Université de Neuchâtel

Les mesures techniques de protection en droit d'auteur

Sabrina Migliozzi

Mémoire de Master

Rédigé sous la direction du Professeur Vincent Salvadé

19 décembre 2014

TABLE DES MATIERES

LISTE DES ABREVIATIONS

17 USC	Title 17 of the United States Code : Copyrights
al.	alinéa
art.	article
cf.	confer
CP	Code pénal suisse du 21 décembre 1937 ; RS 311.0
Directive sur le droit d'auteur	Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur *l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information*.
DMCA	Digital Millennium Copyright Act of 1998 ; 17 USC
DRMS	Digital Rights Management System
DRM	Digital Rights Management
EFF	Electronic Frontier Foundation
éd.	éditeur (s)
édit.	édition
etc.	et caetera
GND	Gestion Numérique des Droits
INDICARE	Informed Dialogue about Consumer Acceptability of DRM Solution in Europe
IPI	Institut fédéral de la Propriété Intellectuelle
IFPI	International Federation of Phonographic Industry

LDA	Loi fédérale sur le droit d'auteur et les droits voisins du 9 octobre 1992 ; RS 231.1
lit.	littera
no.	numéro
ODAu	Ordonnance sur le droit d'auteur et les droits voisins du 26 avril 1993 ; RS 231.11
OMET	Observatoire des Mesures Techniques
OMPI	Organisation Mondiale de la Propriété Intellectuelle
p.	page
ss.	suivant(e)s
UE	Union Européenne
vol.	volume
WCT	Traité de l'OMPI du 20 décembre 1996 sur le droit d'auteur (WIPO Copyright Treaty) ; RS 0.231.151
WPPT	Traité de l'OMPI du 20 décembre 1996 sur les interprétations et exécutions et les phonogrammes (WIPO Performances and Phonograms Treaty) ; RS 0.231.171.1
XCP	Extended Copy Protection

BIBLIOGRAPHIE

I. DOCTRINE

BARRELET D., EGLOFF W., *Le nouveau droit d'auteur : commentaire de la loi fédérale sur le droit d'auteur et les droits voisins*, 3e édit., Berne 2008 (cité : BARRELET/EGLOFF).

DE WERRA J., *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)*, 2001 (disponible sur le site Internet ALAI-USA: http://www.alai-usa.org/2001_conference/Reports/dewerra.doc; cité : DE WERRA, *Legal system*).

DE WERRA J., *La protection juridique contre le contournement des mesures techniques,* in : Internet 2003, CEDIDAC, Lausanne 2004, p. 275ss (cité : DE WERRA, *Protection juridique*).

ERBER G., *Proprietary Digital Rights Management Systems and music-downloads : obstacles for innovation from a competition policy perspective*, July 2007 (disponible sur le site Internet Social Science Research Network : http://ssrn.com/abstract=1475059; cité : ERBER).

GASSER U., *Legal frameworks and technological protection of digital content : moving forward towards a best practice model*, 2006 (disponible sur le site Internet Social Science Research Network : http://papers.ssrn.com/abstract=908998; cité : GASSER).

GASSER U., BEGUE G. R., *iTunes : Some observations after 500 millions downloaded songs*, Berkman Center for Internet & Society at Harvard Law School, 2005 (disponible sur le site Internet de Berkman Center for Internet & Society : http://cyber.law.harvard.edu/BerkmanPress/iTunes_August_update_final%5B1%5D.pdf; cité : GASSER, BEGUE).

GASSER U., PALFREY J., *DRM-protected music : interoperability and eInnovation*, Berkman Publication Series, November 2007 (disponible sur le site Internet de Berkman Center for Internet & Society : http://cyber.law.harvard.edu/interop/pdfs/interop-drm-music.pdf; cité : GASSER, PALFREY).

GILLIERON P., *La gestion numérique des droits (DRM) dans les législations nationales*, in : sic ! 2004, p. 281 (cité : GILLIERON).

JACCARD M., HEUMANN J., in : *Propriété intellectuelle*, Commentaire romand (DE WERRA, GILLIERON éd.), Bâle 2013 (cité : CR PI JACCARD/HEUMANN).

JONES A., SUFRIN B., *EU Competition Law : Texts, cases and materials*, Oxford University press, 5th ed., Oxford 2014 (cité : JONES, SUFRIN).

HADLERMAN A. J., FELTEN, E. W., *Lessons from the Sony CD DRM episode* (extended version), February 2006 (disponible sur le site Internet de Halderman A. J. : https://jhalderm.com/pub/papers/rootkit-sec06-full.pdf; cité : HALDERMANN, FELTEN, *Lessons from Sony episode*).

HADLERMAN A. J., FELTEN, E. W., *Digital Rights Management, spyware, and security*, IEEE Security & Privacy, vol. 4, January/February 2006, p. 18-23 (disponible sur le site Internet de Halderman A. J. : https://jhalderm.com/pub/papers/drm-sp06.pdf; cité : HALDERMANN, FELTEN, *DRM, spyware, security*).

INSTITUT FEDERAL DE LA PROPRIETE INTELLECTUELLE, *Le droit d'auteur à l'ère du numérique : impasse ou autoroute ?*, Berne 2006 (cité : Brochure IPI).

LA BELLE M., *The rootkit debacle : the latest chapter in the story of the recording industry and the war on musical piracy*, Denver University law Review, Vol. 84, No. 1, 2006 , p. 79 (disponible sur le site Internet Social Science Research Network : http://ssrn.com/abstract=1564903; cité : LA BELLE).

MULLIGAN D. K., PERZANOWSKI A. K., *The magnificence of the disaster : reconstructing the Sony BMG rootkit incident*, 2006 (disponible sur le site Internet Social Science Research Network : http://ssrn.com/abstract=1072229; cité : MULLIGAN, PERZANOWSKI).

SALVADE V., *Entre mesures techniques et redevances pour la copie privée*, in : *Jusletter* 17 mars 2007 (cité : SALVADE).

SESSA S., *Le téléchargement d'œuvres sur Internet : légiférer ou ne pas légiférer ?*, Mémoire de master, Université de Neuchâtel, 2012 (cité : SESSA).

SHARPE N. F., AREWA O. B., *Is Apple playing fair ? Navigating the iPod FairPlay DRM controversy*, Northwestern public law research paper No. 07-18, in : Northwestern Journal of Technology and Intellectual Property, vol. 5, 2007, p. 331 (disponible sur le site Internet Social Science Research Network : http://ssrn.com/abstract=997159; cité : SHARP, AREWA).

II. TRAVAUX PREPARATOIRES

Message du 10 mars 2006 concernant *l'arrêté fédéral relatif à l'approbation de deux traités de l'Organisation Mondiale de la Propriété intellectuelle et concernant la modification de la loi sur le droit d'auteur* (cité : MCF 2006).

DFJP – *Rapport explicatif relatif à la modification de la loi fédérale sur le droit d'auteur et les droits voisins*, 2004 (cité : Rapport explicatif).

DFJP - *Rapport sur les résultats de la procédure de consultation relative à la révision partielle de la loi sur le droit d'auteur*, Berne, mai 2005 (cité : Rapport procédure de consultation).

III. SITES INTERNET

ALAI-USA : www.alai-usa.org.

Apple Inc. : www.apple.com.

Berkman Center for Internet & Society : www.cyber.law.harvard.edu.

Blog personnel de Mark Russinovich : http://blogs.technet.com/b/markrussinovich/.

Bloomberg : www.bloomberg.com.

Business Insider : www.uk.businessinsider.com.

DEFCON conference : www.defcon.org.

Electronic Frontier Foundation : www.eff.org.

HADOPI : http://www.hadopi.fr.

Halderman A. J. : www.jhalderm.com

IFPI : www.ifpi.org.

Mac Daily News : www.macdailynews.com.

Roughly Drafted Magazine : www.roughlydrafted.com.

Scribd. : www.scribd.com.

Social Science Research Network : www.ssrn.com.

Zefix : www.zefix.ch.

IV. RAPPORTS

Rapport d'activité de l'OMET : période du 1er juillet 2008 au 30 juin 2011 (cité : Rapport OMET).

Rapport de l'IFPI, *Digital music report*, 2006 (disponible sur le site Internet de l'IFPI : http://www.ifpi.cz/wp-content/uploads/2013/03/Digital-Music-Report-2006.pdf; cité : IFPI rapport 2006, consultation le 24 octobre 2014).

Federal Register/ Vol. 79, n° 180/ Wednesday, September 17, 2014 / Proposed Rules – *Exemption to prohibition on circumvention of copyright protection systems for access control technologies*, p. 55687 (cité: Federal Register).

Electronic Frontier Foundation, *Unintended consequences : sixteen years under the DMCA*, September 2014 (disponible sur le site Internet de l'Electronic Frontier Foundation : http://www.eff.org - rubrique Our Work ; cité : rapport EFF).

INDICARE, *Digital music usage and DRM : results from a European consumer survey*, May 24, 2005 (cité : INDICARE music survey).

INDICARE, *Digital video usage and DRM : results from a European consumer survey*, February 23, 2006 (cité : INDICARE video survey).

INTRODUCTION

Depuis les années nonante, le passage à l'ère du numérique apporte un vent de nouveauté où personne n'est mis à l'écart, la technologie se mettant au service de la communication et du partage. La société est projetée dans un univers où le progrès avance à une vitesse fulgurante, sans jamais s'arrêter.

Dans une telle dimension, chacun doit pouvoir trouver son compte et sauvegarder ses intérêts. Il en est notamment ainsi pour les titulaires de droits d'auteur dont les œuvres sont numérisées et se destinent à se retrouver tôt ou tard sur Internet, à leur grand dam. En principe, les auteurs bénéficient d'un monopole atténué sur leur œuvre, dans le sens où ils sont titulaires de tous les droits, sous réserve de certaines exceptions en faveur du public. Malheureusement, dans un environnement où les possibilités de reproduction et de diffusion sont décuplées, il devient impossible de garder le contrôle sur l'usage de ces œuvres - raison pour laquelle les auteurs se sont armés de mesures techniques de protection visant la lutte contre les actes de piratage. Bien que très complexes, ces systèmes contiennent de nombreuses failles qui, grâce à la rapidité du Web, ne demeurent jamais très longtemps inexploitées.

Une protection juridique s'est avérée nécessaire afin de continuer à encourager l'esprit de création et d'innovation, ou plus généralement le patrimoine culturel. C'est ce qu'a fait l'OMPI en adoptant deux traités internationaux qui introduisent pour la première fois l'interdiction de contourner les mesures techniques protégeant une œuvre. Ces règles ont ensuite été reprises par les législateurs nationaux en raison de leurs obligations internationales.
Avant cela, le sujet d'une protection juridique des mesures techniques était passablement contesté. Les milieux en cause faisaient part de leurs préoccupations, notamment celles relatives aux risques d'abus. Nous verrons par la suite que les Etats se sont dotés de solutions particulièrement différentes qui n'offrent finalement pas de protection uniforme à l'échelle internationale.

Il existe parfois des cas où la réalité prend une direction diamétralement opposée à celle avancée par la théorie. C'est le cas des DRMS. Initialement pensés pour sauvegarder les intérêts des auteurs, ils ont finalement été exploités à d'autres fins aux conséquences déplorables. Plusieurs entités se sont hasardées à analyser leur impact au sein de la société et les résultats ne sont pas réjouissants pour le futur.

Mais c'est à la lumière de deux grandes affaires qui mettent en évidence les dérives des DRMS que le lecteur saisira la face cachée de ces technologies. Les DRMS ont en effet été vivement critiqués pour avoir servi des pratiques anticoncurrentielles, mais également pour avoir causé une atteinte aux droits des consommateurs. L'absence d'interopérabilité se situe au cœur du débat, car dans un monde largement connecté, la compatibilité des systèmes constitue la clé d'un bon fonctionnement. Les détenteurs de cette clé ne semblent pourtant pas enclins à la partager, au détriment du public.

