisation d'un mécanisme de watermarking prévenant la modification de l'œuvre pourrait également être réprimée sur pied de l'infraction d'altération non autorisée des données. Enfin, le contournement d'une mesure technique sécurisant l'accès et l'utilisation d'un programme informatique fonderait l'infraction d'utilisation non autorisée d'un programme informatique. Toutefois, cette infraction particulière a généralement été incluse par les législateurs nationaux dans le cadre de la protection juridique des logiciels et non dans les textes pénaux spécifiques à la criminalité informatique.

Les pays ayant suivi les recommandations du Conseil de l'Europe ont majoritairement introduit dans leur arsenal répressif une infraction d'intrusion non autorisée et une infraction pour l'altération des données. En matière d'accès non autorisé, citons l'article 321-1, alinéa 1er du Code pénal français qui réprime l'accès et le maintien frauduleux dans un système informatique, l'article 202a du Code pénal allemand qui interdit l'obtention de données spécialement sécurisées contre l'accès non autorisé. La Norvège[42] et la Finlande exigent également une violation des règles de sécurité. Par contre, la loi fédérale américaine[43] en la matière requiert en sus de l'accès illicite, l'obtention, la modification ou la destruction d'informations.

L'élément de maintien indu se retrouvant dans la législation française permettrait notamment de couvrir la neutralisation des mesures techniques relatives à l'utilisation des œuvres protégées même si l'accès lui-même a été autorisé par le titulaire du droit. Ainsi imaginons une personne qui souscrit un abonnement à un service de vidéo à la demande dont chaque utilisation lui est facturée par la suite. Elle parvient à neutraliser les mesures techniques qui enregistrent et facturent ces utilisations. Il nous semble que rien ne pourrait empêcher qu'on considère que ces utilisations hors du système technique constituent un maintien indu dans le système de traitement des données punissable par la loi française.

Quant à l'altération des données, notamment en défaisant le marquage numérique de l'œuvre, il s'agira d'un délit en vertu de l'article 303a du Code pénal allemand, ainsi qu'en vertu de l'article 323-3 du Code pénal français.

---

42 Article 145 du Code pénal norvégien.

43 *Federal counterfeit access device and computer fraud and abuse Act of 1984*, USC title 18, chapter 47, § 1030.

C. CONSIDERATIONS FINALES

Depuis l'adoption des Traités de l'OMPI il y a trois ans, quelques pays ont transposé les règles en matière de protection juridique des mesures technologiques ou s'apprêtent du moins à le faire. Ceci démontre à suffisance combien cette protection nouvelle se révélait nécessaire.

En outre, nous avons pu constater que malgré certaines divergences dans l'étendue et les conditions de la protection, les dispositions nationales ou régionales s'accordent sur les éléments essentiels d'une protection adéquate, tels que la définition de l'objet de la protection, la délimitation des actes illicites (à la fois l'acte de neutralisation et la mise à disposition de mécanismes de contournement), ainsi que la définition de l'illicéité de ces mécanismes (respectivement les points 1.1, 1.2 et 1.3 ci-après).

Un certain nombre de questions restent cependant ouvertes, la plus délicate étant certainement l'existence d'un possible conflit entre la protection juridique de la mesure technique et les exceptions et limitations aux droits de l'auteur (point 2 ci-après).

1. Éléments d'une protection adéquate et efficace

1.1. Quant à l'objet de la protection

La définition des mesures techniques dont la neutralisation devrait être interdite a été laissée à l'appréciation des États transposant les Traités de l'OMPI. La seule indication était que ces mesures avaient pour but et fonction de protéger les droits reconnus à l'auteur ou à tout autre titulaire de droits. Il s'agissait donc à première vue de protéger principalement les techniques empêchant la reproduction ou la communication au public d'œuvres ou de prestations protégées. Or, les États ou organisations régionales, telles que l'Union européenne, ont généralement introduit ou adopté des textes dont l'objet n'était pas seulement les technologies protégeant strictement les droits d'auteur, mais également les technologies conditionnant et contrôlant l'accès aux œuvres. Cela est manifeste dans les textes américain et australien; cela ressort également de la définition des mesures techniques reprise dans la proposition communautaire.

