Vol. 15, nº 2

Mesures de protection technique

Partie I – Tendances en matière de mesures de protection technique et de technologies de contournement

Ian Kerr, Alana Maurushat et Christian S. Tacit*

* Ian Kerr, Ph.D., conseiller spécial, Droit des technologies, Nelligan O'Brien Payne LLP; titulaire d'une chaire canadienne de recherche en déontologie, droit et technologies, Faculté de droit, Université d'Ottawa; Alana Maurushat, suppléante, LL.M. (avec concentration en droit et technologies), Faculté de droit, Université d'Ottawa, stagiaire chez Nelligan O'Brien Payne LLP; M. Christian S. Tacit, associé de Nelligan O'Brien Payne LLP et chef du groupe des Pratiques du droit des technologies du cabinet conseil. Les auteurs sont grandement reconnaissants à l'endroit de Loris Mirella pour ses précieuses observations et suggestions. Ils souhaitent également remercier Andrew Huzar, Steven Pink, Tracey Ross, Shannon Ross, Christopher Rootham, Erin Smith et Wing Yan pour leur apport à une version antérieure du présent document. Financée par le ministère du Patrimoine canadien (PCH), cette étude reflète les opinions des auteurs. Elle ne représente pas nécessairement les politiques ni les perspectives du PCH ou du Gouvernement du Canada. Traduction de Luc Larivière.

1.0 INTRODUCTION

Le présent document constitue le premier de deux rapports d'étude indissociables préparés pour le compte de la Direction générale de la politique du droit d'auteur du ministère du Patrimoine canadien par le cabinet d'avocats Nelligan O'Brien Payne LLP. Ces études abordent toute une gamme de questions de politiques relatives à l'utilisation des mesures de protection technique (MPT) comme outils d'application des règles du droit d'auteur dans des environnements numériques. Les études passent également en revue les divers scénarios de politiques compris dans la décision de fournir une protection juridique aux MPT dans le contexte de la *Loi sur le droit d'auteur* au Canada[1].

Dans cette première étude, nous mettons l'accent sur les techniques réelles utilisées pour protéger les droits d'auteur en offrant des descriptions technologiques des diverses MPT, ainsi qu'une énumération de leurs fonctions actuelles et éventuelles. L'objectif est de clarifier la compréhension de l'essence même des MPT, de leurs modalités d'utilisation et des considérations liées à leur contournement. Cette première étude est un préalable absolu à la seconde étude, qui fournira à la lumière des politiques sur le droit d'auteur une analyse de l'utilisation et de la protection juridique des MPT dans le contexte de la décision du Canada quant à la mise en application ou non et les modalités de mise en œuvre du *Traité de l'OMPI sur le droit d'auteur* (WCT)[2] et du *Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes* (WPPT)[3].

Pour faire suite à certains aspects contextuels élémentaires et à quelques concepts clés présentés dans la Partie 2 de la présente

1. L'étude d'accompagnement (c'est-à-dire la seconde étude) s'intitule «Mesures de protection technique: Partie II – Protection juridique des MPT».
2. *Traité de l'OMPI sur le droit d'auteur*, 20 déc. 1996, en ligne (français): <http://www.wipo.int/clea/docs/fr/wo/wo033fr.htm>. Le WCT est entré en vigueur par suite du dépôt de la 30e ratification le 6 mars 2002.
3. *Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes*, 20 déc. 1996, en ligne (en français): <http://www.wipo.int/clea/docs/fr/wo/wo034fr. htm>. Ce traité est entré en vigueur le 20 mai 2002.

étude, la Partie 3 passe en revue certaines tendances récentes en matière d'élaboration de MPT. Dans la Partie 4, nous amorçons notre enquête des mécanismes de contournement des MPT. L'objet de cette enquête est ensuite passé à la loupe dans la Partie 5 au moyen d'un examen des systèmes de gestion des droits numériques (SGDN) à grande échelle[4]. Enfin, dans la Partie 6, nous nous attarderons brièvement à l'avenir des MPT en vue de bien situer le débat de politiques présent dans la seconde étude.

2.0 CONTEXTE

L'intensification de notre capacité de copier et de diffuser l'information par voie électronique a été motivée par un matériel micro-informatique peu coûteux et hyper puissant, jumelé à un accès élargi à la réseautique. Par conséquent, il est possible d'encoder divers types de renseignements en format numérique, de dupliquer le contenu numérisé sans perte de fidélité et de transmettre le tout à un nombre incroyable de destinataires partout dans le monde à un coût différentiel négligeable. Ce nouvel environnement offre de nombreuses nouvelles occasions pour la diffusion rapide et peu coûteuse du contenu numérisé. Cela soulève aussi des défis particuliers pour ce qui est de l'application à la fois des droits de propriété intellectuelle (notamment les droits d'auteur) et les autres droits (tels que les droits contractuels) sur divers types d'œuvres numérisées. Ainsi, les titulaires de droits sur le contenu numérisé se tournent de plus en plus vers l'utilisation des MPT pour faire appliquer et protéger leurs droits et pour faciliter la diffusion de leurs œuvres.

Dans sa plus simple expression, une MPT est une méthode technologique visant à promouvoir l'utilisation autorisée des œuvres numérisées. Cela est rendu possible grâce à un contrôle de l'accès à pareilles œuvres ou aux diverses utilisations de telles œuvres, y compris: i) la copie; ii) la distribution; iii) l'exécution publique; et iv) l'affichage[5]. Les MPT peuvent servir de garde-fou ou de «barrières virtuelles» entourant le contenu numérisé, que le contenu bénéficie ou non d'une protection en vertu des règles du droit d'auteur[6]. Deux

4. Les systèmes de gestion des droits numériques (SGDN) sont également qualifiés de systèmes de gestion des droits électroniques (SGDÉ), de systèmes d'information sur la gestion des droits (SIGD) et de systèmes de gestion des droits d'auteur (SGDA).
5. M. PERRY et C. CHISICK, «Copyright and Anti-circumvention: Growing Pains in a Digital Millennium», (2000) *New Zealand Int. Prop. J.* 261.
6. Des auteurs, y compris E. Mackaay, ont utilisé la métaphore de la barrière numérique pour illustrer comment la propriété intangible peut être protégée. Les

exemples courants de MPT sont: i) les mots de passe; et ii) les techniques de cryptographie.

Les MPT procurent aux titulaires de droits d'auteur un outil de contrôle des utilisations ultérieures des œuvres numérisées d'une manière qui n'était pas possible dans le cas des œuvres intégrées sous d'autres formes. Par exemple, dès qu'une personne achète un livre en format de poche, le titulaire du droit d'auteur n'a aucun moyen de contrôler combien de fois l'acheteur lira ce livre, ou si la personne le prêtera à une autre personne ou en photocopiera des passages. Cependant, les MPT permettent à un titulaire de droits d'auteur d'effectuer toutes ces opérations dans le cas des livres électroniques et d'autres versions numériques de l'œuvre publiée[7].

La tentative de fournir une description simple des MPT a été complexifiée par l'introduction de systèmes d'information plus perfectionnés conçus pour protéger la propriété intellectuelle. Ces systèmes ont été baptisés «systèmes de gestion des droits numériques» (SGDN). Certains SGDN intègrent des mesures techniques dans le cadre de leur infrastructure, tandis que d'autres présentent des caractéristiques qui s'apparentent à une forme plus avancée de MPT. Un auteur a défini les SGDN comme «des systèmes techniques facilitant la gestion fiable et dynamique des droits quel qu'en soit le format d'information numérique, tout au long de son cycle chronologique, et peu importe le mode et le lieu de distribution de cette information numérisée» [Traduction libre][8]. D'ordinaire, un SGDN

techniques d'installation de barrières telles que les MPT ou les accords contractuels offrent aux titulaires de droits la capacité de contrôler l'accès à l'utilisation de leurs œuvres et, dans certains cas, de contrôler l'utilisation même de ces œuvres. Pareille métaphore repose sur la notion énoncée par R. Ellickson, qui discutait de la façon dont l'avènement du barbelé permettait l'utilisation de lots réduits pour l'élevage du bétail, changeant du même coup les règles économiques de pareille utilisation du territoire. Voir E. MACKAAY, «Intellectual Property and the Internet: The Share of Sharing», dans N. NETANEL, N. ELKIN-KOREN et V. BOUGANIM (éd.), *The Commodification of Information,* La Haye: Kluwer Law International, 2001. Voir aussi R. ELLICKSON, «Property in Land», (1993) 102 *Y. L.J.* 1315.

7. D. BURK et J. COHEN, «Fair Use Infrastructure for Rights Management Systems», (2001) 15 *Harv. J.L. et Tech.* 41, 48. Les auteurs notent que les MPT, utilisées de pair avec d'autres protections juridiques, «permettront de contrôler, de surveiller et de mesurer presque toute utilisation imaginable d'une œuvre numérique» [Traduction libre].
8. N. GARNETT, «Outline of Presentation of Nic Garnett, representing InterTrust Technologies», Congrès ALAI 2001, p. 1. On y trouve une définition plutôt vaste des SGDN puisque, comme le souligne l'auteur, «le terme SGDN est désormais appliqué à toute une gamme de différentes technologies, dont la plupart ont trait au contrôle de l'accès à l'information ou à sa copie» [Traduction libre].

comprend deux composantes: i) une base de données contenant de l'information qui précise le contenu d'une œuvre et ses titulaires de droits; et ii) un accord de licence qui stipule les modalités d'utilisation de l'œuvre sous-jacente[9]. Les SGDN permettent l'échange de données sur l'utilisation parmi les titulaires de droits et les distributeurs, et établissent la manière dont une œuvre pourra être utilisée. Pour reprendre l'exemple du livre électronique mentionné ci-dessus, un SGDN pourrait être utilisé pour promouvoir l'utilisation autorisée d'une œuvre en restreignant la capacité de copier une œuvre numérisée, en limitant sa transmission à d'autres utilisateurs, son transfert à des machines autres que celle visée par la licence d'exploitation, et même le nombre de fois que l'œuvre pourra être consultée[10]. Au cours de son exploitation usuelle, un SGDN pourra même servir à assurer un suivi des utilisations des œuvres. Par conséquent, un SGDN peut être utilisé non seulement pour restreindre une utilisation non autorisée, mais également pour permettre une utilisation conformément aux règles énoncées dans les modalités et conditions afférentes à ce SGDN[11]. Les SGDN pourront également servir à autoriser les droits, à faciliter le paiement des redevances en contrepartie de l'utilisation des œuvres, et à dépister et faciliter la poursuite des utilisations non autorisées et des utilisateurs non autorisés des œuvres assujetties aux règles du droit d'auteur[12]. Afin d'atteindre ses objectifs, un SGDN dépendra souvent d'une MPT ou plus[13]. Les descriptions techniques énoncées

9. D. GERVAIS, «Electronic Rights Management and Digital Identifier Systems» (1999), en ligne (anglais seulement): <http://www.press.umich.edu/jep/04-03/gervais.html> (date de consultation: 15 mars 2002). B. Hugenholtz a défini un SGDN à la manière d'un contrat, habituellement un accord de licence, jumelé à une technologie, habituellement une mesure de protection technique telle que le chiffrement. Voir B. HUGENHOLTZ, «Copyright, Contract and Code: What Will Remain of the Public Domain», (2000) 26 *Brook. J. Int'l L.* 77.
10. Pour un examen complet des caractéristiques du SGDN, voir D. GERVAIS, *ibid*.
11. J. CUNARD, «Technological Protection of Copyrighted Works and Copyrighted Management Systems: A Brief Survey of the Landscape», Congrès ALAI 2001, p. 2.
12. C. BARLAS et M. ISHERWOOD, «Security Technology and Rights Management Information», dans J. KENDRICK (éd.), *Collective Licensing: Past, Present and Future,* Pays-Bas: Maklu Publishers, 2002, p. 182.
13. Voir M. STEFIK, «Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge us to Rethink Digital Publishing», (1997) 12 *Berkely Tech. L.J.* 137. Le SGDN, à son tour, peut être écrit au moyen d'un logiciel créé à cette fin. XrML est un exemple de logiciel de langage des droits numériques. Ce type de logiciel est annexé à une œuvre numérique et permet au titulaire de droits d'établir les modalités d'utilisation de l'œuvre sous-jacente. Comme l'indique Stefik:
    Pour illustrer l'utilisation des langages des droits numériques, dans une situation typique, un auteur créerait une œuvre numérique au moyen de tout système auteur de son choix. Les droits de propriété numériques sont neutres en matière

dans les parties suivantes de la présente étude serviront à établir une distinction, dans la mesure du possible, entre les SGDN qui ont recours aux MPT et ceux qui n'y ont pas recours.