Dans la première partie, nous commencerons par présenter le cadre légal des mesures techniques. Il s'agira de voir comment la Suisse, l'Union européenne et les Etats-Unis ont transposé les « Traités Internet » de l'OMPI au sein de leur droit national. Nous constaterons les disparités de ces régimes. Nous aborderons également les raisons pour lesquelles les DRMS sont actuellement controversés.
La deuxième partie sera quant à elle axée sur un aspect plus pratique, notamment avec le dernier chapitre, ce qui permettra de nous projeter dans la réalité et de voir comment les DRMS ont été utilisés. Trois rapports y seront analysés, mettant en évidence d'une part les conséquences inattendues des DRMS et, de l'autre, l'intérêt du public pour les DRMS. Nous terminerons par une analyse plus détaillée de deux exemples concrets concernant les sociétés Sony BMG et Apple, dont les technologies respectives ont toutes deux été la cible des détracteurs des DRMS.

PARTIE 1 – LES MESURES TECHNIQUES DE PROTECTION & LA THEORIE

1. Définitions

1.1. Les DRMS et les mesures techniques de protection

A titre liminaire, il est utile de rappeler la notion *d'œuvre* puisqu'il s'agit de l'objet spécifiquement protégé par les mesures techniques de protection efficaces. Au sens de la LDA, l'œuvre est définie comme « toute création de l'esprit, littéraire ou artistique, qui a un caractère individuel » et ceci quelles qu'en soit la valeur ou la destination (art. 2 al. 1 LDA). Il convient de remarquer que les logiciels d'ordinateurs sont considérés comme des œuvres (art. 2 al. 3 LDA), mais sont parfois exclus de certaines règles (par exemple le droit à la copie privée, art. 19 al. 4 LDA). De plus, la loi couvre également des genres particuliers d'oeuvres, à savoir les oeuvres dérivées et les recueils (art. 3 et 4 LDA).

La protection du droit d'auteur dans l'environnement numérique est garantie par plusieurs instruments dont le tout forme la *gestion numérique des droits* ou le *digital rights management*. Plus communément connus sous l'acronyme de GND ou DRMS, ils désignent « l'ensemble des moyens technologiques gouvernant le processus d'exploitation autorisée des contenus numériques »[1]. Ces moyens technologiques englobent deux instruments distincts : les mesures techniques de protection et l'information sur le régime des droits[2].
Les mesures techniques de protection sont généralement définies comme « [u]ne technologie, un dispositif ou un composant qui, dans le cadre normal de son fonctionnement, est destiné à empêcher ou à limiter certains actes d'utilisation d'une œuvre non autorisés par les titulaires de droits. Il peut s'agir, par exemple, d'un dispositif anti-copie ou d'un mécanisme de contrôle d'accès »[3].
L'information sur le régime des droits est un tatouage numérique inséré à l'œuvre numérisée[4] qui identifie notamment les titulaires de droit et renseigne sur les conditions et les modalités d'utilisation de l'œuvre. De ce fait, les DRMS constituent de véritables boucliers pour la sauvegarde des droits dans l'univers numérique.

1.2. Les types de mesures techniques de protection

Généralement, les mesures techniques de protection se divisent en deux catégories : les systèmes de contrôle *d'accès* à l'œuvre et les dispositifs contrôlant *l'usage* de l'œuvre[5].

[1] SALVADE, p. 2 et la doctrine citée.
[2] SESSA, p. 13.
[3] Notion reprise du glossaire figurant sur le site Internet de l'HADOPI : http://www.hadopi.fr/glossaire (consultation le 30 septembre 2014).
[4] SESSA, p. 13 et voir également l'art. 12 ch. 2 WCT.
[5] DE WERRA, *Legal system*, p. 4.

1.2.1. Les mesures techniques contrôlant l'accès à l'œuvre

Cette catégorie de mesures empêche l'accès à l'œuvre. A titre illustratif, DE WERRA explique que cela est comparable à une porte fermée à clé, bloquant ainsi l'accès à la pièce où se trouve l'œuvre – en l'occurrence, un livre. Cette image parle d'elle-même : il faut forcer la porte pour accéder au livre, donc contourner les mesures de protection mises en place pour accéder à l'œuvre[6]. Cette technique vise principalement à empêcher l'accès non autorisé à du contenu numérique.

De manière concrète, une telle mesure serait, par exemple, le code d'accès au compte client iTunes. En principe, seule l'identification de l'utilisateur par un nom et un mot de passe permet d'accéder au répertoire de musique. Trouver un moyen permettant de télécharger des titres, sans devoir passer par l'étape « identification » revient à forcer la porte protégeant le livre.

La question de savoir si les dispositifs contrôlant l'accès à une œuvre peuvent aussi bénéficier de la protection légale du droit d'auteur est grandement débattue en doctrine. Le plus souvent, ce ne sera pas l'auteur lui-même qui contrôlera l'accès à l'œuvre, mais un fournisseur de service, comme par exemple une plateforme de téléchargements payante. Le processus d'identification vise alors à protéger le patrimoine du fournisseur de service et empêcher que des internautes accèdent à du contenu sans payer. De ce fait, est-ce qu'il mérite d'être protégé en vertu du droit d'auteur ? Cela reste discutable.
En vertu du droit suisse, SALVADE signale que « l'accès à l'œuvre n'est nullement une utilisation réservée à l'auteur par la loi »[7]. De plus, le code pénal protège déjà largement le patrimoine du fournisseur en application des articles 150, 150bis, 143 et 143bis CP[8]. Ces dispositions sanctionnent non seulement la soustraction de données et l'accès indu à un système informatique, mais également l'obtention frauduleuse d'une prestation et la fabrication et mise sur le marché d'équipements servant à décoder frauduleusement des services cryptés. Sur la base de ces deux considérations, l'avis de la doctrine qui estime que « l'arsenal juridique suisse existant, à savoir les articles 150 ou 150bis CP, aurait été suffisant afin de protéger les titulaires de droit sous l'angle du contrôle d'accès à l'œuvre »[9] est justifiable.

Nous verrons que la solution adoptée par les législateurs nationaux diffère selon les pays et certains systèmes juridiques protègent les dispositifs de contrôle d'accès de manière privilégiée.

1.2.2. Les mesures techniques contrôlant l'usage de l'œuvre

Souvent qualifiée de « dispositif anti-copie » dans la littérature, cette dénomination se révèle être inadéquate, étant donné que ces mesures empêchent également d'autres actes que la reproduction. Certains dispositifs visent à rendre impossible la mise à disposition d'un contenu en ligne ou à rendre inaptes certaines vidéos au streaming[10].

BARRELET et EGLOFF remarquent que ce type de mesures techniques vise à empêcher l'exercice d'une partie des droits exclusifs d'utilisation prévus par le droit d'auteur. Ceux-ci incluent le droit de reproduction, de distribution, de représentation, de mise à disposition et de diffusion (art. 10 al. 2 LDA)[11].

---

[6] DE WERRA, *Legal system*, p. 4.
[7] SALVADE, p. 5.
[8] CR PI JACCARD/HEUMANN, art. 39a LDA n°18 et la doctrine citée.
[9] Idem.
[10] DE WERRA, *Legal system*, p. 5.
[11] BARRELET/EGLOFF, art. 39a LDA n°7.

2. Le cadre légal

2.1. Au niveau international : les « Traités Internet » de l'OMPI

L'environnement technologique a poussé les créateurs, producteurs et autres titulaires de droits à protéger les œuvres publiées sous forme numérique. Les DRMS nécessitent une protection juridique car ils ne demeurent que peu de temps inviolés, les pirates informatiques trouvent en effet rapidement le moyen de neutraliser la sécurité mise en place. C'est ainsi que les « Traités Internet » ont été adoptés lors de la Conférence diplomatique qui s'est déroulée à Genève en décembre 1996 sous l'égide de l'OMPI. Il s'agit du traité sur le droit d'auteur (WCT) et du traité sur les droits voisins (WPPT). Ces textes instituent des minimas de protection que les Etats membres s'engagent à respecter en vertu de leur droit national.

C'est à l'auteur ou au titulaire de droits voisins de décider s'il désire prévoir une mesure technique de protection sur son œuvre. Les droits protégés peuvent être tant de nature économique que morale[12].

2.1.1. Les articles-clés : 11 WCT et 18 WPPT

Les deux traités contiennent chacun une disposition relative aux mesures techniques de protection; celles-ci pouvant être lues en parallèle compte tenu de leur similitude. Elles instaurent une protection juridique contre tout acte de contournement des mesures techniques utilisées par le titulaire de droits d'auteur ou de droits voisins.

Art. 11 WCT – Obligations relatives aux mesures techniques	**Art. 18 WPPT – Obligations relatives aux mesures techniques**
Les Parties contractantes doivent prévoir une protection juridique appropriée et des **sanctions juridiques efficaces** contre la neutralisation des mesures techniques **efficaces** qui sont mises en œuvre par les auteurs **dans le cadre de l'exercice de leurs droits** en vertu du présent traité ou de la Convention de Berne et qui restreignent l'accomplissement, à l'égard de leurs œuvres, **d'actes qui ne sont pas autorisés** par les auteurs concernés ou permis par la loi.	Les Parties contractantes doivent prévoir une protection juridique appropriée et des **sanctions juridiques efficaces** contre la neutralisation des mesures techniques **efficaces** qui sont mises en œuvre par les artistes interprètes ou exécutants ou les producteurs de phonogrammes **dans le cadre de l'exercice de leurs droits** en vertu du présent traité et qui restreignent l'accomplissement, à l'égard de leurs interprétations ou exécutions ou de leurs phonogrammes, **d'actes qui ne sont pas autorisés** par les artistes interprètes ou exécutants ou les producteurs de phonogrammes concernés ou permis par la loi.

[12] GASSER, p. 9.

2.1.2. Les quatre éléments essentiels

Avant tout, il faut noter que la notion de *mesures techniques de protection* n'est pas définie par les « Traités Internet ». L'OMPI a préféré un « terme technologiquement neutre » pour rester compatible avec les évolutions de la technologie[13]. Les législateurs nationaux disposent alors d'une large marge de manœuvre quant à la sélection des dispositifs protégés[14].

Les articles 11 WCT et 18 WPPT contiennent quatre éléments essentiels (exposés ci-dessous) sur lesquels les législateurs nationaux doivent se fonder pour transposer ces dispositions dans leur droit.

a. Notion d'efficacité

Les mesures techniques sont protégées uniquement si elles sont *efficaces*, c'est la première condition. Le concept d'efficacité n'étant pas défini par les « Traités Internet », il incombe aux législateurs de déterminer leur propre conception de la *mesure efficace.*

b. La mesure technique de protection doit être utilisée par des titulaires de droit dans l'exercice d'un droit garanti par les traités de l'OMPI ou la Convention de Berne

Cette condition doit se comprendre dans le sens suivant : la mesure technique doit protéger du *contenu* qui bénéficie de la protection du droit d'auteur ou des droits voisins – soit une œuvre, une prestation, etc. A contrario, les art. 11 WCT et 18 WCT ne s'appliqueront pas aux mesures techniques qui protègent du contenu qui n'est pas couvert par le droit d'auteur ou les droits voisins. Cela concerne les œuvres et prestations tombées dans le domaine public et le contenu qui n'entre pas dans le champ d'application du droit d'auteur ou des droits voisins[15].

c. La mesure technique de protection doit être utilisée dans le but d'empêcher des actes qui ne sont pas autorisés par l'auteur ou par la loi

Cette troisième condition est liée à la deuxième condition susmentionnée. Ainsi, il faut comprendre le tout comme suit : non seulement la mesure technique doit *protéger du contenu* qui soit couvert par le droit d'auteur ou les droits voisins, mais elle doit aussi avoir pour *fonction d'empêcher des actes* qui ne soient pas autorisés par la loi ou par le titulaire de droits lui-même. En d'autres termes, la mesure technique doit éviter que des droits protégés soient violés.