En conséquence, la protection technique de l'accès à une œuvre devient protégée dans la mesure où son contournement est interdit, ce qui instaure une protection *de facto* de l'accès à l'œuvre, dont le contrôle deviendrait ainsi une prérogative du titulaire de droit sans que celle-ci soit pourtant prévue par la loi . Il est vrai qu'une grande majorité des systèmes techniques actuellement utilisés pour protéger des œuvres sont des mesures basées sur la cryptographie qui à titre principal empêchent un accès non autorisé au contenu crypté. Le simple accès à une œuvre qui aurait nécessité le déplombage d'une barrière technique, sans toutefois qu'un acte soumis au droit de l'auteur n'ait été accompli postérieurement à l'accès, tomberait sous le coup de la sanction.

Cette extension indique à suffisance combien l'accès à une œuvre est essentiel pour les titulaires de droit. Jane Ginsburg écrivait notamment que "*access probably will become the most important right regarding digitally expressed works, and its recognition, whether by the detour of prohibitions on circumvention of access controls, or by express addition to the list*

of exclusive rights under copyright, may be inevitable".[44] Ceci entraîne néanmoins une certaine confusion dans les transpositions des Traités OMPI à cet égard et dans certains cas une protection hybride où la limite entre la protection des droits et la protection de l'accès aux œuvres devient floue. Cette protection des systèmes de contrôle d'accès semble en tout cas outrepasser l'étendue des dispositions des Traités de l'OMPI.

Le souci de protéger les technologies relatives à l'accès se comprend parfaitement. Toutefois, il relève davantage de la protection de l'accès au service contenant les œuvres et surtout de la protection de la rémunération du service. Il s'agit donc davantage d'une préoccupation de l'exploitant ou du distributeur des œuvres que d'une protection directe des ayants droit. L'intérêt protégé à travers la protection légale des mesures techniques est lié à la distribution des œuvres sur les réseaux. Cet intérêt mérite certes une protection, telle que par exemple celle de la directive européenne sur l'accès conditionnel. Mais il faut reconnaître que cette protection ne peut plus exclusivement se justifier par des considérations liées à la propriété intellectuelle. Ce déplacement de la raison d'être de la protection technique et juridique devrait, à tout le moins, faire l'objet d'une réflexion plus approfondie.

1.2. Quant aux types d'actes illicites

Si les Traités de l'OMPI ne visent à première vue que l'acte de contournement même des mesures techniques de protection, les dispositions nationales que nous avons abordées ont unanimement complété l'interdiction de la neutralisation par une prohibition générale de la fabrication et de la distribution de dispositifs permettant ou facilitant une telle neutralisation. Il paraît en effet évident qu'une diffusion à large échelle de mécanismes permettant de défaire les protections techniques causera un préjudice plus grand pour les titulaires de droits que des actes de neutralisation isolés. Dans certains cas, la protection ainsi instaurée par les pays se limite d'ailleurs à cette incrimination des actes dits préparatoires, à l'exclusion des activités de contournement elles-mêmes. C'est notamment le cas en Australie et aux États-Unis en ce qui concerne les mesures techniques protégeant les droits des auteurs.

D'autre part, on peut regretter que la plupart des textes ne soient pas plus clairs sur les activités de distribution des dispositifs de neutralisation. Ainsi, l'offre sur un site web de tels systèmes n'est pas explicitement visée, de même que la mise à disposition gratuite et sans but lucratif de systèmes de déverrouillage. Dans la plupart des cas où des pirates ont "craqué" la protection technique, ils ont en effet communiqué leurs astuces en quelques heures par le biais d'Internet sans poursuivre le moindre but lucratif. Toutefois, la protection instaurée aux États-Unis et en Europe paraît être suffisamment large pour englober les actes de distribution autres que ceux effectués dans le cadre d'une commercialisation.