Il est important de reconnaître que les technologies mêmes qui ont été utilisées pour contrôler les droits à la propriété intellectuelle dans le cyberespace et ailleurs ont également été utilisées pour en tirer profit. Par «contournement» d'une MPT, nous entendons le non-respect ou l'évitement des règles d'utilisation d'une mesure de protection en vue d'empêcher l'accès non autorisé à un système ou à un mécanisme tel qu'une base de données, un système de communication par satellite ou un dispositif de sécurité rattaché aux films en format DVD[14]. Une bonne part des incitations en faveur d'une mesure qui fournirait des protections juridiques aux MPT découle de la reconnaissance que bon nombre des MPT sont vulnérables au phénomène de contournement.

3.0 MPT

3.1 Introduction

Dans cette partie de l'étude, nous décrirons un certain nombre de MPT qui régissent l'accès aux œuvres et autres MPT qui contrôlent l'utilisation des œuvres. Ce n'est nullement notre but de fournir une vue d'ensemble complète des MPT – pareille tâche serait impensable en raison de l'évolution rapide des technologies. Notre but est plutôt de fournir suffisamment de détails techniques pour permettre une compréhension plus ferme des «*mesures techniques efficaces*» et autres notions terminologiques clés énoncées dans le WCT et le WPPT de l'OMPI[15]. Par conséquent, les descriptions de ces technolo-

---

de format de données et d'interprétation; en d'autres termes, ils sont susceptibles de fonctionner avec toute représentation numérique de textes, d'images, de bases de données, de musiques ou de vidéos. Une fois une œuvre créée, un éditeur pourrait l'importer dans un système fiabilisé [p. ex., XrML ou le langage des droits numériques de Xerox]. Il déciderait des droits auxquels associer l'œuvre, et les encoderait au moyen de l'éditeur de droits d'un programme d'édition. Il pourrait ensuite rendre l'œuvre accessible sur un serveur pour fins de vente [ou de délivrance de licences] en ligne.
[Traduction libre]

14. Traduction libre d'une définition extraite de *Universal Studio* c. *Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).
15. *Supra*, notes 2 et 3. Tel qu'il sera abordé plus en détail dans la seconde étude, les deux traités de l'OMPI stipulent que «les Parties contractantes doivent prévoir une protection juridique appropriée et des sanctions juridiques efficaces contre la neutralisation [sic] des *mesures techniques efficaces*...».

gies ne sont pas énoncées de manière à satisfaire la curiosité intellectuelle des techniciens qui les créent et les utilisent. La barre est placée ici beaucoup moins haute. Notre but se résume à fournir à propos des techniques des descriptions suffisantes pour éclairer de manière significative un débat de politiques sur les exigences de conformité au WCT et au WPPT.

Les MPT sont souvent classifiées selon leurs fonctions. Une ligne de démarcation est fréquemment tracée entre les MPT qui contrôlent l'*accès* aux œuvres et celles qui régissent l'*utilisation* de ces œuvres[16]. Cependant, tel qu'il est indiqué ci-dessous, les MPT présentent souvent les deux types de caractéristiques. Cela complique la vie des législateurs qui peuvent souhaiter offrir une protection anti-contournement à l'une des catégories de MPT mais pas à l'autre. Cela rend également plutôt imparfaite la classification des MPT de contrôle de l'accès et des MPT de contrôle de l'utilisation, comme le démontre la discussion ci-après.

3.2 MPT de contrôle de l'accès

Cette première catégorie de MPT est utilisée pour empêcher les personnes non autorisées d'*obtenir l'accès* aux œuvres numérisées. C'est l'équivalent d'un verrou virtuel sur pareilles œuvres. Un certain nombre de différentes méthodes peuvent être utilisées pour identifier si une personne en particulier est autorisée. Les deux modes les plus courants sont: i) les mots de passe; et ii) la cryptographie[17].

3.2.1 Cryptographie

La cryptographie est la science du chiffrement et du déchiffrement. Jules César a popularisé cette pratique. Douteux de ses messagers au moment de communiquer avec ses gouverneurs et officiers, il encodait ses messages[18]. Le chiffrement est le codage du texte clair

16. K. KOELMAN et N. HELBERGER, «Protection of Technological Measures», dans B. HUGENHOLTZ (éd.), *Copyright and Electronic Commerce Legal Aspects of Electronic Copyright Management*, Londres: Kluwer Law International, 2000, p. 165. Voir aussi CUNARD, *supra*, note 11.
17. J. de WERRA, «The Legal System of Technological Protection Measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union Directives and other National Laws (Japan, Australia)», Congrès ALAI 2001, p. 4 et 5.
18. M. McINNES, I. KERR, C. CARMODY et J.A. VANDUZER, *Managing The Law: The Legal Aspects of Doing Business*, Toronto: Pearson Education, 2002, ch. 17.

dans un format illisible appelé **cryptogramme** afin de le rendre incompréhensible aux yeux de ceux qui ne sont pas dans le secret du code. César créait un système plutôt simple selon lequel chaque caractère de ses messages était remplacé par un caractère situé trois places plus loin dans l'alphabet romain. Les destinataires autorisés obtenaient la grille de décodage. Le déchiffrement est le processus qui consiste à reconvertir le texte chiffré dans sa forme originale afin qu'il puisse être compris et appliqué. La cryptographie permet la communication de l'information d'une manière déguisée afin de garder son contenu à l'abri des yeux de destinataires indésirables ou non autorisés[19].

Le système qu'utilisait César reposait sur la création et le partage d'un code privé, aujourd'hui appelé clé privée (composée de caractères ou de chiffres). La cryptographie à clé privée, également connue sous le nom de cryptographie symétrique, utilise la même clé pour les processus à la fois de chiffrement et de déchiffrement[20]. Voici une explication du fonctionnement de la cryptographie symétrique:

> Les messages chiffrés et la clé sont envoyés séparément au destinataire voulu. S'il s'agissait simplement du cas de deux amis qui souhaitent partager des renseignements secrets, cela serait facile. La personne A encode le message et fait parvenir le message chiffré ainsi que la clé séparément à la personne B. La personne B peut ensuite décoder le message [au moyen de la clé]. Si la clé est laissée en clair (mode déchiffré), elle risquerait d'être captée durant la transmission et utilisée sur-le-champ pour décoder le message, ce qui entraînerait un manquement à la sécurité.[21]

Pour cette raison, la cryptographie à clé publique (ou asymétrique) est souvent l'approche privilégiée. En vertu de la cryptographie à clé publique, une paire jumelle de clés est créée: une clé est privée; l'autre, publique. Leur propriété fondamentale est que,

19. C. RISHER, «Technological protection measures (anti-circumvention devices) and their relation to exceptions to copyright in the Electronic environment», Forum sur le droit d'auteur de l'UIE (Union internationale des éditeurs), Salon du livre de Frankfurt, 20 oct. 2000, p. 1 et 2. Voir aussi Network Associates et ses entreprises affiliées, *Introduction to Cryptography* (1990-1999), en ligne (anglais seulement): <http://www.pgpi.org/doc/pgpintro> (date de consultation: 8 avril 2002).
20. L. JANCZEWSKI, *Internet and Intranet Security Management: Risks and Solutions*, Hershey: Idea Publishing, 2000, p. 149.
21. RISHER, *supra*, note 19, p. 2.

même si une clé ne peut être déduite de l'autre, un message encodé au moyen d'une clé ne peut être déchiffré qu'avec l'autre clé. Puisque les deux clés sont requises – l'une pour chiffrer et l'autre pour déchiffrer – personne n'a besoin de partager sa clé privée avec autrui. En fait, il est essentiel que la clé privée demeure secrète et soit maintenue sous la garde de la personne dont elle relève. La clé publique, par contre, n'est utile que si elle est possédée par le plus grand nombre de personnes possible. C'est seulement en rendant la clé publique facilement accessible que l'on peut permettre à d'autres d'envoyer des données chiffrées. Bien que ce ne soit pas nécessairement le cas, les clés sont souvent interchangeables[22]. En d'autres termes, «si la clé A sert à chiffrer un message, alors la clé B permet de le déchiffrer, et si la clé B sert à chiffrer un message, alors la clé A permet de le déchiffrer» [Traduction libre][23].

Une procédure similaire est utilisée pour créer des signatures électroniques, qui peuvent servir à authentifier l'identité d'une personne en vue de déterminer si cette personne est autorisée à obtenir l'accès à une œuvre numérisée. Une simple signature électronique est le cryptogramme résultant de l'encodage d'un message. Ce processus de signature électronique n'est qu'une façon de satisfaire à l'exigence d'équivalence fonctionnelle des signatures électroniques dans la plupart des lois canadiennes sur le commerce électronique. Si une personne signe son message et l'envoie à une autre accompagnée d'une signature électronique annexée, elle peut déchiffrer la signature électronique annexée au moyen de sa clé publique et la comparer avec le message. Si les deux versions sont identiques, et en présumant que la clé publique utilisée pour déchiffrer la signature est réellement sa clé publique, la personne peut présumer de manière raisonnable que le message provient effectivement de l'autre personne puisqu'il doit avoir été signé grâce à sa clé privée[24]. Par conséquent, le déchiffrement d'une signature électronique au moyen d'une clé publique est une façon de vérifier une signature électronique[25].

Une autre forme d'authentification similaire à une signature numérisée est un certificat numérique. Servant à confirmer l'iden-

22. *Ibid.*
23. RISHER, *supra*, note 19, p. 2.
24. Une technique plus évoluée comprend la prise initiale d'un «hachage», c.-à-d. une version comprimée de votre message, à partir duquel le message ne peut être déduit, et de chiffrer ce hachage. Voir R.E. SMITH, *Internet Cryptography*, Reading: Addison Wesley, 1997, p. 280.
25. McINNES, KERR, CARMODY et VANDUZER, *supra*, note 18.

tité des utilisateurs dans l'univers cybernétique, les certificats numériques sont distribués par des tierces parties fiables connues sous le nom d'autorités de certification (AC). Un certificat numérique contient le numéro de version du certificat, le numéro de série de l'utilisateur, l'algorithme utilisé pour signer le certificat, l'AC qui a délivré le certificat, la date d'expiration du certificat, le nom de l'utilisateur, la clé publique de l'utilisateur et la signature numérisée de l'utilisateur[26]. Les certificats jouent un rôle important en matière de sécurité, puisque les administrateurs du système peuvent configurer les serveurs pour n'accepter que les certificats signés par certaines AC. Afin d'améliorer davantage la sécurité sur Internet, des protocoles ont été élaborés afin de s'occuper seulement du chiffrement et du déchiffrement des données. Un exemple est le protocole sécurisé SSL (pour «Secure Socket Layer»): «Le protocole SSL fournit entre deux systèmes tout un canal de transmission consacré exclusivement à l'échange de données chiffrées ... [et] il peut être utilisé comme outil de base pour d'autres protocoles d'application [sur le Web] tels que HTTP, SMTP, TELNET, FTP, etc.» [Traduction libre][27].

3.2.2 Dispositifs et lecteurs d'activation des MPT de contrôle de l'accès

Reposant sur le modèle de la cryptographie, un certain nombre de méthodes ont été mises au point afin de faire le pont entre les fichiers chiffrés et les dispositifs ou lecteurs composés d'éléments matériels et/ou logiciels de sorte qu'un message chiffré puisse n'être déchiffré qu'au moyen d'un dispositif ou d'un lecteur particulier[28].