Cette condition ouvre la porte aux exceptions au droit d'auteur, en vertu desquelles le public peut utiliser une œuvre sans autorisation – l'utilisation de l'œuvre est *tolérée*. Il est donc possible de neutraliser une mesure technique si le but est de faire une utilisation tolérée (par la loi ou par le titulaire de droits s'il a donné son accord) – par exemple l'usage privé en droit suisse (art. 19 al. 1 LDA).

d. Des sanctions juridiques efficaces

Les « Traités Internet » commandent aux Etats d'adopter des sanctions juridiques efficaces. Cette notion n'étant pas définie par l'OMPI, les législateurs nationaux sont entièrement libres quant aux poursuites juridiques qu'ils entendent appliquer.

---

[13] GASSER, p. 8 et voir notes de bas de page n°9 et 10.
[14] DE WERRA, *Legal system*, p. 9.
[15] DE WERRA, *Legal system*, p. 11.

2.2. En Suisse : l'article 39a LDA

2.2.1. La révision de la loi sur le droit d'auteur

En 2008, la Suisse a ratifié les « Traités Internet ». C'est donc pour se conformer à ses obligations internationales qu'elle a entrepris la révision de la loi sur le droit d'auteur (LDA), car il était primordial à cette époque d'adapter la loi aux nouveautés technologiques. Pour se faire, la révision a reposé sur trois piliers principaux : la reconnaissance du droit de mise à disposition sur Internet des œuvres et d'autres objets protégés, l'interdiction de contourner les mesures techniques et la protection des informations électroniques permettant d'identifier les œuvres[16].
D'autres modifications ont également été adoptées parmi lesquelles l'introduction d'une exception en faveur des personnes handicapées (art. 24c LDA)[17].

Même si la nécessité d'adapter la LDA semblait incontestable, la proposition d'introduire une protection juridique des mesures techniques a suscité de vives discussions dans les milieux concernés (par exemple l'industrie du divertissement, les associations de consommateurs ou des partis politiques). Lors de la procédure de consultation, certains groupes émettaient déjà des craintes quant à « [...] un usage abusif de la protection des mesures techniques pour court-circuiter les restrictions au droit d'auteur »[18]. En outre, les archivistes et bibliothécaires revendiquaient une exception en leur faveur qui leur permettrait de copier les œuvres sur des supports à des fins de conservation[19]. Le challenge était de taille pour le législateur, car il devait satisfaire des intérêts divergents et assurer l'équilibre de la loi[20].

2.2.2. Le principe : interdiction de contournement des mesures techniques de protection efficaces et interdiction des actes préparatoires

La loi dispose qu'« [i]l est interdit de contourner les mesures techniques efficaces servant à la protection des œuvres et d'autres objets protégés » (art. 39a al. 1 LDA).

La doctrine précise que les mesures techniques sont protégées uniquement si elles portent sur du contenu couvert par la LDA (œuvres et autres objets protégés)[21]. Cela renvoie à la condition no. 2 décrite ci-dessus relative aux WCT et WPPT.

a. Notion de mesures techniques de protection

Selon l'art. 39a al. 2 LDA, toute technologie ou dispositif, de nature électronique ou mécanique, dont la fonction est de contrôler l'accès à l'œuvre ou limiter certaines utilisations constitue une mesure technique de protection[22].

b. Notion d'efficacité

Les mesures techniques de protection sont *efficaces* lorsqu'elles sont « [...] destinées et propres à empêcher ou à limiter les utilisations non autorisées d'œuvres et d'autres objets protégés » (art. 39a al.

16 MCF 2006, p. 3264.
17 MCF 2006, p. 3305.
18 Rapport procédure de consultation, p. 9.
19 Idem.
20 Brochure IPI, p. 28-29.
21 BARRELET/EGLOFF, art. 39a LDA n°3.
22 BARRELET/EGLOFF, art. 39a LDA n°7.

2 LDA). Le Message du Conseil fédéral précise que « la protection ne dépend pas du type de technologies ou de dispositifs utilisés, mais de leur finalité. [...] Elles doivent donc avoir un effet »[23]. Cela renvoie à la condition no. 3 décrite ci-dessus relative aux WCT et WPPT.
A contrario, lorsqu'elles visent à empêcher ou limiter des utilisations *autorisées*, elles ne sont *pas efficaces* : le contournement est alors autorisé (voir 39a al. 4 LDA). Par exemple, le DRMS qui limite le nombre de copies d'un CD ne constitue pas une mesure efficace étant donné que la copie privée est autorisée (en vertu de l'art. 19 al. 1 LDA).

Malgré le texte de la loi, la notion d'efficacité demeure relativement vague et il s'agit de consulter la doctrine pour en trouver une interprétation convaincante. Celle-ci a développé la *théorie de l'utilisateur moyen* : « [u]ne mesure est efficace lorsqu'elle empêche un consommateur moyen ou un utilisateur moyen d'utiliser ou de reproduire une œuvre ou une prestation protégée. Même si une personne disposant de connaissances particulières parvient à contourner les mesures techniques, celles-ci continuent à être efficaces au sens de la loi »[24].

Certains auteurs soulignent que l'utilisateur moyen se destine à devenir de plus en plus expert en matière de technologie, notamment par une utilisation intensive d'Internet. De ce fait, ce critère devra être adapté (par la jurisprudence) à la réalité afin de respecter la volonté du législateur[25].

c. Le premier comportement interdit : le contournement

Une personne contourne une mesure technique lorsqu'elle commet « tout acte et toute manipulation technique qui rendent inefficace la mesure technique et qui permet ainsi l'utilisation d'une œuvre ou d'une prestation protégée »[26]. Si le dispositif de protection est contourné, le lésé peut ainsi déposer une plainte pénale (art. 69a LDA).

Le Message du Conseil fédéral explique que dans la plupart des cas, le contournement de la mesure technique va être suivi d'une violation du droit d'auteur ; donc le contournement devient un acte préparatoire à la violation[27]. En effet, la protection mise en place sera généralement neutralisée afin de faire une utilisation non autorisée de l'œuvre. Par conséquent, il est nécessaire d'interdire tout acte de contournement, ceci afin d'assurer un niveau élevé de protection aux mesures techniques. S'il s'avère ensuite que le contournement a servi à une utilisation autorisée, alors la protection juridique de la mesure technique tombe[28].

d. Le deuxième comportement interdit : les actes préparatoires

L'art. 39a al. 3 LDA prévoit l'interdiction des actes préparatoires, bien que cela ne soit pas commandé par les « Traités Internet ». Le droit suisse confère donc une protection des mesures techniques qui va au-delà du minimum requis par l'OMPI.
Il s'agit de tous les comportements pouvant aider d'une manière ou d'une autre à contourner des mesures techniques. Il est alors interdit de fabriquer, d'importer ou de distribuer des dispositifs, produits ou composants de nature mécanique ou électronique « propres à éliminer entièrement ou partiellement l'efficacité des mesures techniques servant à la protection des œuvres et d'autres objets protégés. Il peut s'agir de programmes de décodages, de codes d'accès, etc. »[29].

---

[23] MCF 2006, p. 3297.
[24] BARRELET/EGLOFF, art. 39a LDA n°5.
[25] CR PI JACCARD/HEUMANN, art. 39a LDA n°12.
[26] BARRELET/EGLOFF, art. 39a LDA n°6.
[27] MCF 2006, p. 3297.
[28] Rapport explicatif, p. 23.
[29] BARRELET/EGLOFF, art. 39a LDA n°10.

Afin de déterminer si le dispositif, produit ou composant est destiné à éliminer l'efficacité de la mesure technique, la loi propose trois critères alternatifs (art. 39a al. 3 lit. *a* à *c*) :

a. L'effet ressenti par le public[30] : les dispositifs, produits ou composants font l'objet d'une publicité, promotion ou commercialisation vantant les possibilités de contournement des mesures techniques de protection.
b. La fonctionnalité et l'utilité commerciale[31] : les dispositifs, produits ou composants n'ont pas d'autre utilité commerciale que celle de contourner les mesures techniques.
c. Le but principal des dispositifs, produits ou composants est de contourner les mesures techniques[32] : la théorie de l'utilisateur moyen s'applique.

Si l'un des trois critères est rempli, l'acte préparatoire est retenu et une plainte pénale peut être déposée en vertu de l'article 69a LDA.

L'interdiction de contournement des mesures techniques et l'interdiction des actes préparatoires ne sont punissables que si elles sont intentionnelles et commises sans droit. Le dol éventuel suffit[33]. Il s'agit donc de prendre en considération le critère de l'intention de l'auteur de commettre une infraction, puis de savoir s'il avait ou non l'autorisation de commettre un tel acte. S'il bénéficie d'une exception au droit d'auteur ou de l'autorisation du titulaire de droit, la violation n'est pas retenue. Ceci reflète l'art. 39a al. 4 LDA qui fait office de garde-fou : la neutralisation de la mesure est autorisée si elle conduit à faire un usage licite d'une œuvre ou d'un autre objet protégé.

2.2.3. La sanction : la plainte pénale

L'art. 69a LDA concrétise l'obligation de prévoir des sanctions adéquates imposée par les « Traités Internet ». Cette disposition sanctionne pénalement le « piratage informatique »[34] en lien avec le droit d'auteur[35] et donc s'applique spécifiquement à la violation des mesures techniques et à la violation du régime des droits (art. 39c LDA). Elle doit par conséquent être distinguée de la protection de la sphère informatique prévue par le CP qui est plus générale (art. 143, 143bis, 144bis, 150, 179, 179bis CP)[36].

D'après les termes de l'art. 69a al. 1 LDA, toute personne lésée peut déposer plainte contre celui qui contourne une mesure technique efficace dans le but d'en faire une utilisation illicite ou qui commet un acte préparatoire au sens de l'art. 39a al. 3 LDA. En principe, la sanction est l'amende. Les dispositions générales du code pénal étant applicables[37], le montant maximum est plafonné à CHF 10'000.- (art. 106 CP). La loi prévoit également l'infraction par métier (art. 69a al. 2 LDA). L'auteur est alors poursuivi d'office et encoure une peine privative de liberté d'un an maximum ou une peine pécuniaire.

Seule la personne lésée dispose de la qualité pour déposer plainte et les règles générales du CP y relatives sont applicables (art. 30ss CP). Toutefois, la détermination de la personne lésée est controversée en doctrine, donc la qualité pour déposer plainte l'est également. Certains auteurs estiment que seuls les titulaires de droit d'auteur sont concernés, tandis que d'autres accordent également le droit de déposer plainte aux personnes utilisant des mesures techniques (par exemple un fournisseur de musique en ligne). SALVADE signale que dans l'univers en ligne, les DRMS sont le plus souvent utilisés par des preneurs de licence et non par les titulaires de droit[38]. Il s'agit par exemple des

[30] CR PI JACCARD/HEUMANN, art. 39a LDA n°22.
[31] CR PI JACCARD/HEUMANN, art. 39a LDA n°23.
[32] CR PI JACCARD/HEUMANN, art. 39a LDA n°24.
[33] CR PI JACCARD/HEUMANN, art. 69a LDA n°5 et la doctrine citée.
[34] CR PI JACCARD/HEUMANN, art. 69a LDA n°2.
[35] Idem.
[36] Idem et la doctrine citée.
[37] CR PI JACCARD/HEUMANN, art. 69a LDA n°6 et BARRELET/EGLOFF, art. 69a LDA n°2.
[38] SALVADE, p. 3.

cas où une plateforme prévoit un contrôle d'accès via un nom d'utilisateur et un mot de passe. Ainsi, la question est de savoir si les preneurs de licence entrent dans la catégorie des « personnes lésées » et, le cas échéant, s'ils ont le droit de déposer plainte en vertu l'art. 69a LDA[39].