1.3. Quant au type d'appareils illicites

La question de savoir à partir de quel moment un appareil permettant la neutralisation de mesures techniques devient illicite, est difficile à déterminer. Il faut certainement tenir compte des intérêts de l'industrie électronique et informatique qui souhaiterait ne pas voir certains des appareils qu'elle développe interdits au seul motif que certains utilisateurs en usent pour défaire la protection technique. L'équilibre est difficile à définir. Nous avons vu

---

[44] J. GINSBURG, op. cit., p. 171.

que la plupart des dispositions existantes se réfèrent au critère de la raison commerciale ou de l'utilisation limitée. Les appareils interdits seront ceux qui n'ont qu'une raison commerciale ou une utilisation limitée autre que de neutraliser la protection, ce qui laisse une marge de manœuvre raisonnable aux juges qui devront mettre en œuvre ces dispositions. La promotion et la commercialisation de dispositifs dans un but explicite de neutralisation sont bien entendus également visées. En conclusion, la limite ainsi dressée entre dispositifs licites et illicites repose de manière logique sur l'évidence du but du dispositif ainsi conçu, produit, promu ou vendu.

Bien sûr, les contours de ce critère sont encore sujets à de multiples interprétations qu'il reviendra à la jurisprudence d'éclaircir. Il est toutefois important de souligner l'intérêt de définir l'illicéité des dispositifs de contournement de manière identique dans de nombreux pays.

2. Limitations du droit d'auteur et exceptions

La question de l'interférence des exceptions et limitations au droit d'auteur et de la protection juridique des mesures techniques constitue un des points les plus complexes de la matière. Il est évident qu'une mesure technique peut par définition en verrouillant l'accès à une œuvre ou en empêchant l'accomplissement d'un acte soumis à l'autorisation de l'auteur restreindre fortement la capacité de l'utilisateur à effectuer des actes permis en vertu d'une exception légale. Si, suite à l'usage d'une protection technique, l'utilisateur n'est plus capable de citer l'œuvre, d'en faire une copie privée, de l'utiliser dans un but d'éducation ou d'information, la portée de ces exceptions dans le monde numérique risque de se réduire énormément.

Dans le cadre de la protection des mesures techniques, la question se pose d'une double manière. Puisque les États ont généralement instauré une double protection des mesures techniques, à la fois à l'égard de la neutralisation et de la mise à disposition de mécanismes illicites, l'incidence des exceptions doit être envisagée pour les deux branches de cette protection.

D'une part, on peut se demander si l'acte de neutralisation de la mesure technique est également interdit s'il est accompli pour avoir accès à une œuvre non protégée ou pour accomplir des actes couverts par une exception.

D'autre part, certains fabricants ou distributeurs de systèmes permettant la neutralisation des mesures techniques sont parfois tentés d'invoquer le fait que leurs appareils ne poursuivent qu'un but parfaitement licite, notamment de permettre aux utilisateurs de contourner la barrière technique afin d'avoir accès à des œuvres du domaine public. Nous commencerons par l'analyse de cette deuxième branche de la question avant d'affronter celle, plus périlleuse, du sort des exceptions face à l'interdiction de l'acte de neutralisation.

2.1. Exceptions et fabrication de dispositifs de contournement

En ce qui concerne l'interdiction des actes dits préparatoires à un acte de contournement, l'enjeu des exceptions se résume à la question de l'éventuelle tolérance à l'égard de systèmes qui ne permettent la neutralisation que dans le but d'accéder à des contenus non protégés ou dans le but d'exercer une exception permise par la loi.

Si les mesures techniques de protection portent indifféremment sur les œuvres protégées et celles qui sont libres de droits, les dispositifs censés les neutraliser le feront également de manière indifférenciée. On peut difficilement imaginer qu'un dispositif ne soit conçu que dans le but de réaliser des copies privées ou des copies d'une œuvre non protégée. Il est évident que les mêmes systèmes permettront la neutralisation des mécanismes de protection dans des buts illégitimes. En outre, autoriser la mise en circulation de systèmes uniquement utilisés dans des buts légitimes permettrait à leurs fabricants de se dégager systématiquement de toute responsabilité.

La réponse nous semble donc relativement simple. Les concepteurs et distributeurs de dispositifs qui permettent de contourner les œuvres protégées, même si leur utilisation est susceptible de ne se limiter qu'au déverrouillage de l'accès aux œuvres non protégées, ne pourraient pas échapper à l'interdiction sur cette seule base. Rien n'empêche toutefois ces concepteurs de négocier avec les titulaires de droit l'autorisation de systèmes relatifs à des déverrouillages spécifiques, par exemple pour des contrôles de sécurité ou à l'avantage des bibliothèques qui souhaiteraient, là où la loi le leur permet, réaliser une copie de sauvegarde ou d'archivage.