Risher décrit un certain nombre de méthodes différentes[29]:

> **Contenu scellé:** Le contenu est chiffré et ne peut être ouvert que lorsqu'un jeton unique et authentique est présent dans le dispositif. Le jeton en soi ne peut être reproduit. Par conséquent, le contenu ne peut être déchiffré sur un autre appareil, puisque l'autre appareil ne disposerait pas du même jeton. Cependant, dans certains systèmes antérieurs, dès que le con-

26. L. JANCZEWSKI, *supra*, note 20, p. 12. L'auteur trace une analogie entre les certificats numériques et un permis de conduire ou un passeport.
27. *Ibid*.
28. RISHER, *supra*, note 19, p. 2.
29. RISHER, *supra*, note 19, p. 2 à 4.

tenu était ouvert avec l'aide du jeton, le contenu devenait accessible de manière non protégée par la suite et pouvait être copié et distribué.

Association de dispositifs: Les unités centrales de traitement (UCT), disques durs et cartes d'interface réseau (CIR) des ordinateurs comportent des identificateurs (ID) uniques. La méthode d'association de dispositifs se prévaut de cette caractéristique en reliant la clé de déchiffrement avec l'un de ces ID uniques dans un ordinateur à partir duquel l'achat de contenu s'effectue. Ainsi, le dispositif présent dans l'ordinateur qui déchiffre et lit le contenu (le «lecteur») utilise l'un des ID de ce dispositif pour obtenir la clé de déchiffrement requise pour décoder le contenu de sorte qu'il puisse être lu, mais il n'est déchiffré que pendant son utilisation sur ce dispositif spécifique. Par conséquent, si un fichier est distribué ultérieurement à un autre ordinateur, il ne pourra être «lu» sur cet ordinateur.

Lecteur validé: Certains systèmes de lecture de livres électroniques recherchent la clé imbriquée dans le contenu. Le lecteur n'activera le contenu à visualiser que si la clé y est présente. La clé est unique à une marque et à une version particulières de lecteur.

Lecteur à validation activée: Selon ce scénario, un lecteur qui peut lire les œuvres à contenu non chiffré fonctionne de pair avec un enfichable (c.-à-d. un logiciel téléchargé vers le système et reconnu par le lecteur) qui contrôle l'accès au contenu lorsque le lecteur est utilisé. Le module enfichable prend le contrôle du lecteur durant le processus de lecture. Ainsi, par exemple, l'enfichable pourrait ne pas permettre que certains éléments de contenu visualisés au moyen du lecteur soient imprimés ou sauvegardés dans un fichier.

Dispositif validé (environnement fermé): Un lecteur relevant de cette catégorie est conçu pour lire certains types d'éléments de contenu, mais pas pour exécuter de logiciels. Certains types de lecteurs du contenu des livres électroniques tombent sous cette catégorie. Le contenu est chiffré et la clé de déchiffrement ne fonctionne que dans l'environnement fermé du lecteur même. Par conséquent, aucun autre logiciel ne peut trouver la clé et le lecteur est restreint aux utilisations pour lesquelles il a été fourni.

Dispositif validé (détection): Dans le cas du contenu audio et vidéo, une mesure additionnelle est utilisée (outre le chiffrement) pour sécuriser le contenu. Afin d'être reconnu comme autorisé, le contenu doit comprendre un certain masque ou code qui peut être détecté par le dispositif de lecture avant que le dispositif ne puisse le lire.

Contrôles de l'accès en ligne: Le déroulement en continu est utilisé pour l'affichage de prestations en direct ou en temps réel de contenu musical et vidéo. Le contenu numérisé est déchiffré pendant une courte période durant son acheminement au lecteur puis il est réenchiffré afin d'empêcher toute copie. Certaines variations permettent le chiffrement de seulement 10 à 20 p. 100 du contenu pendant son affichage en mode audible ou visible. Cette technologie fonctionne parce que ces types de fichiers de contenu sont très gros et toute copie ne peut être effectuée que lentement pendant les courts moments où le contenu est perceptible par les humains.

Haute sécurité à clés multiples: Dans certains systèmes, le déchiffrement est accompli selon un mode page à page. Chaque page utilise une clé distincte transmise avec le contenu pour la page en question et, dès que la page est visualisée, la clé utilisée pour déchiffrer cette page est détruite. Ce système exige une connexion en ligne pendant la visualisation du contenu.

Avant de conclure l'exposé sur les MPT de contrôle de l'accès qui utilisent le chiffrement, deux observations critiques sont de mise. Premièrement, certaines des MPT décrites ci-dessus contrôlent non seulement l'accès à une œuvre, mais également l'utilisation ultérieure de cette œuvre. Par exemple, un lecteur à validation activée peut à la fois contrôler l'accès au contenu au moyen du chiffrement et servir à déterminer si ce contenu, une fois déchiffré de manière légitime, peut être copié, entreposé ou imprimé par l'utilisateur. Cet exemple illustre le fait que le régime de classification énoncé précédemment est simplifié à outrance: souvent, la distinction entre les fonctions de contrôle de l'accès et les fonctions de contrôle de l'utilisation est illusoire.

Deuxièmement, les MPT – en particulier les MPT de contrôle de l'accès – peuvent créer des problèmes pour les utilisateurs légitimes d'une œuvre. Envisagez, par exemple, un consommateur qui a acheté un accès en ligne à un contenu qui est sécurisé au moyen d'une association de dispositifs. Souvenez-vous que cette association

de dispositifs est propre à chaque appareil – un fichier sera accessible sur un dispositif spécifique (p. ex., un ordinateur portable particulier) mais sera inaccessible au moyen d'un dispositif différent (p. ex., un autre ordinateur). Le premier problème auquel sera confronté l'utilisateur est qu'il lui sera impossible d'accéder au contenu à partir de l'autre ordinateur. En outre, si le disque dur qui porte l'ID utilisé pour l'association de dispositifs échoue et est remplacé par un autre disque dur, comme c'est souvent le cas des ordinateurs portables, le consommateur perdra tout accès au contenu même s'il est un utilisateur légitime.

3.2.3 Système de brouillage du contenu (SBC)

Le SBC est un système bien connu comme MPT visant à protéger les films diffusés en format DVD (Digital Versatile Disk, c.-à-d. disque numérique polyvalent). Le SBC comporte les caractéristiques suivantes:

1) le contenu du disque est chiffré;

2) les clés qui permettent à un lecteur DVD ou à un lecteur DVD-ROM d'accéder à ce contenu sont également chiffrées;

3) seuls les dispositifs DVD fabriqués conformément à une licence SBC peuvent déchiffrer et lire le film sur un disque protégé;

4) il est strictement interdit aux dispositifs DVD de permettre la copie du contenu des DVD protégés, sauf exceptions[30].

Les licences de déchiffrage SBC imposent les exigences suivantes aux dispositifs DVD assujettis à une activation SBC:

1) le contenu qui est déchiffré en toute légitimité au moyen d'un dispositif DVD doit être sécurisé contre tout accès non autorisé à l'intérieur de l'appareil (c.-à-d. que le dispositif DVD doit être protégé contre toute tentative d'altération);

2) le contenu ne peut être envoyé qu'à certaines sorties informatiques autorisées, notamment:

   a) les sorties analogiques dotées d'une technologie (p. ex., Macrovision) pour prévenir toute copie par les magnétoscopes analogiques, notamment;

30. CUNARD, *supra*, note 11, p. 6.

b) les sorties numériques sécurisées, p. ex., PCTN (voir ci-après), qui garantissent également que le contenu se rendra à une destination connue au moyen d'une MPT de contrôle de la copie;

3) les dispositifs vendus dans une zone géographique particulière ne peuvent lire que les disques autorisés pour une lecture dans cette zone;

4) les fabricants qui enfreignent ces règles contractuelles sont passibles de poursuite, d'une saisie de leurs produits et du versement de dommages-intérêts rigoureux;

5) les studios de cinéma obtiennent le droit d'«encoder» leurs films DVD et ils peuvent empêcher toute copie numérique à partir d'un dispositif d'enregistrement[31].

Fait intéressant à souligner, la technologie SBC et la licence qui en régit l'utilisation allient de multiples fonctions de protection du contenu. Pareilles fonctions comprennent (mais sans s'y limiter) «le contrôle de l'accès, le contrôle de la copie, le contrôle de la diffusion électronique et même un mécanisme visant à restreindre la redistribution géographique non autorisée des DVD en tant que tels» [Traduction libre][32].

Tel qu'il sera discuté plus en détail dans notre seconde étude, le SBC a été piraté au moyen de la technologie DeCSS[33]. Le logiciel DeCSS a été mis au point par Jon Johansen, un adolescent norvégien, collaborateur de deux autres individus sur Internet, afin de développer un lecteur DVD fonctionnant sur le système d'exploitation Linux. Si un utilisateur exécute DeCSS sur une plate-forme Microsoft avec un DVD dans le disque dur de son ordinateur, le DeCSS déchiffrera la protection SBC du DVD, permettant à l'utilisateur d'accéder aux fichiers DVD et en placera une copie sur le disque dur de l'utilisateur. Le fichier résultant, bien qu'il soit très large, pourra être lu sur un lecteur non conforme à la norme SBC et pourra être copié ou manipulé comme un fichier informatique ordinaire. La qualité du film déchiffré résultant est presque identique à celle du film chiffré original sur le DVD. Le fichier produit par le

31. CUNARD, *supra*, note 11, p. 6 et 7.
32. *Ibid.*, p. 7.
33. *Universal City Studios* c. *Remeirdes*, 111 F. Supp. 2d 294 (S.D.N.Y 2000) [ci-après appelé *Universal* c. *Remeirdes*]; conf. sous le nom *Universal City Studios* c. *Corley*, 273 F.3d 429 (2e Circuit 2001).

DeCSS peut également être comprimé par le logiciel appelé DivX, facilement accessible sur Internet[34]. Le fichier comprimé peut être copié sur un DVD et transmis sur Internet[35].

Le contournement du SBC a donné lieu à une importante cause type relative aux dispositions anti-dispositif de la *Digital Millennium Copyright Act (DMCA)*[36] américaine de 1998[37]. Bien que la Cour ait confirmé ces dispositions et accordé à huit studios de cinéma une injonction permanente interdisant à deux intimés d'afficher le DeCSS sur leur site Web et d'inclure un lien vers d'autres sites contenant le DeCSS, ce dispositif de contournement continue d'être largement accessible sur Internet.

Une leçon intéressante à tirer de cette cause est que, dès qu'un dispositif de contournement à base de logiciel devient accessible, les législations anti-contournement jumelées à des mesures d'application rigoureuses ne suffisent pas toujours à éliminer la menace de contournement. Une autre leçon intéressante est que la diffusion de masse du DeCSS sur Internet a favorisé la création et le développement d'une technologie innovatrice. Mis au point grâce à l'accès libre au code source du DeCSS, le logiciel de compression DivX est maintenant largement utilisé dans bon nombre de fonctions d'applications légitimes, notamment les consoles de jeux et l'affichage vidéo en continu. L'aspect ironique de tout cela est que le DivX est une technologie que de nombreuses sociétés, y compris Sony et Universal Studios, utilisent pour faire défiler en continu des vidéos en ligne[38].