Le raisonnement complet de la doctrine au sujet de la qualité pour déposer plainte ne sera pas présenté dans ce travail. Toutefois, la réflexion se conclut par le fait qu'a priori une plateforme ne peut pas porter plainte, et ce pour deux raisons. Premièrement, les DRMS utilisés par le preneur de licence visent avant tout à sauvegarder son patrimoine, or ceci n'est pas une prérogative du droit d'auteur. La mesure n'apparaît pas efficace au sens de la loi, donc ne bénéficie pas d'une protection légale. Deuxièmement, l'art. 62 al. 3 LDA accorde au preneur de licence *exclusive* le droit d'agir sur le plan civil (pour autant que cela ne soit pas expressément exclu par la licence). Dès lors, il semble acceptable que ce dernier puisse également déposer plainte, malgré que cela ne soit pas prévu par la loi[40]. Or, une plateforme en ligne ne dispose généralement pas d'une licence exclusive. A priori, il semblerait donc que le fournisseur de musique en ligne ne disposerait pas de la qualité pour déposer plainte[41].

2.2.4. L'exception : le contournement autorisé

L'article 39a al. 4 LDA dispose que « [l]'interdiction de contourner ne peut pas frapper celui qui contourne une mesure technique efficace exclusivement dans le but de procéder à une utilisation licite ».

L'équilibre recherché par la LDA entre les intérêts des titulaires de droits et les intérêts du public ne doit pas être déstabilisé par l'introduction de l'interdiction de contourner les mesures techniques efficaces[42]. Leur protection juridique n'est donc pas absolue : « [...] les auteurs et titulaires ne peuvent pas interdire les utilisations licites même si celles-ci impliquent un contournement des mesures techniques »[43]. Dès lors, aucune poursuite civile ni pénale ne menace la personne qui contourne une mesure technique dans le but d'en faire un usage autorisé[44]. Il s'agit de ne pas favoriser les titulaires de droits en ne privant pas les utilisateurs des exceptions au droit d'auteur.
Par *utilisation licite*, la doctrine entend toute utilisation autorisée par un contrat ou par la loi. C'est le cas lorsque l'utilisateur peut se prévaloir d'une restriction au droit d'auteur prévue par la LDA ou d'une autorisation par l'auteur lui-même.

L'exception de l'usage privé (art. 19 LDA) constitue le gardien de l'équilibre de la loi. En effet, par cette disposition, l'usage d'une œuvre est autorisé pour autant qu'il reste dans le domaine privé ou dans un cercle restreint de personnes. Cependant, afin que l'utilisateur puisse bénéficier de l'usage privé, il doit pouvoir déjouer la mesure technique de protection. Or, nous ne sommes pas tous égaux quant aux connaissances informatiques : il y a ceux que l'on peut qualifier d'utilisateurs *moyens* et l'utilisateur *expert.* Ce dernier dispose d'un avantage considérable, car il sera capable de trouver la possibilité de contourner le DRMS mis en place dans la plupart des cas. Par conséquent, dans le cas d'un usage privé, il pourra non seulement profiter de l'œuvre, mais ne risquera en plus aucune poursuite civile ou pénale. En revanche, l'utilisateur *moyen* est entravé dans son bon droit et ne dispose d'aucune action légale pour faire sauter la mesure technique de protection. Etant donné que les exceptions au droit d'auteur ne sont pas considérées comme des droits[45], il ne peut pas revendiquer « l'usage privé » en justice. En conséquence, un utilisateur risque de ne pas pouvoir utiliser une œuvre, alors qu'il y serait autorisé par la loi. Cet aspect des DRMS ne joue pas en leur faveur, raison pour laquelle ils sont vivement contestés par les associations de consommateurs.

---

[39] Idem.
[40] Idem.
[41] SALVADE p. 4 et la doctrine citée.
[42] MCF 2006, p. 3297.
[43] Idem.
[44] MCF 2006, p. 3298 et voir également Rapport explicatif, p. 23.
[45] SALVADE, p. 2.

2.3. En Europe : l'article 6 de la Directive sur le droit d'auteur

2.3.1. L'adoption de la Directive sur le droit d'auteur

Les défis posés par l'évolution fulgurante de la technologie ne laissent personne à part et forcent les législateurs nationaux à s'adapter. En tant que législateur supranational, l'Union européenne se devait d'harmoniser certaines règles afin de garantir une protection adéquate aux droits d'auteur.
C'est pourquoi, en 2000, l'UE a décidé formellement d'adhérer aux « Traités Internet » de l'OMPI, puis a adopté la Directive sur le droit d'auteur[46].

A titre liminaire, il convient de rappeler qu'une directive européenne est un acte juridique contraignant qui fixe des objectifs aux Etats membres. Ceux-ci ont l'obligation de la transposer dans leur droit national, tout en restant libres quant au mode et aux moyens pour la mettre en œuvre. Cela entraîne souvent – c'est le cas pour la Directive sur le droit d'auteur – des disparités dans les transpositions nationales[47].

2.3.2. La Directive sur le droit d'auteur

a. L'article 6

La base légale pour la protection des mesures techniques efficaces se trouve à l'art. 6 §1 qui dispose que « [l]es Etats membres prévoient une protection juridique appropriée contre le contournement de toute mesure technique efficace, que la personne effectue en sachant, ou en ayant des raisons valables de penser, qu'elle poursuit cet objectif ».

Les mesures techniques sont définies comme « toute technologie, dispositif ou composant qui, dans le cadre normal de son fonctionnement, est destiné à empêcher ou à limiter, en ce qui concerne les œuvres ou autres objets protégés, ***les actes non autorisés par le titulaire d'un droit d'auteur ou d'un droit voisin du droit d'auteur prévu par la loi, ou du droit sui generis*** prévu au chapitre III de la directive 96/9/CE » (art. 6 §3).
La directive européenne est particulière puisqu'elle définit les mesures techniques selon leur but : celui **d'empêcher des actes non autorisés par le titulaire des droits d'auteur ou tout autre droit apparenté aux droits d'auteur**[48]. Elle octroie à l'auteur un droit de contrôle sur son œuvre.

Par conséquent, la question essentielle sera de savoir si la mesure technique a été neutralisée pour utiliser l'œuvre selon l'autorisation du titulaire de droit, ceci indépendamment du fait que la mesure technique protège un acte qui ne soit pas couvert par le droit d'auteur (par exemple l'usage personnel). Sur ce point, DE WERRA explique que si le titulaire de droit n'a pas autorisé l'acte en question, toute mesure technique de protection entrera alors dans le champ d'application de l'art. 6 §1 et sera protégée juridiquement, indifféremment du fait que l'acte tombe ou non sous le coup du droit d'auteur[49]. Cette proposition est confirmée par GASSER qui signale que la protection des mesures techniques est étendue à toutes les situations où le titulaire de droit n'a pas donné son autorisation, y compris les actes qui seraient exemptés en vertu de la loi[50] (par exemple l'usage personnel).

---

[46] Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.
[47] GASSER, p. 17.
[48] DE WERRA, *Legal system*, p. 27.
[49] Idem.
[50] GASSER, p. 27.

A titre d'illustration, DE WERRA donne l'exemple d'un journal en ligne : « [...] if a copyright owner (for instance an on-line news company) specifically prohibits by contract (in a « click on » agreement) the quotation for news reporting of the access protected content, a technological protection measure protecting such content would be enforceable (circumventing it would be unlawful) under art. 6 §3 CISD [Directive sur le droit d'auteur], because the act at issue (i.e. the further quotation of the content) has not been authorized by the right holder, even though the quotation for news reporting of protected works might not be prohibited by copyright law »[51].

Sur la base de ces considérations, il faut admettre que la Directive sur le droit d'auteur offre une protection accrue des mesures techniques. Elle va au-delà de ce qui est nécessaire pour protéger les droits de l'auteur.

Néanmoins, il faut encore que les systèmes de protection mis en place soient *efficaces*. Or, la directive européenne se contente de mentionner que « [...| l'utilisation d'une œuvre protégée, ou celle d'un autre objet protégé, est contrôlée par les titulaires du droit grâce à l'application d'un code d'accès ou d'un procédé de protection, tel que le cryptage, le brouillage, ou toute autre transformation de l'œuvre ou de l'objet protégé ou d'un mécanisme de contrôle de copie qui atteint cet objectif de protection »[52].
Au sein de la doctrine, cette proposition ne satisfait pas tous les auteurs, car une interprétation littérale conduirait à ce que seuls les dispositifs de contrôle d'accès et les protections contre la copie aient la qualité de mesures *efficaces*[53]. Il serait déplorable que la Directive sur le droit d'auteur soit exclusive et ne protège pas les mesures techniques destinées à protéger d'autres droits que celui de reproduction.
Par ailleurs, il appartient aux titulaires de droits de prouver que la mesure technique de protection utilisée dans le cas d'espèce atteint un certain niveau d'efficacité. Il s'agit de démontrer qu'elle ne peut être contournée facilement (« test d'efficacité »)[54].

L'interdiction de contournement suppose un élément d'intention : la personne qui a commis un acte de neutralisation savait, ou avait des raisons de croire, qu'elle commettait une violation de la loi. Cette règle vise à protéger les personnes qui contournent innocemment une mesure technique, sans savoir qu'elles commettent un acte punissable[55]. Seuls les actes volontaires ou commis avec un degré grave de négligence seront poursuivis[56].

De manière similaire à la LDA, les actes préparatoires sont également interdits. Le texte de l'art. 6 §2 de la Directive sur le droit d'auteur ressemble en tous points à l'art. 39a al. 3 LDA.

Finalement, l'art. 6 §4 (1) introduit une particularité relative cette fois-ci aux exceptions : il incombe tout d'abord aux titulaires de droit de favoriser la conclusion d'accords avec les bénéficiaires des exceptions au droit d'auteur. Ce n'est qu'en l'absence de tels accords, que l'Etat doit intervenir en prenant des mesures appropriées aux fins de garantir le bénéfice des exceptions[57].
Cette obligation subsidiaire de l'Etat ne s'applique pas pour des accords conclus entre parties privées dans le cadre de services interactifs à la demande (art. 6 §4 (4)).

b. Les sanctions

En vertu de l'art. 8 de la Directive sur le droit d'auteur, les Etats membres doivent prévoir des sanctions et des voies de recours et veiller à leur bonne application : « [l]es sanctions prévues sont efficaces, proportionnées et dissuasives et doivent comprendre la possibilité de demander des dommages et

[51] Idem.
[52] Art. 6 §3 Directive sur le droit d'auteur.
[53] DE WERRA, *Legal system*, p. 28 et voir également GASSER, p. 17 et la doctrine citée.
[54] DE WERRA, *Legal system*, p. 28 et la doctrine citée.
[55] DE WERRA, *Legal system*, p. 28.
[56] GILLIERON, p. 284 et la doctrine citée.
[57] Directive sur le droit d'auteur, considérant no. 51 et voir également GASSER, p. 28.

intérêts et/ou une ordonnance sur requête et, le cas échéant, la saisie du matériel ayant servi à commettre l'infraction »[58]. Cette disposition concrétise l'obligation de prévoir des sanctions appropriées commandée par les « Traités Internet ».
Le texte laissant une grande marge de manœuvre aux législateurs nationaux, il n'est dès lors pas surprenant de trouver tout un éventail de sanctions différentes au sein d'un ordre juridique qui se veut harmonisé.

c. Les exceptions

L'art. 5 prévoit une liste exhaustive d'exceptions que les Etats membres doivent introduire dans leur droit national, garantissant ainsi l'équilibre des intérêts. Sont exclusivement visés le droit de reproduction, le droit de communication d'œuvres au public, le droit de mettre à disposition du public d'autres objets protégés et, dans certains cas, le droit de distribution. Les exceptions au droit d'auteur comprennent notamment l'autorisation de faire des copies pour l'usage privé (art. 5 §2 lit. b), les reproductions effectuées par des bibliothèques, des établissements d'enseignement, des musées ou des archives (art. 5 §2 lit. c), les utilisations au bénéfice de personnes handicapées (art. 5 §3 lit. b) ou encore le droit de citation (art. 5 §3 lit. d).
Cette liste peut être volontairement enrichie par le titulaire de droits en concluant des accords en vertu de l'art. 6 §4 (1).