2.2. Exceptions et acte de neutralisation

L'utilisateur qui souhaiterait exercer une exception sera parfois forcé de déverrouiller la protection technique qui l'en empêcherait. Si l'on estime que ce type de contournement est illicite, l'utilisateur sera sanctionné alors même qu'il se trouve hors du droit d'auteur et ne peut être poursuivi à ce titre. Cela tendrait à démontrer que l'objet de la protection est plus la technique elle-même, au titre de l'investissement dans la fabrication et dans l'utilisation de celle-ci, que le droit d'auteur. Si, au contraire, ce contournement est considéré comme licite, l'utilisateur ne sera poursuivi ni pour violation droit d'auteur, ni pour violation de la protection de la mesure technique, ce qui pose alors la question de la détermination du but poursuivi par l'utilisateur lors du contournement. En effet, comment pourrait-on démontrer qu'une neutralisation de la technologie protectrice n'a été effectuée que pour exercer une exception?

La solution souvent proposée à cette problématique est de donner aux exceptions un caractère impératif auquel ni les contrats ni les mesures techniques ne pourraient déroger.[45]

Cette solution n'est pourtant qu'imparfaite. La technologie en effet est aveugle et ne réagit qu'aux demandes d'actes techniques telles qu'une copie, une impression, un envoi, une lecture, un accès. Elle ne peut reconnaître le cadre dans lequel se réalise cet acte. Les conditions souvent subjectives posées à l'exercice d'une exception ne peuvent être analysées et reconnues par de telles mesures techniques. Un exemple en est le caractère impératif accordé par la directive européenne sur les bases de données à l'exception permettant à l'utilisateur légitime d'effectuer les actes nécessaires à une utilisation normale. Comment la mesure technique protégeant la base de données pourrait-elle déterminer ce qu'est une utilisation normale?

---

[45] B. HUGENHOLTZ, *Rights, Limitations and Exceptions: Striking a Proper Balance*, Keynote Speech at the Imprimatur Consensus Forum, 30/31 October 1997, Amsterdam; L. GUIBAULT, *Contracts and Copyright Exemptions*, Amsterdam, Institute for Information Law, 1997.

De même une exception également impérative est reconnue à l'utilisateur d'une base de données protégée par un droit *sui generis* pour extraire des parties non substantielles. Le système protégeant la base ne pourrait définir ce qu'est une partie non substantielle à moins d'être programmé à cet effet par le titulaire de droit, ce qui enlèverait une partie de son sens à l'exception.

Une autre solution peut être trouvée dans le cadre des relations contractuelles entre les titulaires de droit et les utilisateurs. Les auteurs pourraient soit fournir à certains types d'utilisateurs ayant légitimement acquis l'œuvre une copie de celle-ci dépourvue des protections techniques ou fourniraient une copie dont la protection technique tiendrait compte du type d'exceptions particulier que cet utilisateur est habilité à exercer. Cette solution ne concernerait toutefois que de grandes catégories d'utilisateurs, tels les bibliothèques, les journalistes, les chercheurs, les enseignants, auxquels sont associés certaines exceptions déterminées. Ces mêmes utilisateurs pourraient bénéficier d'une sorte de présomption les exemptant de l'interdiction, présomption devant être renversée par les titulaires de droit au cas où ces utilisateurs ont neutralisé la protection technique en dehors du cadre de la limitation du droit d'auteur dont ils bénéficient généralement. Toutefois, ces différentes alternatives pénaliseraient les utilisateurs individuels qui ne se verraient pas reconnaître une telle possibilité. Le système des exceptions ne deviendrait plus qu'une affaire de négociation contractuelle entre les ayants droit et quelques utilisateurs qu'on pourrait appeler collectifs.

Ces solutions peuvent néanmoins servir de pistes à une réflexion sur cette question particulièrement délicate des exceptions.

[Fin du document]