3.2.4 Segmentation asymétrique d'applications (SAA)[39]

La SAA est une technologie qui consiste à extraire une petite partie du code exécutable d'une application binaire, de placer le code

34. La compression est la réduction de la taille d'un fichier au moyen d'un algorithme mathématique qui supprime l'information redondante ou non essentielle. Voir S.M. KRAMARSKY, «Copyright Enforcement in the Internet Age: The Law and Technology of Digital Rights Management», (2001) 11 *DePaul-LCA J. Art & Ent. L.* 1, 5 et 6.
35. *Universal* c. *Remeirdes*, *supra*, note 33, p. 438.
36. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codifié, dans la partie pertinente de 17 U.S.C. s. 1201 (Supp. IV 1999)).
37. *Universal* c. *Remeirdes*, *supra*, note 33, p. 435.
38. Voir le site Web de DivX annonçant les entreprises qui utilisent sa technologie, en ligne (anglais seulement): <http://www.divx.com> (date de consultation: 8 avril 2002).
39. La description de la «SAA» au paragraphe 3.2.4 et la description de «billets numériques» au paragraphe 3.2.5 ne sont que deux des nombreux exemples d'avènements brevetés en matière de technologies d'accès aux MPT.

extrait sur un serveur et de combler le vide créé par l'extraction au moyen d'un «point d'accueil»[40]. Lorsque l'utilisateur exécute l'application, celle-ci s'exécute jusqu'à ce que le point d'accueil soit atteint. À ce point, l'application reconnaît la nécessité du code exécutable extrait. Cela amène l'ordinateur à accéder à Internet à la recherche du code manquant. Le point d'accueil conserve également en mémoire le contexte de l'application – notamment, qui l'utilise, où l'application est utilisée et à quelle étape en est l'application. Le point d'accueil se met en connexion avec le serveur approprié, qui authentifie l'utilisateur et renvoie une demande de précisions sur le contexte d'entrée de l'application. Le serveur éloigné saisit ensuite le contexte de l'application dans le code extrait. Il déduit une sortie, qui est retournée à l'utilisateur. Cela active l'application pour qu'elle puisse continuer d'être exploitée. Puisque l'application est essentiellement inutile sans le code extrait, l'application a peu de risques d'être copiée.

3.2.5 Billets numériques

La technologie des «billets numériques» repose sur un code intégré à une carte à puce ou un ordinateur[41]. Ce code détermine si quelqu'un a le droit d'accéder au contenu numérique. Lorsque le billet est présenté, «il est poinçonné électroniquement pour indiquer qu'un droit a été utilisé» [Traduction libre][42]. Une personne pourrait se servir d'un billet numérique entreposé sur un ordinateur personnel ou un autre dispositif pour afficher une image, imprimer un livre ou faire jouer de la musique.

L'aspect intéressant de cette méthode est que le billet peut être associé au contenu ou l'accompagner en permanence. Par conséquent, si le contenu (p. ex., une chanson, un film ou un livre) est transmis par courriel, téléchargé ou copié, le billet est poinçonné à nouveau. Cela permet au propriétaire du contenu d'être rémunéré chaque fois qu'une copie est produite. En d'autres termes, outre la protection contre tout accès non autorisé aux œuvres numérisées, les

40. Une description de la SAA est fournie en ligne (anglais seulement): <http://www.netquartz.com/technology/techno2.htm> (date de consultation: 31 mars 2002). Conçue et brevetée par netquartz, la SAA est utilisée dans le système de gestion des droits numériques de l'entreprise.
41. Voir une description de «billets numériques» en ligne (anglais seulement): <http://www.content-wire.com/Home/Index.cfm?ccs=86&cs=546> (date de consultation: 27 fév. 2002). ContentGuard est le concepteur et le titulaire du brevet de cette technologie.
42. *Ibid.*

billets numériques peuvent être utilisés pour le contrôle de la tarification et le paiement dans le cadre d'un SGDN.

3.3 MPT de contrôle de l'utilisation (contrôle de la copie)

Cette deuxième catégorie de MPT permet à un titulaire de droits de *contrôler l'utilisation sous-jacente* d'une œuvre, même une fois l'accès obtenu. Habituellement, cela a signifié le *contrôle des copies non autorisées* d'une œuvre – les mesures de contrôle de la copie sont les mesures de contrôle de l'utilisation les plus courantes[43]. Cependant, pareilles MPT prévoient les contrôles de l'utilisation plutôt que la simple copie. Comme le souligne de Werra:

> [...] ces technologies peuvent protéger non seulement contre la simple copie de l'œuvre, mais également contre les actes qui violent les *autres* droits exclusifs des propriétaires de droits d'auteur ... Une mesure de protection technique pour le contenu audio (et vidéo) pourrait également être développée afin de prévenir l'affichage en continu de ces œuvres sur Internet. Puisque l'affichage en continu n'effectue aucune copie de la musique sur le disque dur de la personne qui l'écoute, mais lui permet simplement de l'écouter, pareille technologie empêcherait principalement la violation du droit d'exécution publique et du droit de diffusion, et non le droit de reproduction. [Traduction libre][44]

Un exposé de certaines des MPT de contrôle de la copie les plus populaires se trouve ci-après.

3.3.1 Macrovision

Macrovision est une méthode de protection contre la copie destinée aux magnétoscopes analogues VHS. Cette méthode sert à empêcher la copie de bandes vidéo préenregistrées. Si une bande protégée fait l'objet d'une copie, les images de la version copiée s'afficheront mal au moment de la lecture sur le magnétoscope où la fonction Macrovision est activée. À la place, l'image deviendra foncée à intervalles périodiques et instable à son point le plus foncé[45].

---

43. J. de WERRA, *supra*, note 17, p. 6.
44. *Ibid*.
45. Voir une description en ligne (anglais seulement): <http://66.40.78.100/Services/TECH_Notes/nineteen.html> (date de consultation: 5 mars 2002). Voir aussi une description technique de Macrovision, en ligne (anglais seulement): <http://macrovision.com/acp.html>.

Macrovision exploite le circuit à contrôle automatique du gain (CAG) du magnétoscope lorsqu'une bande est en cours d'enregistrement. Le but du CAG est de s'assurer que les signaux faibles sont amplifiés et que les signaux forts sont atténués, de sorte que l'ensemble des capacités d'enregistrement des bandes magnétoscopiques soient utilisées. Grâce à Macrovision, les nouveaux signaux sont insérés dans la partie non visible de l'image. Ces signaux permettent au magnétoscope de détecter les moments où l'image normale est trop lumineuse. Le circuit CAG assombrit l'image jusqu'à ce qu'il détecte un état normal. Cependant, puisque l'image n'était pas très lumineuse au départ, elle devient maintenant trop foncée. Ce processus se répète. Le téléviseur n'est pas, en soi, affecté étant donné que la plupart des téléviseurs ne sont pas munis de circuits CAG et ceux qui en sont munis ont un fonctionnement différent des circuits CAG des magnétoscopes.

Ce type de MPT peut être utilisé pour la télé payante, la télé à la carte et les vidéocassettes en vue d'empêcher la prise de copies des œuvres audiovisuelles ou la détérioration de la qualité de l'enregistrement ou de la lecture.

Le contournement de Macrovision est possible avec l'aide de stabilisateurs commerciaux[46]. Ces stabilisateurs sont des dispositifs coûteux qui permettent de déjouer un logiciel de sécurité de commerce comme Macrovision[47].

3.3.2 Système de gestion de la duplication en série (SGDS)

Le SGDS empêche la production illicite de multiples générations de copies numériques à partir d'un original assujetti aux règles du droit d'auteur[48]. Cela se fait au moyen d'un filigrane. Un filigrane, c'est l'information qui est encodée numériquement de manière cachée dans une œuvre numérisée[49]. Les données en filigrane peuvent être utilisées pour authentifier ou autrement retracer les copies[50], ou

46. *Ibid*.
47. Voir une description en ligne (anglais seulement): <http://slashdot.org/articles/99/11/04/1415200.shtml> (date de consultation: 1er avril 2002).
48. Voir une description en ligne (anglais seulement): <http://www.mitsuicdrstore.com/SCMS_nh.html> (date de consultation: 7 mars 2002).
49. R. JONES, «Wet Footprints? Digital Watermarks: A Trail to the Copyright Infringer on the Internet», (1999) 26 *Pepp. L. Rev.* 559, 569.
50. Par exemple, afin de retracer l'origine des œuvres protégées lorsqu'elles se trouvent sur des sites Web ou à d'autres emplacements où elles ne sont pas censées être. Voir CUNARD, *supra*, note 11, p. 9.

encore pour faciliter la mise en œuvre d'une fonction de contrôle de la copie.

Dans le SGDS, les données en filigrane sont utilisées pour indiquer si un disque compact (DC) peut ou non être copié sans restriction, copié une seule fois (à des fins personnelles) ou pas du tout[51]. Si quelqu'un tente de se servir d'un dispositif d'enregistrement conçu selon la norme SGDS pour copier un DC qui ne contient pas un filigrane SGDS, la tentative de copie échouera[52].

Un certain nombre de techniques de contournement existent déjà pour le matériel SGDS[53]. Il est également intéressant de mentionner que la norme SGDS n'empêche pas la prise de multiples copies numériques d'une œuvre numérisée si chaque copie est exécutée à partir d'un DC encodé selon la norme SGDS. La norme SGDS peut seulement empêcher la prise de copies numériques à partir de copies numériques.

3.3.3 Protection du contenu des transmissions numériques (PCTN)

Le but de la technologie PCTN est d'empêcher la distribution non autorisée du contenu audiovisuel reçu au foyer en format numérique une fois déchiffré[54].

Cette technologie contrôle le contenu qui se déplace entre un «dispositif de départ» en mode PCTN (notamment le coffret d'abonné de la télé par câble ou par satellite, le lecteur DVD ou un appareil PlayStation de Sony) et un «dispositif d'arrivée» en mode PCTN (tel qu'un téléviseur, un ordinateur personnel ou un magnétoscope). Le

51. Voir une description en ligne (anglais seulement): <http://www.mitsuicdrstore.com/SCMS_nh.html> (date de consultation: 2 juillet 2002).
52. L'*Audio Home Recording Act of 1992*, Pub. L. No. 102-563, 106 Stat. 4237 (1992) (codifiée à 17 U.S.C. ss. 1001-1010 (1994)) exige l'incorporation de la fonctionnalité SGDS dans tout dispositif d'enregistrement audio numérique importé, fabriqué ou distribué aux États-Unis. Voir s. 1002.
53. Voir, p. ex., une description en ligne (anglais seulement): <http://www.fet.uni-hannover.de/~purnhage/dat/dat.html> (date de consultation: 7 mars 2002).
54. CUNARD, *supra*, note 11, p. 7. PCTN est une création commune de: Hitachi, Ltd., Intel Corp., Matsushita Electric Industrial Co., Ltd., Sony Corp., et Toshiba Corp. Le consortium est mentionné sous l'abrévication de 5C (pour cinq compagnies ou entreprises). Voir «Digital Transmission Content Protection White Paper», en ligne (anglais seulement): <http://www.dtcp.com/data/wp_spec.pdf> (date de consultation: 7 avril 2002).

dispositif d'arrivée est programmé de manière à traiter le contenu reçu en toute sécurité. Ainsi, par exemple, il ne peut servir à retransmettre le contenu vers le Web[55].

Le mode PCTN comporte les caractéristiques suivantes:

1) Il comprend le chiffrement entre tous les dispositifs de départ et d'arrivée.

2) Il exige l'établissement d'une liaison entre tous les dispositifs de départ et d'arrivée sur le réseau (afin de s'assurer que les dispositifs d'arrivée traitent le contenu conformément aux règles PCTN). Jusqu'à ce que cela se produise, le dispositif de départ ne pourra acheminer le contenu au dispositif d'arrivée.

3) Il comprend une disposition pour le transport de «données de contrôle de la copie» dans le train binaire entre tous les dispositifs de départ et d'arrivée qui envoie un signal au dispositif d'arrivée lui indiquant si et quand il pourra faire une copie du contenu reçu en mode PCTN.

4) Il appuie la «révocation» des dispositifs qui ont été piratés, ou de clones piratés de dispositifs qui ont fait l'objet d'une effraction. Les dispositifs révoqués sont simplement désactivés par rapport à la réception d'un contenu numérisé en mode PCTN[56].

La technologie PCTN, tout comme la SBC, est assujettie à un régime complet d'obtention de licences. Le régime PCTN contient les éléments suivants:

1) Les propriétaires de contenu sont autorisés à encoder certains films et types de transmissions ou de services d'acheminement selon l'un des critères suivants:

   a) «copie strictement interdite» – aucune copie ne peut en aucun cas être effectuée;

   b) «copie d'une génération seulement» – une génération de copies numériques est autorisée;

---

55. *Ibid*.
56. *Ibid.*, p. 8. Pour de plus amples explications, voir *DTCP Tutorial* (le didacticiel de PCTN), en ligne (anglais seulement): <http://www.dtcp.com/data/dtcp_tut.pdf> (date de consultation: 7 avril 2002).

c) «copie autorisée, mais toute retransmission interdite» – de multiple copies peuvent être exécutées, mais aucune retransmission à une sortie non autorisée n'est permise.