2.4. Aux Etats-Unis : § 1201 DMCA

2.4.1. Introduction

Les Etats-Unis ont fait pression pour que le droit d'auteur et les droits voisins fassent l'objet d'un traité international. Il n'est donc pas surprenant qu'ils aient été les premiers à transposer les « Traités Internet » de l'OMPI dans leur droit national, en adoptant le Digital Millennium Copyright Act en 1998[59].

A titre liminaire, il est utile de signaler que le DMCA est particulier car il opère une distinction entre les systèmes de contrôle d'accès et les autres mesures de protection destinées à contrôler l'usage d'une œuvre. La protection juridique dépendant alors du type de la mesure. L'acte de contournement n'est réprimé que s'il concerne un contrôle d'accès, tandis que l'interdiction des actes préparatoires (*trafficking*) s'applique également aux autres mesures techniques. Il est donc légal de contourner un dispositif anti-copie d'un programme d'ordinateur pour en faire une copie[60]. Ceci est un choix du Congrès qui ne voulait pas pénaliser des actes qui ne violent pas le droit d'auteur, tels que le *fair use*[61].

La doctrine est unanime : le texte américain est complexe et il ne respecte pas l'équilibre des intérêts des parties, il favorise les titulaires de droits d'auteur[62].

---

[58] Directive sur le droit d'auteur, considérant no. 58.
[59] 17 USC.
[60] DE WERRA, *Legal system*, p. 23.
[61] Idem.
[62] DE WERRA, *Legal system*, p. 15.

2.4.2. Le principe : interdiction de contournement des mesures de contrôle d'accès

Le § 1201 (a) (1) DMCA interdit le contournement des mesures techniques qui contrôlent effectivement l'accès à une œuvre protégée par le droit d'auteur. Le texte est clair : seuls les mécanismes de contrôle d'accès bénéficient d'une protection juridique. GASSER précise que l'interdiction porte sur tous les comportements de contournement, même si ceux-ci ont un but légitime – par exemple le *fair use* – et qu'ils sont autorisés par la loi[63].
Les auteurs sont d'avis que cette interdiction de contournement va au-delà de ce que prévoient les art. 11 WCT et 18 WPPT, c'est-à-dire que le DMCA offre aux titulaires de droits un nouveau droit, celui de contrôler l'accès à l'œuvre[64]. En effet, les « Traités Internet » visent à protéger les mesures techniques qui défendent effectivement un droit d'auteur prévu par le droit conventionnel. Or, le droit d'accès à l'œuvre n'en fait pas partie. Cependant, ce droit de contrôle d'accès n'est pas absolu puisque le DMCA prévoit des exceptions grâce auxquelles il est autorisé de neutraliser la protection en place.

La loi définit la notion de contournement d'une mesure technique de façon étendue, puisqu'il peut s'agir de tout acte brouillant, décryptant, encryptant une œuvre ou encore du fait de contourner, désactiver, ou supprimer une mesure technique sans l'autorisation du titulaire de droit[65].

En outre, pour que le contrôle d'accès soit juridiquement protégé, il doit être *efficace*. Au sens du DMCA, cela signifie que la mesure technique nécessite l'usage d'informations dans le cours ordinaire de son utilisation, soit un processus soit un traitement, permettant l'accès à l'œuvre avec l'autorisation du titulaire de droit[66].

Cette définition demeure particulièrement vague et pose quelques problèmes d'interprétation. Tel est notamment le cas pour DE WERRA qui se demande si l'acte de contournement serait retenu – donc puni – si un utilisateur autorisé à accéder à l'œuvre transmettait ses codes d'accès à un tiers[67]. En effet, cette personne disposerait des codes nécessaires, octroyés par le titulaire de droits : elle ne neutraliserait pas le système de protection. Il est donc incertain de savoir si le fait de transmettre les informations d'accès à un tiers non autorisé par le titulaire de droits suffit à commettre une violation de l'interdiction de contourner les dispositifs d'accès[68].

2.4.3. L'interdiction du « *trafficking* »

Il s'agit de l'interdiction de procurer des dispositifs permettant de contourner une mesure technique de protection, similaire aux actes préparatoires prévus par le droit suisse (cf. art. 39a al. 3 LDA).
L'interdiction du *trafficking* couvre tant les systèmes limitant l'accès à l'œuvre que les autres mesures techniques contrôlant l'usage d'une œuvre (§ 1201 (a) (2) et § 1201 (b) (1) DMCA).

De manière globale, les actes préparatoires comprennent tous les actes tels que la fabrication, l'importation, l'aliénation, la distribution ou la mise à disposition de technologies, produits, services, ou dispositifs permettant de contourner une mesure technique de protection.
Afin que la technologie soit un élément constitutif d'un acte préparatoire, il faut qu'elle possède une des trois caractéristiques suivantes : qu'elle soit principalement conçue dans le but de contourner des mesures techniques, qu'elle ait un but commercial limité en-dehors du but de contourner les mesures techniques ou qu'elle soit commercialisée dans le but de contourner des mesures techniques[69].

---

[63] GASSER p. 19.
[64] DE WERRA, *Legal system*, p. 14 et GASSER, p. 19.
[65] § 1201 (a) (3) (A) DMCA.
[66] § 1201 (a) (3) (B) DMCA.
[67] DE WERRA, *Legal system*, p. 16 et voir également la question des « *deep link* » p. 17.
[68] Idem.
[69] § 1201 (a) (2) et § 1201 (b) (1) DMCA ; DE WERRA, *Legal system*, p. 22 et GASSER, p. 20.

Le fait que la technologie doive remplir un de ces trois critères permet d'écarter les appareils électroniques ou produits pour ordinateurs usuels qui pourraient potentiellement être utilisés à des fins de contournement des mesures techniques[70].

2.4.4. La sanction : poursuites civiles et pénales

Toute personne lésée par la violation de l'interdiction de contournement ou par des actes préparatoires peut introduire une action civile devant un tribunal de district des Etats-Unis (§ 1203 (a) DMCA). Le juge peut entre autres allouer des dommages et intérêts à la partie lésée, mais également les diminuer ou ne pas en octroyer dans les cas d'une violation innocente. Ce dernier point vise à protéger la personne qui ignorait ou n'avait pas de raisons de croire qu'elle commettait un acte puni par le DMCA.

La poursuite pénale est également prévue et le système est particulièrement répressif (§ 1204 (a) DMCA). Dans le cas d'une première violation, la peine prévue est une amende plafonnée à $ 500'000 et/ou l'emprisonnement de 5 ans maximum. Pour la récidive, l'amende peut atteindre $ 1'000'000 et/ou l'emprisonnement jusqu'à 10 ans.

2.4.5. Les exceptions et la « *Rulemaking procedure* »

Le DMCA prévoit plusieurs exceptions très spécifiques en vertu desquelles les bénéficiaires peuvent *légalement* contourner une mesure technique contrôlant l'accès à une œuvre, sans crainte de poursuites civiles ni pénales. De manière générale, les exceptions concernent le milieu de l'archivage, des institutions dans le domaine éducatif, des bibliothèques à but non lucratif, de certaines activités gouvernementales, du reverse engineering (ingénierie inversée) et d'autres (voir § 1201 (d) à (j)). Dans certains cas, une autorisation est toutefois nécessaire.

Le système des exceptions est essentiel car il garantit le juste équilibre entre les droits des auteurs et les intérêts des utilisateurs. Pourtant, son champ d'application est excessivement restreint[71], les exceptions portant uniquement sur des domaines très spécifiques et n'étant octroyées que pour une durée limitée de trois ans. C'est le principe de la « *rulemaking procedure* », ou procédure de révision périodique[72] (§ 1201 (a) (1) (C) DMCA).
Tous les trois ans, *The Library of Congress* [La Bibliothèque du Congrès] a l'obligation de revoir la liste des exceptions à l'interdiction du contournement des dispositifs de contrôle d'accès (§ 1201 (a) (C) DMCA). Le principe est le suivant : « [...] the primary responsibility of the Register and the Librarian in the rulemaking proceeding is to assess whether the implementation of access controls impairs the ability of individuals to make noninfringing use of copyrighted works within the meaning of section 1201 (a)(1) »[73]. Les milieux intéressés doivent soumettre une requête et expliquer en quoi il est essentiel qu'ils bénéficient d'une exception pour les trois prochaines années.

Il est à noter que le système des exceptions porte uniquement sur des « classes particulières d'œuvres ». Ce terme n'est pas défini par la loi et donc il revient à *The Library of Congress* de déterminer le critère de particularité de ces classes. En septembre 2014, le Copyright Office a ouvert la 6e « *rulemaking procedure* » qui prendra effet en 2015. Les requêtes d'exemptions devaient être déposées jusqu'au 3 novembre 2014.

---

[70] DE WERRA, *Legal system*, p. 22.
[71] Federal Register, p. 55690.
[72] DE WERRA, *Protection juridique*, p. 281.
[73] Federal Register, p. 55688.

3. Les constatations

3.1. Les distinctions entre les différents régimes

L'interdiction de contournement est la pierre angulaire du régime de protection des mesures techniques. Mais, l'interdiction des actes préparatoires semble une règle nécessaire pour compléter le régime de manière satisfaisante. Les législations étudiées ont apparemment saisi l'importance de ces interdictions, puisqu'elles les prévoient toutes deux.

Les Etats ont opté pour une définition « technologiquement neutre » des mesures techniques de protection. Cette caractéristique demeure l'outil indispensable pour assurer la compatibilité de la loi avec les innovations technologiques.

Une liste d'exceptions à la protection des mesures techniques figure dans tout régime juridique. Malgré leur statut de garde-fou de l'équilibre des intérêts, ces exceptions n'ont pourtant pas la même importance dans tous les pays. Alors qu'en Suisse ou dans l'Union européenne, il faut attendre une révision de la loi pour introduire de nouvelles restrictions ; aux Etats-Unis il s'agit d'une procédure essentielle qui se tient tous les trois ans. Le système américain n'est pourtant flexible qu'en apparence. En effet, non seulement la « *rulemaking procedure* » est coûteuse – la plupart des consommateurs étant dans l'incapacité d'agir individuellement – mais en plus elle n'accorde le bénéfice des exceptions que de manière limitée.

Par les « Traités Internet », les Etats avaient l'obligation de prévoir des sanctions juridiques efficaces (art. 11 WCT et 18 WPPT). Les Etats-Unis font preuve d'une grande répression en prévoyant des amendes élevées, voire l'emprisonnement, dès la première violation. La Suisse a suivi le même chemin, même si elle demeure moins incisive. En Europe, la liberté laissée aux législateurs nationaux d'adopter des *sanctions appropriées* a bien entendu entrainé des disparités.

Il faut également mentionner qu'un système de surveillance de l'impact des mesures techniques de protection sur les droits des utilisateurs a été mis en place par la plupart des Etats. Bien que cela ne soit pas requis par les « Traités Internet », cette surveillance apparaît nécessaire pour s'assurer que la collectivité puisse encore profiter des libertés laissées par la loi. En Suisse, ce système de surveillance est assuré par l'Observatoire des Mesures Techniques (art. 39b LDA). Concernant l'Union européenne, un comité de contact a été institué (art. 12 Directive sur le droit d'auteur). Les Etats-Unis quant à eux appliquent la « *rulemaking procedure* » à cet effet.

Au vu de ces constatations, nous partageons le point de vue soutenu par DE WERRA qui remarque que désormais, les auteurs jouissent de trois niveaux de protection : le premier niveau est le droit d'auteur traditionnel. Le deuxième niveau comprend la protection technique réelle des œuvres assurée par des mesures techniques de protection. Le troisième niveau concerne la protection légale des mesures techniques de protection[74].

[74] DE WERRA, *Legal system*, p. 3.

3.2. Les effets

Les DRMS reposent sur d'innombrables intentions, parmi lesquelles figurent notamment la protection du droit d'auteur, la sauvegarde des intérêts, la lutte contre le piratage, le soutien à l'innovation. Pourtant ceci ne se reflète pas toujours dans la réalité.

Les DRMS sont en effet au centre d'une grande controverse : alors que beaucoup d'acteurs dénoncent plusieurs abus, d'autres reconnaissent leur importance. L'absence d'interopérabilité, par exemple, est souvent citée par les détracteurs des DRMS. Or, la doctrine mentionne que l'interopérabilité n'est pas un droit : « la loi n'a jamais obligé l'auteur à publier son œuvre de manière à ce qu'elle soit reproductible sous tous les formats et sur n'importe quel appareil. Ainsi, *l'absence d'interopérabilité* ne porte pas atteinte à un droit que les utilisateurs pourraient invoquer »[75].
Plusieurs entités, à l'image de l'EFF aux Etats-Unis, agissent aux fins de garantir la protection des libertés des citoyens dans un monde de plus en plus numérisé. Elles rejoignent l'idée largement répandue que les DRMS sont nuisibles : « Le DRM doit être ainsi vu comme un véritable verrou informatique par lequel l'utilisateur est restreint dans ses droits d'utilisation de l'œuvre numérique »[76].

Il y a cependant des partis qui encouragent l'utilisation des DRMS et revendiquent une interdiction totale de contournement, comme ce fût le cas en Suisse lors de la révision de la loi sur le droit d'auteur en 2007[77]. Au niveau international, l'IFPI[78], dont le but associatif est de promouvoir les droits et les intérêts des producteurs de phonogrammes et vidéogrammes, a fait part de l'importance des DRMS dans le monde musical. Dans son rapport de 2006, elle décrit les DRMS comme un instrument essentiel pour toute industrie dont le commerce repose sur des droits de propriété intellectuelle dans un environnement numérique. Il s'agit d'un outil très sophistiqué, nécessaire aux modèles économiques de la branche musicale et assurant une rémunération adéquate à toutes les parties concernées par la création de la musique[79]. Le DRMS a donc une utilité : « DRMS is designed to stop the uploading of purchased songs onto file-sharing services where they will be distributed without any recompense to the rights owner »[80].
Pour mieux faire comprendre son point de vue, l'IFPI explique que grâce aux DRMS les consommateurs peuvent obtenir de la musique facilement tout en disposant d'une certaine liberté d'utilisation ; liberté reflétée dans le prix de cette musique. Dès lors, il serait inconcevable qu'un utilisateur puisse transférer sa bibliothèque entière sur l'iPod d'un ami sans que ce dernier ait payé la moindre chanson.

Cependant, l'IFPI reste consciente de l'impopularité des DRMS et reconnaît que le challenge réside dans la création de systèmes qui soient imperceptibles par les consommateurs. Un grand obstacle se pose au niveau des fabricants de DRMS qui tendent de plus en plus à créer des dispositifs incompatibles entre eux. C'est justement ce manque d'interopérabilité qui est attaqué par des consommateurs mécontents de voir leur choix limité[81].

---

[75] SALVADE, p. 3.
[76] CR PI JACCARD/HEUMANN, art. 39a LDA n°2.
[77] MCF 2006, p. 3275 : « Le PRD, l'UDC, l'Association économique suisse de la bureautique, de l'informatique, de la télématique et de l'industrie du divertissement soutiennent en revanche une interdiction générale de contournement comme l'UE le prescrit à ses Etats membres. Dans leur majorité, ces milieux demandent en particulier la suppression de la disposition qui prévoit que le contournement ne peut pas être interdit s'il permet une utilisation licite de l'œuvre ».
[78] L'IFPI est une association enregistrée en Suisse (au registre du commerce dans le canton de Zurich - numéro CHE -108.793.095 – consultation de www.zefix.ch en date du 24 octobre 2014) et qui, selon son site Internet, dispose de bureaux à Londres, Brussels, Hong Kong et Miami (site Internet : www.ifpi.org; consulté le 24 octobre 2014).
[79] IFPI rapport 2006, p. 22
[80] Idem.
[81] Idem.

PARTIE 2 – LES MESURES TECHNIQUES DE PROTECTION & L'APPLICATION DANS LA REALITE

1. Plusieurs rapports

1.1. Aux Etats-Unis : le rapport 2014 de l'Electronic Frontier Foundation

L'EFF a rédigé en septembre 2014 un rapport relevant les conséquences inattendues du DMCA[82] et mettant en lumière les obstacles auxquels les utilisateurs sont confrontés ainsi que l'absurdité de certaines situations créées par une application restrictive de la loi.

Selon le présent rapport, le DMCA – plus spécifiquement la section § 1201, relative à la protection des mesures techniques – n'a pas eu l'effet escompté. Pire, il aurait provoqué des conséquences désastreuses : « [t]he law was ostensibly intended to stop copyright infringers from defeating anti-piracy protections added to copyrighted work. In practice, the anti-circumvention provisions have been used to stifle a wide array of legitimate activities. As a result, the DMCA has become a serious threat to several important public policy priorities »[83]. Comme *public policy priorities*, le rapport cite notamment la liberté d'expression, la recherche scientifique, l'usage privé, la concurrence ou encore l'innovation. En conséquence, le système de sanctions particulièrement répressif prévu par le DMCA freine certains milieux dans leur volonté de partager leurs opinions ou leurs découvertes scientifiques[84].

Le DMCA pousse très loin la protection accordée aux mesures techniques, au risque d'entraver le partage du savoir dans le domaine de la recherche. Ce fût le cas pour Alex Halderman, étudiant de Princeton aux Etats-Unis, qui a fait l'objet de menaces de poursuites en vertu du DMCA pour avoir publié le résultat de sa recherche. En effet, celle-ci démontrait la défaillance du système anti-copie développé par une certaine société et expliquait comment le contourner. Cette affaire a provoqué un mouvement de presse négatif envers cette société qui a alors retiré ses menaces. Cependant, le mal était déjà fait : « [a]lthough Halderman was spared, the controversy again reminded security researchers of their vulnerability to DMCA threats for simply publishing the results of their research »[85].

Ajoutons à cela que certains scientifiques sont allés jusqu'à boycotter les conférences tenues aux Etats-Unis, ceci après qu'un programmeur russe – Dmitry Sklyarov – ait passé plusieurs semaines dans une prison américaine suite à son intervention lors de la *DEFCON conference*[86] à Las Vegas en 2001[87].

Le fléau DMCA touche également la liberté d'expression. En 2000, les grands majors de l'audiovisuel ont poursuivi *2600 Magazine* pour avoir publié sur son site Web un programme de décryptage (DeCss) des DRMS utilisés pour protéger les DVD (CSS encoding). Malgré le fait que la liberté d'expression soit garantie aux Etats-Unis, *2600 Magazine* a été débouté : « [i]n essence, the movie studios effectively obtained *a stop the presses order* banning the publication of truthful information by a news publication

[82] Rapport EFF, Unintended consequences : sixteen years under the DMCA, September 2014.
[83] Rapport EFF, p. 1.
[84] Rapport EFF, p. 3.
[85] Rapport EFF, p. 5 : SunnComm threatens researchers.
[86] La *DEFCON conference* est la « hacker » conférence la plus large au monde. Elle a lieu chaque année à Las Vegas et réunit des professionnels de tous les horizons tels que programmeurs, avocats, hackers, agents du gouvernement, gestionnaires de sécurité informatique, etc. Le but est de discuter de programmation et de piratage et de tester l'efficacité de certains systèmes de sécurité. Le site Internet: http://www.defcon.org.
[87] Rapport EFF, p. 9 : Foreign scientists avoid U.S.

concerning a matter of public concern – an unprecedented curtailment of well-established First Amendment principles »[88].

Enfin, le *fair use* [utilisation loyal] se place en tête parmi les motifs fondant les craintes de limitation excessive. Selon le droit américain, il permet au public d'utiliser une œuvre de manière raisonnable sans l'autorisation de son auteur[89]. Or, aujourd'hui, les DRMS protègent trop de contenu numérisé, ce qui empêche certains utilisateurs d'exploiter légitimement des œuvres protégées.
L'enjeu se situe donc dans le contournement de ces mesures techniques. Or, le DMCA interdit également les actes préparatoires, donc la mise à disposition d'instruments ou programmes qui permettent d'outrepasser les dispositifs de sécurité[90]. Par conséquent, il faut malheureusement constater que seules les personnes disposant de connaissances spécifiques sont enclines à déjouer ces systèmes pour profiter du *fair use* qui leur est reconnu.

1.2. En Europe : les enquêtes INDICARE

Deux enquêtes relatives aux habitudes et connaissances des consommateurs de musique et vidéo digitales méritent notre attention[91]. Elles ont été conduites par INDICARE sous l'impulsion de l'Union européenne dans le cadre d'une Europe numérisée et mettent en évidence la méconnaissance des DRMS par le public.

A titre liminaire, il convient de rappeler que ces enquêtes ont été menées en 2005 pour la musique digitale et en 2006 pour la vidéo digitale et qu'aucune enquête de ce genre n'a été menée depuis. Bien qu'elles ne couvrent que cinq pays de l'Union européenne, elles n'en demeurent pas moins une source d'information non négligeable.

Etonnamment, une grande majorité des utilisateurs sondés n'a jamais entendu parler des DRMS, malgré leur très large application dans le monde de la musique et de l'audiovisuel[92]. Pire, certaines personnes admettent ne pas se sentir concernées par les droits d'auteur et leur respect.
Il ressort de l'enquête relative à la musique digitale qu'il existe une très forte incertitude quant aux usages autorisés et à ceux qui sont illicites. En effet, les utilisateurs ignorent dans quelles circonstances ils peuvent faire une copie d'un CD acheté pour eux ou un ami[93]. Ils n'ont également aucune connaissance quant à la question de la légalité du *upload* et du *download* lors d'échanges *peer-to-peer* (P2P)[94].
Le seul argument en faveur des DRMS résultant de l'enquête musicale porte sur la possibilité laissée aux consommateurs d'acheter la musique qu'ils désirent, par exemple en ne payant qu'une seule chanson.

L'enquête sur la vidéo digitale se conclut à peu près de la même manière, c'est-à-dire sur la méconnaissance des DRMS très marquée parmi les internautes sondés, sur le peu d'intérêt montré vis-à-vis des droits d'auteur et sur l'ignorance quant aux restrictions prévues pour la vidéo téléchargée[95].

88 Rapport EFF, p. 10 : 2600 Magazine censored.
89 GASSER, BEGUE, p. 6.
90 Rapport EFF, p. 13.
91 INDICARE music survey et INDICARE video survey.
92 INDICARE music survey, p. 37 et INDICARE video survey, p. 32.
93 INDICARE music survey, p. 41.
94 INDICARE music survey, p. 42.
95 INDICARE video survey, p. 40.