2) Les dispositifs à activation de la norme PCTN doivent être construits de façon robuste.

3) Les dispositifs ne peuvent transmettre un contenu protégé selon la norme PCTN qu'aux sorties suivantes:

a) les sorties analogiques comportant une fonction de protection de la copie;

b) les sorties selon la norme PCTN ou toute autre norme approuvée et les sorties numériques sécurisées.

4) Le contenu ne peut jamais être acheminé sur Internet, puisque les connexions à Internet ne sont pas sécurisées.

5) Les dispositifs peuvent seulement enregistrer le contenu si le propriétaire du droit d'auteur en a autorisé la copie, conformément aux règles de chiffrement.

6) Toute copie effectuée par un dispositif relevant d'une licence PCTN doit être enregistrée de manière sécuritaire, par exemple, seulement par un système de chiffrement autorisé, de sorte que l'enregistrement même soit chiffré[57].

3.3.4 Initiative de musique numérique sécurisée (IMNS)

Le chiffrement n'a pas habituellement servi à protéger le contenu des DC de musique produits pour le commerce. La musique sur ces DC peut facilement être enregistrée et comprimée numériquement en fichiers beaucoup plus petits. La technologie la plus couramment utilisée à cette fin est la norme MP3. La musique qui a été traitée de cette manière peut être copiée sur les disques durs, copiée sur des DC pour enregistrement et distribuée facilement sur

57. CUNARD, *supra*, note 11, p. 8 et 9. Voir aussi *DTCP Specifications Volume 1 Version 1.2*, en ligne (anglais seulement): <http://www.dtcp.com/data/info_dtcp_v1_12_20010711.pdf> (date de consultation: 7 avril 2002).

Internet moyennant une reproduction quasi exacte de sa qualité sonore d'origine[58].

L'IMNS, une initiative regroupant plus de 200 entreprises et organisations représentant la technologie de l'information (TI), l'électronique grand public, les technologies de la sécurité, l'industrie du disque partout dans le monde et les fournisseurs de services Internet (FSI), a entrepris de corriger cette situation[59]. L'IMNS a permis de rédiger des lignes directrices et des spécifications visant à intégrer les MPT aux fichiers de musique commerciale. Les mesures de protection prennent la forme d'un régime de chiffrement à des fins particulières seulement, c.-à-d. des interactions autorisées avec les éléments de contenu. Parfois, la procédure de chiffrement et les certificats connexes sont appelés filigrane – c'est le cas lorsque les mesures de protection sont imbriquées dans les dispositifs de reproduction en vue de reconnaître le code de contenu intégré et de le comparer à une liste de révocation. La musique comportant le filigrane de «copie strictement interdite» serait à la fois comprise et appliquée par les dispositifs de reproduction favorables.

En vertu de l'IMNS, la musique serait protégée non seulement par les filigranes, mais également par des communications sécurisées (c.-à-d. chiffrées et authentifiées) entre une application logicielle conforme à la norme IMNS et un dispositif portable, notamment un lecteur de MP3 de poche[60]. En septembre 2000, l'IMNS publiait son code et lançait un défi à la collectivité cryptographique, offrant 10 000 $ à quiconque «pourrait retirer le filigrane ou mettre en échec les autres aspects technologiques du système proposé de protection du droit d'auteur» [Traduction libre][61]. Une équipe de

58. *Ibid.*, p. 11. Pour de plus amples explications, voir Fraunhofer Institut Integrierte Schaltungen (invention du module ISO-MPEG Audio Layer 3), en ligne (anglais seulement): http://www.iis.fhg.de/amm/techinf/layer3/index.html. Voir aussi Moving Pictures Experts Group, en ligne (anglais seulement): <http://www.mpeg.telecomitalialab.com>.
59. Voir Secure Digital Music Initiative Foundation, en ligne (anglais seulement): <http://www.sdmi.org> (date de consultation: 7 avril 2002). Voir aussi Recording Industry Association of America, en ligne (anglais seulement): <http://www.riaa.org/Music-SDMI-1.cfm> (date de consultation: 7 avril 2002).
60. «Commission Staff Working Paper Digital Rights Background, Systems, Assessment», Commission des Communautés européennes (Bruxelles, 2002) («Projet GDN de l'UE»), p. 19. CUNARD, *supra*, note 11, p. 14. Voir SDMI Portable Device Specification Part 1 Version 1.0, en ligne (anglais seulement): <http://www.sdmi.org/download/port_device_spec_part1.pdf> (date de consultation: 6 avril 2002).
61. Voir Secure Digital Music Initiative Foundation, en ligne (anglais seulement): <http://www.sdmi.org/pr/OL_Sept_6_2000.htm> (date de consultation: 7 avril 2002).

chercheurs de l'université Princeton a rapidement percé les algorithmes de chiffrement servant à protéger le contenu numérique.

Par la suite, l'un des chercheurs a reçu des menaces de représailles par rapport à son intention de publier les détails du perçage de l'IMNS, le tout en vertu des dispositions de la *DMCA* américaine interdisant la distribution de technologies permettant le contournement des mesures de protection et/ou l'élimination ou la modification des données sur la gestion du droit d'auteur[62]. L'équipe de recherche a réagi par une poursuite au fédéral à l'endroit de RIAA *et al.*, poursuite qui demandait la permission de publier les résultats des chercheurs selon le principe de liberté de la collectivité scientifique et des milieux universitaires[63]. Felten *et al.* s'étant fait refuser leur demande de contestation initiale, ils ont depuis «décidé de renoncer à des appels permanents à la lumière de la garantie offerte par les gouvernements et l'industrie et selon laquelle les universitaires sont libres d'effectuer leurs recherches et d'en publier les résultats» [Traduction libre][64].

4.0 CONTOURNEMENT

Le contournement d'une MPT instaurée par un propriétaire de droits d'auteur pour contrôler une œuvre numérisée assujettie aux règles du droit d'auteur a été décrit par certains comme l'équivalent électronique d'une introduction par effraction dans une salle verrouillée en vue d'obtenir une copie d'une œuvre, telle qu'un livre[65]. Certaines estimations du coût du contournement illicite sont renversantes. Par exemple, de l'avis de la Motion Picture Association (MPA), l'industrie cinématographique américaine subit des pertes de revenus de plus de 3 milliards $US chaque année en raison du piratage[66]. De plus, la Business Software Alliance (BSA) estime que l'industrie du logiciel a perdu 11,75 milliards $US de recettes en l'an

62. Lire la lettre de RIAA au professeur Edward Felten de l'Electronic Frontier Foundation, en ligne (anglais seulement): <http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010409_riaa_sdmi_letter.html> (date de consultation: 8 avril 2002).
63. Voir *Felten* c. *RIAA*, cas nº 01 CV 2669 (E.D. NJ. 2001), Electronic Frontier Foundation, en ligne (anglais seulement): <http://www.eff.org/Cases/Felten_v_RIAA/20011128_hearing_transcript.html> (date de consultation: 2 juillet 2002).
64. Voir Electronic Frontier Foundation, en ligne (anglais seulement): <http://www.eff.org/Legal/recent_legal.html> (date de consultation: 2 juillet 2002).
65. De WERRA, *supra*, note 17, p. 4.
66. Motion Picture Association of America, <http://www.mpaa.org/anti-piracy/content.htm> (date de consultation: 9 avril 2002).

2000 en raison du piratage[67]. Pour la même année, les estimations canadiennes chiffrent à 305 millions $CAN les pertes dans l'industrie nationale du progiciel seulement[68].

En outre, l'augmentation des coûts de sécurité résultant de la prolifération des technologies de contournement signifie une hausse de coûts pour les consommateurs de contenu et des dissuasions correspondantes pour une production continue[69].

Bien que plusieurs cas de contournement aient déjà été mentionnés précédemment, il est important de brosser un tableau clair de la nature et du fonctionnement des dispositifs de contournement.

Malgré les préoccupations croissantes entourant un possible contournement, il reste un corpus relativement modeste de documentation non technique exposant en détail les techniques de contournement. Cette pénurie de documentation s'explique en partie par l'effet dissuasif des poursuites possibles subies par des universitaires comme le professeur Felten. Cependant, bon nombre des techniques de contournement existent et sont bien connues de la collectivité du piratage. Risher fournit les exemples suivants[70]:

> **Affichage des mots de passe et des numéros d'enregistrement:** L'affichage de pareille information permet aux autres qui n'ont pas acheté les droits d'accès d'utiliser des versions piratées du logiciel ou d'obtenir un accès non autorisé à un réseau ou à tout autre système contenant des œuvres protégées par le droit d'auteur.
>
> **Interception du contenu déchiffré:** Cette méthode comprend l'utilisation d'un logiciel qui saisit le programme pendant son déchiffrement et avant son interaction avec le logiciel utilisé pour visionner ou lire le contenu.
>
> **Déchiffrement selon la technique de la force brute:** Cette forme de contournement emploie de multiples variations

67. Business Software Alliance, <http://www.bsa.org/resources/2001-05-21.55.pdf> (date de consultation: 9 avril 2002).
68. Alliance canadienne contre le vol de logiciels (ACCVL), <http://www.caast.org/resources/FINAL.CanadianReport.pdf> (date de consultation: 9 avril 2002).
69. L. LESSIG, *Code and Other Laws of Cyberspace*, New York: Basic Books, 1999, p. 131.
70. RISHER, *supra*, note 19, p. 5 et 6.

d'algorithmes jusqu'à ce que le contenu soit déchiffré, ce qui exige donc beaucoup de puissance informatique.

Vol de la clé de décryptage durant la transmission: Les pirates du numérique s'adonnent à l'interception des canaux de transmission afin de saisir une clé au moment de sa transmission.

Piratage des systèmes fermés: Cette forme de contournement comprend le démontage de dispositifs validés de systèmes fermés et de percer le code de décryptage en interagissant avec les circuits.

Utilisation d'enfichables piratés: Cette méthode de contournement sous-entend le développement de modules logiciels enfichables illégaux qui peuvent surpasser les enfichables du lecteur à validation activée.

Tel qu'il est mentionné précédemment, certaines des MPT les plus courantes, notamment Macrovision, le SBC, le SGDS et l'IMNS ont déjà été contournées. Bref, on assiste à une escalade de la «course aux armements» entre ceux qui conçoivent les MPT et ceux qui les mettent en échec. Cependant, il est important de noter que les incitations au contournement varient. Bien que ce phénomène soit parfois motivé par une soif d'«empiètement» et le désir de diffuser illégalement des œuvres numérisées assujetties aux règles du droit d'auteur, on trouve également des motifs légitimes en faveur du contournement. Nous avons déjà constaté un exemple du genre, soit la création de DeCSS afin de faire fonctionner les lecteurs de DVD sur le système d'exploitation Linux. Dans d'autres cas, le contournement a été motivé par ce qui suit: i) une quête d'interopérabilité entre les systèmes; ii) le désir de mettre à l'essai la robustesse d'une MPT et d'améliorer par conséquent les outils de pointe; iii) le désir de satisfaire une curiosité intellectuelle; iv) d'autres fins purement universitaires; et v) l'objectif de faire avancer la science de la cryptographie. Certaines personnes affirment également être motivées à contourner les MPT par souci de justice, en particulier lorsqu'elles sont d'avis que les MPT les empêchent d'exercer leurs droits sur une œuvre numérisée qu'elles affirment posséder ou avoir le droit de posséder en vertu de la loi. Tel qu'il sera abordé plus en détail dans notre seconde étude, les motifs de contournement des MPT énoncés précédemment laissent entendre qu'une décision de politique menant à

des lois anti-contournement devrait être abordée avec beaucoup de prudence[71].

5.0 LES SGDN

5.1 Le concept de SGDN

Un système de gestion des droits numériques (SGDN) repose habituellement sur deux fondements théoriques: i) une base de données qui contient l'information servant à préciser le contenu et les titulaires de droits sur une œuvre; et ii) un accord d'obtention de licences qui stipule les modalités d'utilisation de l'œuvre sous-jacente[72]. Les SGDN permettent l'échange de données sur l'utilisation parmi les propriétaires de droits et les distributeurs, et établit la manière dont une œuvre peut être utilisée.

Les SGDN relèvent de deux grandes catégories: les systèmes de gestion des droits numériques qui n'utilisent pas de mesures de protection techniques ou MPT et celles qui le font[73].

5.1.1 Les SGDN qui n'utilisent pas les MPT

Ces types de SGDN sont aisément associés aux organisations de gestion collective (OGC) ou aux sociétés de droits d'auteur[74]. Les OGC sont généralement des organisations représentant des artistes qui accordent aux utilisateurs la permission d'utiliser leurs œuvres inscrites aux répertoires des OGC. Règle habituelle, les OGC négocient les tarifs et modalités d'utilisation des œuvres au nom des artistes, et s'occupent ensuite de recueillir ces tarifs et de répartir les redevances. Puisque les OGC s'occupent le plus souvent de détermi-

71. Voir <http://www.macfergus.com/niels/dmca/cia.html> (date de consultation: 7 mars 2002) pour un exemple concret de l'effet néfaste que la législation anti-contournement des MPT peut avoir sur la recherche légitime dans le domaine de la cryptographie.
72. GERVAIS, *supra*, note 9.
73. T. KOSKINEN-OLSSON, «Secure IPR-Content on the Internet», Congrès ALAI 2001.
74. Un exemple bien connu d'OGC canadienne est celui de la SOCAN. Quant à un exemple américain bien connu, on n'a qu'à penser au Copyright Clearance Center. Pour une excellente vue d'ensemble des différents types d'organismes de gestion collective tant au plan national qu'au plan international, voir D. GERVAIS, «Gestion collective du droit d'auteur et des droits voisins au Canada: Perspective internationale», dans un rapport préparé pour le ministère du Patrimoine canadien (2002), en ligne (en français): <http://www.pch.gc.ca/culture/cult_ind/cpd-pdd/collective/cont_r.cfm> (date de consultation: 8 avril 2002).

ner et d'autoriser les droits de reproduction (réutilisation, réédition, redistribution et copie), elles sont parfois qualifiées d'agents d'affranchissement des droits d'auteur[75].

Bon nombre d'OGC fournissent des services Internet et autres technologies en ligne afin d'assurer une médiation en matière d'affranchissement des droits, d'établissement des modalités de licences et de paiement des tarifs en contrepartie de l'utilisation d'une œuvre[76]. Pareilles technologies facilitent la rapidité et l'efficacité du processus de délivrance de licences sur le contenu. On doit bien faire la distinction entre le recours à ces technologies et l'utilisation des MPT. Dans le second cas, il s'agit uniquement des technologies de contrôle de l'accès à une œuvre ou de l'utilisation d'une œuvre.

5.1.2 Les SGDN à MPT activées

Bien que SGDN soit un terme générique désignant une méthode qui sert à préciser le contenu et stipule les conditions de délivrance des licences, il semble que ce terme soit devenu récemment synonyme des SGDN qui utilisent les MPT. De plus en plus, les SGDN tablent sur les MPT pour gérer les droits qui accompagnent le contenu numérisé[77]. À partir de ce point-ci dans la présente étude ainsi que dans l'ensemble de la seconde étude, toute mention de SGDN fera référence aux SGDN à MPT activées.

Les SGDN ont la capacité de contrôler, de surveiller et de mesurer la plupart des utilisations d'une œuvre numérique. À cet égard, les SGDN peuvent être apparentés aux systèmes de dépistage et de comptabilisation des redevances en vertu desquels le titulaire de droits d'auteur a la possibilité d'assurer un suivi des utilisations et des paiements. Les SGDN mettent également à profit toute une gamme de modèles administratifs au-delà des ventes et des abonnements, notamment la délivrance de licences comportant des conditions et modalités variables. Par exemple, les SGDN permettent à un titulaire de droits d'auteur d'autoriser des clients éventuels à échantillonner un contenu numérisé en mode de démonstration. Les SGDN permettent également d'offrir des licences d'utilisation sur site adaptées au nombre d'utilisateurs simultanés ou reliées à un matériel spécifique. Les modalités d'utilisation peuvent prévoir une

75. KOSKINEN-OLSSON, *supra*, note 73, p. 4.
76. *Ibid*.
77. CUNARD, *supra*, note 11, p. 4.

utilisation limitée ou illimitée, ou un calcul du temps selon l'utilisation réelle[78]. La meilleure illustration de ce principe est sans doute l'exemple présenté dans la section qui suit.

5.1.2.1 Norme DOI

La Digital Object Identifier Foundation est une organisation internationale sans but lucratif qui œuvre à la conception d'un système d'identification international pour la propriété intellectuelle numérisée[79]. Cette fondation est un consortium d'organismes d'édition tels que Microsoft Corporation, l'Association of American Publishers et l'Alliance of European Music Rights Societies[80]. DOI (Digital Object Identifier ou identificateur d'objet numérique) se veut une norme volontaire dans le domaine de l'édition.

L'identification du contenu auquel les droits précisés par un SGDN sont affiliés est une condition préalable à l'application efficace des droits numériques. Des normes relatives aux identificateurs telles que ISBN, ISWC et ISRC ont été mises au point en vue de préciser diverses catégories d'œuvres matérielles. Le DOI est leur équivalent virtuel.

Le système DOI a recours à un répertoire central réparti. L'avantage particulier de ce système est sa capacité d'orienter les personnes à la recherche d'un élément de contenu particulier au moyen d'un identificateur DOI vers la destination qui détient ce contenu. Lorsqu'un utilisateur clique sur un DOI, le système fait parvenir un message au répertoire où l'adresse courante associée au DOI est inscrite. Les données d'emplacement sont transmises à l'utilisateur, ce qui permet la réorientation du fureteur vers la destination réelle associée au DOI. Ainsi, l'utilisateur verra soit le contenu même, soit de plus amples renseignements au sujet du fournisseur du contenu de même que les modalités d'obtention du contenu[81].

Une fois le contenu numérique identifié, le DOI établit la connexion vers une description de l'œuvre. La description, qui est

78. RISHER, *supra*, note 19, p. 5.
79. Voir en ligne (anglais seulement): <http://www.doi.org/overview/sys_overview_021601.html> (date de consultation: 2 avril 2002).
80. Une liste des organismes participants se trouve en ligne (anglais seulement): <http://www.doi.org/idf-member-list.html>.
81. *Supra*, note 75.

appelée métadonnée, comprend l'information sur la propriété du contenu. Les renseignements habituels comprennent des éléments tels que le nom de l'auteur, la date de publication et le territoire d'exploitation[82].

Dès que le contenu numérique est identifié et décrit, une série de règles quant à son utilisation doit être élaborée. Les droits numériques relèvent d'un certain nombre de catégories. Par exemple, les droits de transport comprennent les droits de copier, de transférer et de prêter. Les droits d'exécution comprennent les droits de jouer ou d'imprimer. Les droits connexes comprennent les droits d'extraire, d'intercaler et d'éditer. Un certain nombre de libellés des droits ont été mis au point pour décrire les divers droits[83]. Par exemple, une règle peut permettre qu'un élément du contenu soit imprimé, mais qu'il ne soit pas copié numériquement.

5.1.2.2 Langage XrML

XrML (eXtensible Rights Markup Language ou langage de marquage des droits) est un logiciel du langage des droits numériques mis au point au Centre de recherches de Xerox à Palo Alto sous la direction de M. Mark Stefik, Ph.D. XrML est un système automatisé qui permet aux titulaires de droits d'intercaler des règles dans un code/hypertexte[84]. Ce logiciel peut être utilisé dans la vente et la délivrance de licences relativement à des livres électroniques, des vidéos et de la musique numériques, des jeux informatiques, des logiciels et d'autres objets sur support numérique. XrML décrit les droits, les coûts et les conditions d'une œuvre. Des outils évolués d'établissement de règles sont en cours d'élaboration. Les logiciels tels que XrML de ContentGuard permettront l'établissement de règles plus complexes qu'auparavant[85]. Certaines caractéristiques élémentaires de ce logiciel comprennent ce qui suit[86]:

- Les droits sont associés à une partie d'un produit numérique.

---

82. Il a été mentionné que les technologies des métadonnées en sont à une étape évoluée de leur développement. Voir «Projet GDN de l'UE», s*upra*, note 60.
83. Voir STEFIK, *supra*, note 13, p. 140 et 141.
84. Voir en ligne (anglais seulement): http://xrml.org/about.asp (date de consultation: 8 avril 2002).
85. «Projet GDN de l'UE», s*upra*, note 60.
86. Liste disponible en ligne (anglais seulement): <http://www.intellect.vsu.ru/en/management/technology/xrml_e.htm> (date de consultation: 31 mars 2002).

- Chaque catégorie de droits d'utilisation jouit de ses propres transactions[87].

- Les transactions définissent les démarches que doit effectuer un dépôt lorsque les droits se concrétisent.

- Les droits sont décrits en termes de langage orienté machine.

- Les transactions sur les produits numériques exigent des restrictions selon les droits d'utilisation sous-jacents pour chaque produit.

- Les droits sur un produit numérique peuvent être modifiés, à condition que la modification soit autorisée par le propriétaire des droits.

- Chaque droit est relié à un jeu de conditions régissant l'utilisation d'un produit numérique.

- [Chaque] condition peut être de différents types: formule payable à l'utilisation, durée d'utilisation, type d'accès, type de filigrane numérique, type de dispositifs sur lesquels ces opérations sont exécutées, etc.

- Chaque produit numérique comporte ses propres spécifications qui définissent des catégories de droits pour chaque œuvre en totalité ou en partie.

Essentiellement, XrML a pour but de fournir aux titulaires de droits un outil servant à empêcher tout accès non autorisé à leur œuvre et toute utilisation non autorisée de leur œuvre.

87. Tableau disponible en ligne (anglais seulement): <http://www.intellect.vsu.ru/en/management/technology/xrml_e.htm> (date de consultation: 31 mars 2002):

Transfert des droits d'un utilisateur à un autre	Mouvement de produits d'un dépôt à un autre
Droits de reproduction	Impression et affichage de produits
Droits sur les produits dérivés	Utilisation de produits pour la création de nouveaux produits
Droits sur la gestion des fichiers	Création et restauration de copies réservées
Droits sur la configuration de systèmes	Installation de logiciels dans le dépôt

5.2 Incidences de politiques des SGDN

Certains croient que les SGDN deviendront sous peu une norme dans l'industrie. D'autres sont d'avis qu'ils le sont déjà[88]. Ceux qui affirment que les SGDN ne sont pas encore une norme de l'industrie font ressortir divers problèmes en suspens quant à leur avènement technologique, à la difficulté de déterminer des normes pertinentes et à d'autres pierres d'achoppement en matière d'interopérabilité[89]. Quoi qu'il en soit, l'évolution et l'utilisation éventuelle des SGDN comme méthode normalisée de protection numérique continuent de relever plutôt de l'inconnu.

Étant donné leur capacité de dégrouper les droits d'auteur en produits discrets et personnalisés, les SGDN sont gages d'une gamme élargie de choix de consommation et peut-être même d'une réduction des prix. Du même coup, l'adoption des SGDN offrirait également aux titulaires de droit un contrôle accru leur permettant de faire valoir leurs droits sur le contenu numérique, ce qui faciliterait l'accès légitime aux œuvres numérisées. À première vue, cela peut sembler être une situation de type gagnant-gagnant. Cependant, le degré de contrôle qu'obtiendraient les éditeurs sur les œuvres dans un environnement numérique pourrait également mener à des tentatives de faire appliquer et respecter les droits d'auteur selon des manières jamais envisagées jusqu'ici par les règles canadiennes du droit d'auteur. Par exemple, le phénomène pourrait permettre aux titulaires de droits d'auteur d'exclure diverses formes d'accès public à une œuvre numérisée. Cette possibilité très probable pourrait entièrement miner le fragile équilibre entre les droits privés et l'intérêt public que les règles du droit d'auteur cherchent à aménager.