Pire encore, les deux enquêtes ont démontré que plus de la moitié des utilisateurs qui connaissaient (plus ou moins) les DRMS ignoraient les risques d'intrusion dans leur vie privée, tels que surveillance des habitudes du consommateur et profilage[96].
C'est donc à juste titre que l'enquête sur la musique digitale met en garde contre cette profonde ignorance et rappelle deux principales conséquences qui peuvent également se rapporter aux vidéos digitales. Premièrement, certaines utilisations d'œuvres peuvent être illégales. Deuxièmement, du fait que les utilisateurs méconnaissent leurs droits, ils seront peu aptes à se défendre en cas de violation[97].

1.3. En Suisse : le rapport de l'OMET

Au niveau de la Suisse, l'OMET a constaté que l'accès aux informations nécessaires pour utiliser des œuvres conformément aux exceptions prévues par la LDA était difficile tant pour les consommateurs que pour les utilisateurs[98]. Son rapport d'activité ne relève que sept cas d'annonce (en vertu de l'art. 16g ODAu) sur les trois ans faisant l'objet du document.
Il s'agit de savoir si ce petit chiffre reflète réellement la situation actuelle, ce qui est discutable. Cela implique de déterminer si l'impact des mesures techniques sur les droits des utilisateurs est effectivement très faible – ce qui justifierait que peu de cas aient été dénoncés, en l'occurrence sept. Cependant, le manque d'information quant à l'existence de l'OMET peut jouer un rôle et justifier le peu de cas dénoncés : la population ne dénonce pas de cas car elle ne connaît pas la possibilité d'annonce prévue par l'ODAu (art. 16g ODAu).

Au final, l'OMET déclare que les mesures techniques de protection ont posé relativement peu de problème, rapidement résolus de manière satisfaisante. Dans la plupart des cas, les utilisateurs ont en effet pu profiter des exceptions au droit d'auteur[99].

[96] INDICARE music survey, p. 42 et INDICARE video survey, p. 40.
[97] INDICARE music survey, p. 44.
[98] Rapport OMET, p. 3.
[99] Rapport OMET, p. 3.

2. Le scandale Sony BMG Rootkit

2.1. Le scandale

Tout commence le 31 octobre 2005 par un post de Mark Russinovich sur son blog personnel[100] lorsqu'il révèle publiquement avoir découvert un *rootkit* sur son ordinateur. Ce type de logiciel est conçu aux fins de cacher la présence d'un tiers dans l'ordinateur d'un utilisateur[101]. Il demeure invisible au sein du système d'exploitation et ne peut pas être détecté par les anti-virus ou les logiciels de sécurité[102]. C'est donc une porte d'entrée aux virus, utilisateurs malintentionnés et autres.

Après des recherches plus approfondies, Mark Russinovich s'aperçoit que ce *rootkit* fait partie d'un DRMS appelé XCP et qu'il est utilisé par Sony BMG pour protéger certains de ces CD, dont un album que Mark avait exécuté sur son ordinateur quelques temps auparavant.

Cette maladresse de Sony BMG a largement été couverte par les médias et a permis au public de prendre connaissance des DRMS et des conséquences déplorables qu'ils sont susceptibles d'entraîner. La société major a dû faire face à plusieurs *class actions* aux Etats-Unis, qui se sont conclues par des transactions.

2.2. Le DRMS XCP et le *rootkit*

2.2.1. Le DRMS XCP

Apparemment, la société Sony BMG a saisi les enjeux du DRMS XCP qui a été a été conçu en vue de limiter les utilisations de ses CD. En particulier, il permet de faire : une copie de sauvegarde sur le disque dur de l'ordinateur, lire le CD sur l'ordinateur, mais uniquement à l'aide du programme de lecture qui l'accompagne, transférer les musiques du disque vers les appareils compatibles (iPods exclus) et copier le CD trois fois seulement[103].

Le DRMS XCP utilise une protection active : il installe un logiciel de lecture de musique sur l'ordinateur de l'utilisateur. Il permettra uniquement de lire les fichiers musicaux du CD et de les crypter dans un certain format. Ce logiciel s'installe automatiquement sur les ordinateurs munis du système d'exploitation Windows, car celui-ci contient une fonctionnalité dénommée « autorun », par laquelle les systèmes anti-copie s'exécutent automatiquement[104]. Parallèlement à l'installation de la protection anti-copie, le DRMS XCP installe un deuxième logiciel à l'insu du consommateur – le *rootkit*[105]. Additionnellement au *rootkit*, la technologie XCP contient une fonctionnalité de « *phoning home* » qui est également exécutée secrètement.

---

[100] *Sony, Rootkits and Digital Rights Management gone too far*, October 2005 (sur le blog de Mark Russinovich : http://blogs.technet.com/b/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx, consultation, le 27 novembre 2014).

[101] HALDERMANN, FELTEN, *Lessons from Sony episode*, p. 1 et la doctrine citée.

[102] LA BELLE, p. 94 et la jurisprudence citée.

[103] LA BELLE, p. 121.

[104] HALDERMANN, FELTEN, *DRMS, spyware, security*, p. 19.

[105] Idem.

Il convient de signaler également que l'utilisateur est forcé d'accepter un contrat de licence pour utilisateur final faute de quoi le CD sera éjecté et que le DRMS XCP est fourni sans logiciel de désinstallation.

Selon HALDERMANN et FELTEN, cette fonctionnalité de « *phoning home* » associée à l'installation secrète du *rootkit* ainsi qu'une licence douteuse et l'absence de logiciel de désinstallation rend le DRMS XCP typique d'un « *spyware* »[106]. Bien qu'il soit difficile d'en donner une définition précise, le terme *spyware* s'applique généralement aux logiciels qui sont installés sans le consentement éclairé de l'utilisateur, sont difficiles, voire impossibles à désinstaller, et qui transmettent à un tiers des informations relatives aux habitudes du consommateur (à son insu)[107].

a. Le contrat de licence pour utilisateur final

Lorsque le consommateur insérait le CD protégé par XCP dans son ordinateur, il était forcé d'accepter les termes du contrat de licence qui lui était proposé. Or, cette licence était abusive sous deux points[108] : premièrement, le programme de protection anti-copie était déjà en cours d'exécution avant que l'utilisateur ait « cliqué » sur « accepter ». Deuxièmement, la licence invitait l'utilisateur à consentir à l'installation du DRMS désigné comme « [...] a small proprietary software program [...] »[109]. Cette description apparaît fortement inappropriée au vu des fonctionnalités secrètes du XCP.

b. Le « phoning home »

Le DRMS XCP transmettait certaines informations depuis l'ordinateur du consommateur à un site Web relié à Sony BMG, chaque fois qu'il insérait un CD protégé par ce DRMS[110]. Elles portaient notamment sur les habitudes musicales, tel que le titre écouté, et même parfois son adresse IP. Ces données étaient collectées à son insu, ce qui pouvait s'apparenter à une atteinte à la vie privée puisque , selon le droit américain, l'adresse IP est qualifiée d'information personnelle[111].

c. L'absence de logiciel de désinstallation

La technologie XCP était fournie sans logiciel de désinstallation. Le consommateur désireux de supprimer le DRMS de son ordinateur devait effectuer un vrai « parcours du combattant » informatique. Globalement, il devait remplir plusieurs formulaires en indiquant son identité et attendre une réponse par email pour enfin obtenir un lien URL via lequel il pouvait télécharger le logiciel de désinstallation[112].

Non seulement il est inadmissible que l'utilisateur soit obligé de transmettre des données personnelles, mais en plus la solution proposée pour désinstaller créait de nouveaux problèmes. Les consommateurs ont donc dû attendre la fin de la procédure juridique pour obtenir une solution satisfaisante.

2.2.2. Le *rootkit*

Dans « l'affaire Sony BMG *rootkit* », l'installation parallèle du *rookit* au DRMS XCP à l'insu de l'utilisateur était au cœur du scandale.

---

[106] HALDERMANN, FELTEN, *DRMS, spyware, security*, p. 20.
[107] Idem.
[108] HALDERMANN, FELTEN, *DRMS, spyware, security*, p. 20 et LA BELLE, p. 93.
[109] Idem.
[110] HALDERMANN, FELTEN, *Lessons from Sony episode*, p. 14; LA BELLE, p. 125 et MULLIGAN, PERZANOWSK, p. 1167.
[111] LA BELLE, p. 125
[112] HALDERMANN, FELTEN, *Lessons from Sony episode*, p. 21.

Ce *rootkit* avait pour caractéristique de cacher tous les fichiers dont le nom commence par « sys. En d'autres termes, n'importe qui pouvait secrètement introduire sur l'ordinateur d'un tiers des fichiers dénommés *sys*, sans que ces derniers ne soient décelés par l'utilisateur et le système d'exploitation. En plus des *hackers*, des virus, le Cheval de Troie et autres logiciels malveillants pouvaient profiter du « trou » dans le système pour venir s'y installer.

2.3. Les conséquences

2.3.1. Le *Settlement agreement*

L'affaire s'est résolue par la conclusion d'une transaction entre Sony BMG et les différents demandeurs. Le label musical s'est notamment engagé à échanger les albums protégés contre de nouveaux disques sans DRMS, à permettre aux utilisateurs de télécharger la musique sans protection et à mettre à disposition un logiciel de désinstallation pour le XCP[113].

2.3.2. Les possibles applications du DMCA

Tout d'abord, il est utile de noter que le DRMS XCP entre dans la catégorie des mesures de contrôle d'accès[114]. La nécessité de cette précision se justifie par la distinction entre les systèmes de contrôle d'accès et les autres mesures de protection opérée par le DMCA.

Dans « l'affaire Sony BMG *rootkit* », deux questions se posent : quelle est la responsabilité des consommateurs qui ont voulu contourner le DRMS XCP et celle des scientifiques, tels que Russinovich, qui ont publiquement communiqué les faces cachées du DRMS ?

En premier lieu, les utilisateurs qui auraient tenté de désinstaller le DRMS ne commettaient pas de violation du DMCA[115]. En effet, ceux-ci pouvaient se prévaloir de l'exception « *act of security testing* » prévue à la section § 1201 (j), qui permet de recourir à des tests de sécurité et de corriger les failles. Les informations qui en résultent ne doivent servir qu'à des fins sécuritaires, comme la désinstallation du logiciel. La potentielle application de cette exception est confirmée par une lettre de Sony BMG à EFF, par laquelle le label répond aux revendications de l'organisation[116].
Ces utilisateurs pouvaient également invoquer l'exception relative à la protection des données personnelles (§ 1201 (i))[117]. En vertu de cette règle, toute personne peut légitimement contourner un dispositif de contrôle d'accès qui a également pour fonction la collecte de données personnelles. Or, le XCP disposait d'une fonction de « phoning home » et transmettait notamment l'adresse IP de l'utilisateur (qualifiée de donnée personnelle), ce qui permet l'application de cette exception.

En revanche, les personnes ayant communiqué les fonctionnalités malveillantes du XCP, à l'instar de Russinovich, auraient pu être poursuivies en application du DMCA : elles se rendaient coupables de *trafficking,* au sens de la section § 1201 (a) (2). Cette disposition interdit la publication d'informations

[113] *Sony BMG Settlement agreement*, disponible sur le site Internet de l'EFF: https://w2.eff.org/IP/DRMS/Sony-BMG/sony_settlement.pdf. (consultation le 28 novembre 2014).
[114] MULLIGAN, PERZANOWSKI, p. 1202 et la disposition légale citée.
[115] LA BELLE, p. 125.
[116] La réponse de Sony BMG à la lettre ouverte de l'EFF du 14 novembre 2005 ; disponible sur le site Internet de l'EFF: https://www.eff.org/files/filenode/Sony-BMG/sony_response.pdf (consultation le 28 novembre 2014).
[117] LA BELLE, p. 125.

qui pourraient aider d'une manière ou d'une autre des personnes à neutraliser une mesure technique qui contrôle l'accès à une œuvre[118].