5.2.1 Les SGDN pourraient miner l'équilibre du droit d'auteur entre les droits privés et l'intérêt public

Les technologies telles que XrML et d'autres logiciels de gestion des droits numériques ont la capacité d'établir les modalités de déli-

88. Voir M. EINHORN, «Digital Rights Management and Access Protection: An Economic Analysis», Congrès ALAI 2001. Voir aussi J. KAESTNER, «Law and Technology Convergence: Intellectual Property Rights», en ligne (anglais seulement): <http://www.europa.eu.int/information_society/newsroom/documents/drm_workingdoc.pdf> (date de consultation: 31 mars 2002). Il s'agit d'une étude préparée pour l'Union européenne. L'auteur y discute de nombreuses activités d'uniformisation en matière de protection du droit d'auteur. Voir aussi «Projet GDN de l'UE», *supra*, note 60. Cette étude contient un inventaire complet des projets relatifs aux SGDN.

89. Voir CUNARD, *supra*, note 11, p. 3. Voir aussi M. STEFIK, *supra*, note 13.

vrance de licences et la capacité technologique de contrôler les utilisations d'une œuvre bien au-delà des frontières du régime de droit d'auteur. Les SGDN présentent donc des défis profonds et ardus aux personnes qui souhaitent maintenir un régime de droit d'auteur équilibré. Comme l'indiquaient Burk et Cohen:

> Les industries du droit d'auteur ont également réussi à obtenir une protection juridique extrêmement vaste pour les systèmes de gestion des droits... La mise au point de systèmes de gestion des droits démontre avec puissance la capacité de la technologie à réguler les comportements... Cependant, comme l'ont déjà mentionné Larry Lessig et Joel Reidenberg, les normes techniques relèvent du champ de contrôle du concepteur et confèrent donc au concepteur le pouvoir de régir les comportements à propos de ce système... La conception de jeux de règles techniques, toutefois, n'est pas le seul apanage de l'État; en effet, elle est le plus souvent laissée aux parties privées. Dans le cas des systèmes de gestion des droits, les propriétaires de droits déterminent les règles qui sont intégrées aux contrôles technologiques. *En aménageant des contraintes techniques à l'accès à l'information numérique et à son utilisation, un propriétaire de droit peut efficacement surpasser les règles du droit sur la propriété intellectuelle... Les ramifications de ces avènements sont désolantes: Là où les contraintes technologiques se substituent aux contraintes juridiques, le contrôle sur la conception des droits à l'information se retrouve entre les mains des parties privées, lesquelles peuvent ou non honorer les politiques publiques qui animent les principes d'accès public tels que l'utilisation équitable*. [Traduction libre][90]

Ces auteurs et ceux qu'ils citent ne sont pas les seuls à souscrire à ce point de vue. Ce moment crucial est un motif récurrent dans l'œuvre de presque tout éminent chercheur en propriété intellectuelle qui écrit sur le sujet[91].

---

90. BURK et COHEN, *supra*, note 7, p. 49 (insistance ajoutée et notes de bas de page omises).

91. Voir, p. ex., Y. BENKLER, «Through the Looking Glass: Alice and the Constitutional Foundations of the Public Domain» (2001); J. BOYLE, «The Second Enclosure Movement» (2001); D. LANGE et J. LANGE-ANDERSON, «Copyright, Fair Use and Transformative Critical Appropriation» (2001); L. LESSIG, «The Architecture of Innovation» (2001); E. OSTROM et C. HESS, «Artifacts, Facilities & Content» (2001), extrait de la Duke Law Conference on the Public Domain, en ligne (anglais seulement): <http://law.duke.edu/pd/rcalcust.htm> (date de consultation: 8 avril 2002). Voir aussi BURK et COHEN, *supra*, note 7; J. FOLEY, «Comment: Enter the Library: Creating a Digital Lending Right»,

Lorsqu'une personne achète une copie d'une œuvre intégrée à un support physique, p. ex., en format de poche, sur DC ou sur vidéocassette, le titulaire du droit d'auteur n'a plus de contrôle sur la fréquence à laquelle l'œuvre est lue, écoutée ou visionnée par l'acheteur. Cependant, un SGDN peut restreindre le nombre de fois qu'une personne peut utiliser l'équivalent numérique de pareille œuvre.

De façon similaire, en vertu des règles canadiennes du droit d'auteur, dès qu'une œuvre a été publiée sous une forme particulière, le titulaire du droit d'auteur ne peut empêcher la publication ultérieure de l'œuvre sous cette forme[92]. Cela signifie, par exemple, que dans le cas d'un livre, d'un enregistrement sonore ou d'un enregistrement audiovisuel, dès qu'une personne acquiert légalement une copie de l'œuvre, l'acheteur peut prêter l'article ou le revendre à une autre personne. Cependant, un SGDN pourrait empêcher le transfert subséquent du format numérique de pareille œuvre par l'acheteur.

La législation canadienne sur le droit d'auteur contient également une défense d'utilisation équitable devant les réclamations pour violation du droit d'auteur lorsqu'une œuvre est utilisée pour fins d'étude privée, de recherche, de compte rendu, de critique ou de communication des nouvelles et lorsque les modalités d'utilisation sont équitables[93]. D'autres exceptions spécifiques existent dans le cas des établissements d'enseignement[94], des bibliothèques, musées et services d'archives[95], des programmes d'ordinateur[96], des incorpo-

(2001) 16 *Conn. J. Int'l L.* 369; D. GERVAIS, «Lock-it Up or License», 87-1, dans H. HANSON (éd.), *International Intellectual Property Law & Policy – Volume 6,* Huntington, Juris Publishing, 2001; J. GINSBURG, «Copyright and Control over New Technologies of Dissemination», (2001) 101 *Colum. L. Rev.* 1613; B. HUGENHOLTZ, «Copyright, Contract and Code: What Will Remain of the Public Domain», (2000) 26 *Brook. J. Int'l L.* 77; C. JEANNERET, «The Digital Millennium Copyright Act: Preserving the Traditional Copyright Balance», (2001) 12 *Fordham Intell. Prop. Media & Ent. L.J.* 157; J. LITMAN, «The Breadth of the Anti-Trafficking Provisions and the Moral High Ground», Congrès ALAI 2001; G. LUNNEY, «The Death of Copyright: Digital Technology, Private Copying and the Digital Millennium Copyright Act», (2001) 87 *V.A.L.R.* 813; K. KOELMAN, «The Protection of Technological Measures vs. the Copyright Limitations», Congrès ALAI 2001; D. NIMMER, «A Riff on Fair Use in the Digital Millennium Copyright Act», (2000) 148 *U. Pa. L. Rev.* 673; ainsi que M. PERRY et C. CHISIK, *supra*, note 5.

92. Le titulaire de droits d'auteur peut toutefois toujours empêcher la reproduction ultérieure de l'œuvre. Voir *Les Amusements Wiltron* c. *Mainville*, (1991) 40 C.P.R. (3d) 521 (C.S.), p. 532.
93. *Loi sur le droit d'auteur*, L.R. 1985, c. C-42, art. 29, 29.1 et 29.2, tels qu'amendés.
94. *Ibid.*, art. 29.3, 29.4, 29.5, 29.6, 29.7, 29.8, 29.9 et 30, tels qu'amendés.
95. *Ibid.*, art. 30.1, 30.2, 30.21, 30.3, 30.4 et 30.5, tels qu'amendés.
96. *Ibid.*, art. 30.6, tel qu'amendé.

rations incidentes[97], des enregistrements éphémères[98] et des enregistrements sonores[99]. Il est vrai que les tribunaux canadiens ont eu tendance à interpréter de manière étroite les exceptions à la violation du droit d'auteur[100]. Néanmoins – et il s'agit ici de l'aspect crucial – *l'exercice de toute exception présume de la capacité d'accéder à une œuvre*. Le SGDN qui empêche ou restreint grandement l'accès à une œuvre numérique rend impossible une capacité d'exercer toute exception autorisée par la loi et de bénéficier de ses avantages.

Même si les titulaires de droits souhaitaient concevoir le SGDN pour permettre aux utilisateurs de se prévaloir de l'une ou l'autre des exceptions susmentionnées touchant le droit d'auteur, à l'heure actuelle, ce scénario n'est pas réalisable sur le plan technologique. Les technologies requises pour concrétiser ce niveau de finesse juridique n'ont tout simplement pas été développées à ce jour[101]. De plus, le droit canadien est en soi chargé d'incertitudes marquées au sujet de la portée de certaines de ces exemptions[102], ce qui fait de leur «codification» un exercice hautement subjectif et donc une démarche plus susceptible d'avantager les titulaires de droits qui se prévalent des exceptions que les utilisateurs qui peuvent choisir de s'y remettre.

---

97. *Ibid.*, art. 30.7, tel qu'amendé.
98. *Ibid.*, art. 30.8 et 30.9, tels qu'amendés.
99. *Ibid.*, art. 80, tel qu'amendé.
100. Voir, p. ex., *Compagnie générale des établissements Michelin-Michelin & Cie* c. *Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleurs et travailleuses du Canada (TCA-Canada)*, [1997] 2 C.F. 306 (1re instance), p. 331, où le juge Teitelbaum affirme que «Les exceptions à la violation du droit d'auteur doivent être interprétées strictement» au moment d'envisager une défense reposant sur le principe du traitement équitable dans une poursuite mettant en jeu une réclamation de dommages-intérêts pour violation du droit d'auteur.
101. Voir CUNARD, *supra*, note 11. Voir aussi M. STEFIK, «Roundtable: Life, Liberty, and the Pursuit of Copyright», (1998) en ligne (anglais seulement): <http://theatlantic.com/unbound/forum/copyright/stefik1.htm> (date de consultation: 31 mars 2002). Stefik reconnaît les limites technologiques des SGDN et les problèmes éventuels pouvant en découler en ce qui a trait à l'utilisation équitable. Il offre deux suggestions pour contrer pareil effet négatif. D'abord, comme il l'affirme, la concurrence commerciale assurera que les consommateurs ont un accès équitable au matériel. Ensuite, il discute de l'instauration d'un régime de «licences pour utilisation équitable» [Traduction libre]. Les titulaires de droits d'auteur se fieraient à une tierce partie pour faire délivrer des licences aux personnes qui démontrent qu'elles comprennent les droits et limites de l'utilisation équitable. L'utilisateur aurait ensuite un accès libre à l'œuvre.
102. Par exemple, bon nombre de questions demeurent au sujet de la portée de l'applicabilité de l'exception fondée sur le principe de traitement équitable en matière de protection du droit d'auteur sur le contenu numérique. Voir S. HANDA, *Copyright Law in Canada*, Markham: Butterworth, 2002, p. 291 à 298.

5.2.2 Les SGDN peuvent donner lieu à des préoccupations au sujet de la vie privée des consommateurs

Afin de s'acquitter de leur fonction en propre, les SGDN recueillent, traitent et, parfois, emmagasinent des renseignements personnels[103]. Les SGDN peuvent également surveiller étroitement et dépister de près l'utilisation du contenu numérique[104]. En effet, les SGDN peuvent identifier les consommateurs et créer des profils qui précisent les habitudes de consommation de chaque consommateur. Bien que l'utilisation adéquate de pareils renseignements personnels puisse être positive pour les consommateurs qui souhaitent bénéficier de services personnalisés, l'énorme potentiel d'acquisition de renseignements personnels donne également lieu à de graves préoccupations quant à la vie privée[105].

5.2.3 Les SGDN peuvent entraîner des inconvénients pour les consommateurs

Les SGDN sont des outils très puissants qui donnent aux titulaires de droits d'auteur la capacité d'offrir des services personnalisés et de nouveaux modèles d'affaires. À ce titre, les SGDN promettent de nouvelles sources de revenus pour les propriétaires de contenu. Cependant, certains de ces nouveaux modèles d'affaires doivent toujours être testés sur le marché et, comme nous avons pu le constater récemment dans la présumée «révolution des sites .com», certains pourraient ne pas s'avérer viables[106]. Même si les modèles d'affaires des SGDN sont viables et génèrent de nouveaux avantages, ils sont également portés à créer de nouveaux fardeaux pour les consommateurs.

Afin d'obtenir toutes les œuvres qu'ils convoitent, les consommateurs pourraient être contraints d'utiliser un certain nombre de

---

103. L. BYGRAVE et K. KOELMAN, «Privacy, Data Protection and Copyright», dans B. HUGENHOLTZ (éd.), *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management*, La Haye: Kluwer Law International, 2000.
104. Il a été allégué que la Constitution américaine protège le droit à une lecture anonyme. Voir J. COHEN, «Right to Read Anonymously: A Closer Look at "Copyright Management in Cyberspace"», (1996) 28 *Conn. L. Rev.* 981. Pour un exposé sur l'anonymat en ligne dans le contexte canadien, voir I. KERR, «The Legal Relationship Between Online Service Providers and Users», (2001) 35 *Canadian Business Law Journal* 1 à 40.
105. BYGRAVE et KOELMAN, *supra*, note 103. Voir aussi J.J. BORKING, B.M.A. van ECK et P. SIEPEL, «Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector», La Haye: 1999, en ligne (anglais seulement): <http://www.ipc.on.ca/english/pubpres/papers/isat.htm>.
106. STEFIK, *supra*, note 13, p. 157.

systèmes d'information incompatibles. Cela pourrait imposer un fardeau technique et des coûts additionnels aux utilisateurs et devenir un obstacle à un accès facile au contenu en ligne[107].

Des pressions financières pourraient également se faire sentir. La Commission du droit d'auteur du Canada (CDA) a établi un prélèvement pour les supports d'enregistrement vierges fabriqués au Canada ou importés vers le Canada[108]. Si le contournement des droits d'auteur diminue considérablement à mesure que s'améliorent les technologies SGDN, il y a danger que la présence continue de pareil prélèvement se traduise par une double compensation des titulaires de droits, d'abord par le prélèvement même et ensuite à nouveau par les droits perçus par les SGDN.

6.0 L'AVENIR DES MPT

Ayant envisagé les récentes tendances en matière de MPT et de technologies SGDN, nous concluons notre première étude en jetant brièvement un coup d'œil sur l'avenir des MPT.

L'avenir regorge de points d'interrogation. Néanmoins, une chose qui est claire à partir des tendances récentes discutées précédemment, c'est que l'élaboration de SGDN à grande échelle exige la coopération d'un grand nombre de différents intéressés, y compris: i) les titulaires de droits d'auteur; ii) les exploitants de systèmes; iii) les fabricants de produits finals; et iv) les consommateurs. Ainsi, la réussite des nouvelles technologies SGDN exigera probablement la négociation d'accords parmi cette bande hétéroclite de groupes d'intérêts. Le processus de réalisation de normes et de protocoles acceptables pourrait, dans certains cas, s'échelonner sur plusieurs années. Par conséquent, l'adoption à grande échelle des SGDN pourrait être grandement retardée[109]. Il s'ensuit que l'adoption des MPT correspondantes pourrait également être considérablement repoussée. Ces délais pourraient mener à l'élaboration d'un nombre impossible à gérer de MPT isolées et provisoires de la part de ceux qui sont réticents à attendre la culmination du lent processus d'aménagement du consensus requis pour l'élaboration d'un nombre accru de SGDN généralisés. Une prolifération de MPT provisoires viendrait grandement diminuer l'interopérabilité entre les diverses technologies, phénomène que les consommateurs trouveraient frustrant et inacceptable.

107. *Ibid.*, p. 158.
108. *Tarif pour la copie privée, 2001-2002*.
109. CUNARD, *supra*, note 11, p. 3.

Bien que nous en soyons toujours à une étape où bon nombre de MPT existent et d'autres deviendront disponibles, la réussite des SGDN à grande échelle exige l'élaboration de systèmes d'information uniformes et interopérables. Trois approches possibles ont été proposées pour la création d'une architecture plus complète de protection de la copie. Ces approches sont les suivantes:

1) un jeu de technologies et d'obligations juridiques en cascade, selon lequel une MPT remettra seulement une œuvre protégée sous sa garde à une autre MPT lorsqu'elle obtient une assurance adéquate que la MPT en aval traitera l'œuvre de manière sécuritaire;

2) l'élaboration d'une architecture de MPT unique et complète pour le traitement des MPT qui comprenne des caractéristiques telles que le chiffrement, l'authentification, les filigranes, les mécanismes qui ne déchargeront que vers des sorties sécuritaires, et d'autres mécanismes du genre;

3) une exigence selon laquelle les titulaires de licences qui souhaitent mettre au point un produit dans un format particulier adopteraient une MPT correspondante par des liens vers des octrois de droits sur la propriété intellectuelle de la part de l'organisme de délivrance de licences sur ces technologies[110].

Même s'il est en principe possible que, un jour, l'une des propositions susmentionnées puisse mener à l'élaboration d'un SGDN à grande échelle parvenant à maintenir pour les droits d'auteur un fragile équilibre entre les droits privés et l'intérêt public[111], il va sans dire qu'aucune des propositions susmentionnées ne peut jamais empêcher le contournement éventuel des MPT. Néanmoins, il y a au moins deux approches générales que l'on estime pouvoir contribuer à atténuer la menace de contournement.

La première approche est d'ordre technologique. Dans le contexte de la gestion des droits numériques, on entend par *renouvellement* «le processus de délivrance d'un nouveau certificat au moyen de la même clé publique que pour le certificat antérieur» [Traduction

110. *Ibid.*, p. 10 et 11.
111. Malgré les pressions exercées par Stefik *et al.*, il vaut la peine de mentionner que très peu de chercheurs en propriété intellectuelle sont optimistes à propos de cette possibilité. Voir, p. ex., les personnes mentionnées précédemment, note 91.

libre]. Cela se veut un moyen de valider chaque interaction entre le dispositif d'exécution et l'œuvre protégée. Le certificat d'origine est obtenu par l'inscription d'un code d'enregistrement valide moyennant un paiement ultérieur. Cependant, compte tenu de la capacité de créer des certificats d'enregistrement frauduleux[112], un processus de validation des certificats sert à déterminer la fiabilité du certificat actuellement validé avant de le renouveler. Si le certificat est jugé invalide, soit par suite d'une altération ou d'une inclusion dans une liste de révocation des certificats[113], le certificat est révoqué plutôt que renouvelé. La révocation, dans ce contexte, renvoie à la capacité de désactiver un dispositif qui traite les œuvres assujetties au droit d'auteur si cet appareil a été piraté. La révocation des certificats empêche l'œuvre protégée d'être exécutée[114]. Le renouvellement et la révocation ont tous les deux leurs failles. Si le renouvellement se fait par voie de déchargements de logiciels, les utilisateurs peuvent être mécontents de devoir effectuer la mise à niveau. Ils peuvent également avoir des préoccupations au sujet de la vie privée et de la perte d'autonomie à l'égard de leur usage privé d'œuvres protégées par les règles du droit d'auteur[115]. La révocation est problématique dans la mesure où elle demeure sensible aux autres dispositifs de contournement qui masquent le fait que la mesure de protection technique a été piratée.

La seconde approche générale n'est pas de nature technologique mais bien de nature juridique. Cette approche comprend la

112. Un produit est «percé» lorsqu'un enregistrement de produit est «contrefait», c'est-à-dire que le processus de renouvellement est évité ou déjoué.

113. Une liste des certificats révoqués par suite de leur perçage ou de leur expiration.

114. Pour une explication plus approfondie à la fois du renouvellement et de la révocation dans le contexte de la gestion des droits numériques, voir le glossaire de la sécurité Internet d'Entrust (Entrust Internet Security Glossary), en ligne (anglais seulement): <http://www.entrust.com/security101/glossary.htm> (date de consultation: 8 avril 2002).

115. Cette pratique soulève la question de l'anonymat quant à élargir et à valoriser la commercialisation des idées et du contenu culturel. Afin d'encourager la participation au marketing des idées ou à leur diffusion au public (la base même d'une démocratie), les droits d'un individu à ne pas être associé publiquement à un élément particulier de contenu doivent être respectés. Voir, p. ex., A.W. BRANSCOMB, «Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces», (1995) 104 *Yale L.J.* 1639; A.M. FROOMKIN, «Anonymity and Its Enmities», (1995) *J. Online L.* art. 4; M.E. KATSH, «The First Amendment and Technological Change: The New Media Have a Message», (1990) 57 *Geo. Wash. L. Rev*. 1459; G.P. LONG, «Who Are You?: Identity and Anonymity in Cyberspace», (1994) 55 *U. Pitt. L. Rev.* 1177; et D.G. POST, «Pooling Intellectual Capital: Thoughts of Anonymity, Pseudonymity, and Limited Liability in Cyberspace», (1996) *U. Chi. Legal F*. 139.

création d'une interdiction sur le contournement d'une partie ou de la totalité des types de MPT (le tout accompagné d'une gamme circonscrite d'exceptions possibles)[116]. Cette approche est pleine d'autres difficultés qui seront examinées en profondeur dans notre seconde étude.

Avant de passer au contenu de la seconde étude, il est important de noter qu'une question fondamentale demeure en suspens, à savoir: *L'utilisation des MPT sera-t-elle aussi largement répandue que ce que l'on prévoit?*

Malheureusement, il n'y a aucune façon de prédire avec certitude la réponse à cette question puisque l'issue dépendra fort probablement de la réaction des consommateurs à l'univers dégroupé et payable à l'utilisation du contenu numérique à la fois en ligne et hors ligne. Et il est encore tôt pour se prononcer. Néanmoins, il faut se rappeler que, au début des années 1980, bon nombre d'entreprises qui ont vendu des applications logicielles utilisaient une forme de protection de la copie pour empêcher la copie des disques souples sur lesquels leurs applications étaient vendues. Une résistance massive des consommateurs face à cette approche a mené à l'abandon de cette MPT. Pourtant, les sociétés œuvrant dans le domaine des logiciels ont par la suite constaté que le risque à propos de la copie illicite se situait selon des limites acceptables[117].

Si les consommateurs trouvent les MPT fastidieuses, démesurément restrictives ou trop coûteuses à utiliser, ils pourraient en fait s'investir là où ça clique, forçant les fournisseurs de contenu à atténuer le recours aux MPT. C'est particulièrement vrai si l'utilisation des MPT plus nouvelles crée des problèmes de compatibilité qui empêchent le nouveau contenu (protégé par les MPT les plus à jour) d'être lu sur de l'équipement plus ancien, ou encore le contenu plus ancien (n'intégrant pas les plus récentes MPT) d'être lu sur de l'équipement plus nouveau, les deux scénarios constituant des issues probables si les MPT évoluent en marge d'un format numérique unique et cohérent à un rythme rapide.

---

116. Tel que discuté relativement à fond dans notre seconde étude, les variantes de cette approche ont déjà été adoptées dans des pays tels que les États-Unis et l'Union européenne.
117. P.B. HUGENHOLTZ, «Code As Code, Or The End Of Intellectual Property As We Know It», (1999) 6:3 *Maastricht J. of European & Comparative L.* 308. Voir en ligne (anglais seulement): <http://www.ivir.nl/publications/hugenholtz/MAASTRIC.DOC> (date de consultation: 2 juillet 2002).

Une importante observation doit être signalée à l'égard de toute tentative de prédire l'avenir des MPT. Compte tenu de l'incertitude d'un si grand nombre de facteurs nécessaires à la réussite à long terme de l'utilisation des MPT comme moyen de protéger les droits à la propriété intellectuelle d'un contenu numérique, il semblerait qu'une grande prudence doive être manifestée de la part des décideurs qui étudient une intervention juridique immédiate à ce qui demeure une technologie relativement méconnue, voire à peine naissante. Les ramifications de politiques de l'approche juridique exposée dans notre seconde étude reposeront dans une certaine mesure sur cette observation.