Toutefois, MULLIGAN et PERZANOWSKI signalent que ce raisonnement nécessite d'être nuancé si on l'applique à « l'affaire Sony *rootkit* ». En effet, pour que la responsabilité soit retenue, un lien doit exister entre l'acte de contournement (ou le *trafficking*) et un acte de violation du droit d'auteur[119]. Or, ce lien n'est pas forcément donné lorsque l'on se trouve dans le contexte d'une recherche académique[120].

2.3.3. Les leçons

Il semble très improbable que Sony BMG n'ait pas eu connaissance des fonctionnalités secrètes du XCP ou que cela ne soit qu'une erreur technique. Plusieurs éléments indiquent que le label musical a simplement fait le choix de distribuer des CD dangereux pour les consommateurs. En effet, la société dispose d'une longue expérience dans la vente de CD et en tant que major numéro deux, il est inexplicable qu'elle se soit contentée des tests du développeur du DRMS (First4Internet), sans effectuer elle-même des tests internes. Son erreur réside dans la sous-estimation de la réaction des consommateurs indignés.

Outre les lourdes pertes financières que Sony BMG a connues, difficiles à estimer précisément, l'entreprise a subi d'autres conséquences (moins chiffrables), telles qu'une perte de confiance du public. Les artistes dont l'album figurait sur la liste des CD XCP ont malheureusement payé cher leur affiliation à Sony BMG, perdant des rangs dans les *charts* car leur album ne se vendait plus.

[118] MULLIGAN, PERZANOWSKI, p. 1197 et LA BELLE, p. 129.
[119] MULLIGAN, PERZANOWSKI, p. 1201 et la jurisprudence citée.
[120] MULLIGAN, PERZANOWSKI, p. 1201.

3. Apple : iTunes, iPod et FairPlay

3.1. Introduction

Les chiffres ne trompent pas : les 275 millions d'iPod vendus jusqu'en septembre 2010 témoignent du succès du lecteur MP3 de Apple.
Comment la société californienne en est-elle arrivée là ? Certains dénoncent des pratiques anticoncurrentielles et abusives des consommateurs, d'autres, ardents défenseurs de Apple, vantent un appareil nettement supérieur aux autres par ses fonctionnalités et sa facilité d'utilisation.

Outre l'iPod, la société Apple s'est placée en véritable pionnière en matière de distribution légale de musique en ligne lorsqu'elle a ouvert sa plateforme de téléchargements iTunes en 2003. En effet, l'essor de la musique numérique a permis le développement de nouveaux canaux de distribution et la société a devancé les producteurs majors de la musique (EMI, Sony BMG, Universal Music et Warner Music), qui tardaient à développer leur propre système de distribution par Internet[121]. Apple a profité du fait que le marché ne soit pas encore conquis pour lancer une bombe qui lui a valu un franc succès : le binôme iTunes/iPod.
Via un DRMS dénommé FairPlay, Apple relie techniquement la musique téléchargée au lecteur : les titres achetés sur iTunes sont donc uniquement transférables sur l'iPod et vice/versa.

La doctrine indique d'autres éléments à prendre en considération pour une analyse plus critique de ce succès. Premièrement, l'iPod s'est rapidement imposé sur le marché des appareils MP3 grâce à son caractère innovant (lecteur de petit format permettant de stocker plusieurs gigas de musique) et son interface conviviale[122]. Deuxièmement, la plateforme iTunes est riche d'un large catalogue de musique, fourni notamment par les quatre producteurs majors [123] et d'autres producteurs indépendants. Troisièmement, l'utilisation du DRMS FairPlay bénéficie de la protection légale des mesures techniques prévue par le DMCA, lui permettant ainsi de limiter certains usages et de lutter contre le piratage[124]. Quatrièmement, iTunes repose sur des contrats conclus avec les utilisateurs et impose donc par là ses conditions quant aux usages possibles de la musique[125]. Enfin, l'iPod offre un nouveau design et des fonctionnalités qu'aucun lecteur ne permettait jusqu'alors.

Le succès de Apple a subi de vives critiques dues à l'absence d'interopérabilité assurée par FairPlay. Les entreprises concurrentes remettaient en question la pratique qui consistait à empêcher l'interopérabilité entre les produits et services Apple et ceux des autres marques.
La société californienne a été plusieurs fois accusée d'abus de position dominante et d'entraver l'accès au marché. De plus, le binôme iTunes/iPod conditionne les choix des consommateurs qui se retrouvent coincés dans le système Apple. Certains auteurs prétendent que ce refus d'interopérabilité constitue la pierre angulaire du business model de Apple[126] et s'interrogent sur sa légalité.

Le concept d'interopérabilité est particulièrement important dans le cas Apple. Il n'est pas défini de manière précise, mais dépend de l'approche sur laquelle l'individu se base. Aux fins du présent travail, le terme *interopérabilité* se réfère à l'idée généralement perçue par le public de « systèmes fonctionnant ensemble ». Il s'agit de la capacité d'une technologie à interagir avec une autre technologie afin de permettre certaines fonctionnalités[127].

---

[121] ERBER, p. 6.
[122] ERBER, p. 7.
[123] Idem.
[124] GASSER, BEGUE, p. 5.
[125] Idem.
[126] GASSER, PALFREY, p. 17 et SHARPE, AREWA, p. 335.
[127] GASSER, PALFREY, p. 5 et la doctrine citée.

Le cas Apple met en évidence les problèmes de légitimité des DRMS sous l'angle du droit de la concurrence et du bien-être des consommateurs. Il est donc intéressant d'analyser si le succès de la société californienne est le fruit d'un produit supérieur ou les conséquences d'une stratégie d'entreprise fondée sur des pratiques anticoncurrentielles[128].

3.2. Le DRMS FairPlay

3.2.1. Les fonctionnalités

En acceptant de fournir de la musique via les contrats de licence, l'industrie musicale se devait de prendre des mesures pour empêcher la distribution illégale de cette musique. C'est la raison pour laquelle la plupart des titres proposés sous licence est munie de DRMS en vue de contrôler certaines utilisations de la musique numérique[129]. Il s'agit notamment d'autoriser la lecture de la musique uniquement sur un type d'appareils et de limiter les copies gravées sur CD[130].

Il n'est dès lors pas surprenant que les contrats conclus avec les producteurs majors contiennent tous une obligation pour Apple de protéger la musique proposée sur iTunes[131]. C'est la raison pour laquelle la société a développé son propre DRMS (FairPlay), fonctionnant à l'aide d'un système d'identification basé sur des clés[132]. L'utilisateur doit commencer par installer iTunes sur son ordinateur et se créer un compte. Cette étape permet de lui assigner un numéro d'identification qui sera stocké sur le serveur de Apple, dans le compte iTunes de l'utilisateur, et qui fera le lien entre l'ordinateur et ce serveur. A chaque fois qu'un utilisateur achètera un titre sur iTunes, un échange de clés s'opérera entre l'ordinateur, le compte iTunes qui se trouve sur le serveur de Apple et le titre. C'est en fait l'interaction de ces clés qui permettra de télécharger la musique. Le même mécanisme est mis en œuvre avec l'iPod : ce dernier, lorsqu'il est connecté à l'ordinateur, télécharge toutes les clés de l'utilisateur stockées sur son compte iTunes et permet ainsi de lire les musiques. En revanche, il ne permet pas de lire d'autres types de clés, donc d'autres contenus non issus de iTunes. En raison de ce système d'identification, le DRMS FairPlay entre dans la catégorie de contrôle d'accès prévu à la section § 1201 (a) (1) DMCA. Le contournement de cette technologie est donc interdit.

Contrairement à d'autres types de DRMS, FairPlay possède un caractère relativement fermé. En effet, l'interopérabilité n'est possible qu'entre les services et les produits Apple car tous sont munis de ce DRMS[133] non compatible avec les systèmes étrangers. Il est néanmoins possible d'importer du contenu non protégé dans la librairie iTunes ou de le transférer sur un iPod.

---

[128] SHARPE, AREWA, p. 338.

[129] GASSER, PALFREY, p. 9.

[130] Idem.

[131] ERBER, p. 7 et GASSER, PALFREY, p. 17 ; voir également la lettre ouverte de Steve Jobs « *Thoughts on music : calls for DRM-free music* », February 6 2007, disponible sur le site Internet de Mac Daily News: http://macdailynews.com/2007/02/06/apple_ceo_steve_jobs_posts_rare_open_letter_thoughts_on_music (consultation le 1er décembre 2014).

[132] Pour une explication approfondie du fonctionnement du DRMS FairPlay voir notamment le site Internet de Roughfly Drafted Magazine : http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60-A4E5-4764-A083-FF8610E66A46.html (consultation le 4 décembre 2014).

[133] GASSER, PALFREY, p. 10.

3.2.2. Selon le droit de la concurrence

Tout d'abord, il convient de signaler que le système iTunes/iPod constitue un *regroupement* (*tying*) dans une perspective fondée sur le droit de la concurrence : « [t]echnical tying occurs when the tying product is designed in such a way that it only works properly with the tied product (and not with the alternatives offered by competitors) [...] »[134]. En bénéficiant d'une position dominante sur le marché liant (le marché du téléchargement de musique en ligne), la société peut profiter d'un effet de projection de dominance sur le marché du produit lié (le marché des lecteurs MP3) : « [...] the dominant undertaking uses its position on the market where it is dominant to foreclose competition on another market and acquire substantial market power there too »[135].

Les concurrents de Apple sur les deux marchés dénonçaient un abus de position dominante, du fait que le regroupement iTunes/iPod constitue une barrière à l'accès au marché. Or, ce regroupement est fondé sur le DRMS FairPlay, ce qui fait que seuls le contenu et les appareils munis de la technologie FairPlay sont compatibles. Ses adversaires estiment que Apple a volontairement lié techniquement iTunes à l'iPod pour acquérir et maintenir une position dominante également sur le marché des lecteurs MP3.
Il est licite d'acquérir une position dominante sur un marché lorsqu'on l'atteint grâce à un produit supérieur à ceux des autres. Cependant, l'entreprise dominante ne peut pas recourir à certaines pratiques pour verrouiller le marché, comme le regroupement par exemple. Le regroupement de produits n'est pas obligatoirement illicite, mais le devient lorsque la vente du produit liant (la musique téléchargée depuis iTunes) est conditionnée à la vente du produit lié (l'iPod)[136]. Il convient alors de se demander si l'iPod est le seul moyen permettant de lire le contenu téléchargé depuis iTunes. Selon SHARPE et AREWA, la réponse serait plutôt négative : les droits d'usages étant conférés par iTunes aux utilisateurs, l'iPod ne serait effectivement pas le seul moyen de lire le contenu téléchargé depuis la plateforme, certains utilisateurs pouvant directement en profiter sur leur ordinateur[137].

Toutefois, c'est le refus d'Apple de permettre l'interopérabilité qui est au centre des dénonciations des concurrents[138]. En effet, depuis les débuts de FairPlay, Apple a toujours refusé d'octroyer des licences sur son DRMS, ce qui aurait pourtant permis d'obtenir un haut niveau d'interopérabilité sur les marchés pertinents. Plusieurs autorités de la concurrence se sont donc penchées sur la question de savoir si Apple, en tant que société dominante, avait l'obligation d'octroyer des licences sur sa technologie[139]. Dans quelques affaires, la jurisprudence européenne a souligné l'obligation d'octroyer des licences en vue de permettre l'interopérabilité de technologies et ce au détriment de la protection de la propriété intellectuelle[140]. Cette obligation de licence concerne des circonstances exceptionnelles et requiert plusieurs conditions. Selon GASSER et BEGUE, appliquées à Apple et FairPlay, certaines conditions font défaut, notamment lorsqu'il s'agit de démontrer que le refus d'octroyer des licences permet d'écarter toute concurrence[141].

Plusieurs tentatives ont été menées pour déjouer FairPlay et permettre ainsi l'interopérabilité avec d'autres DRMS, mais elles ne se sont pas avérées fructueuses, Apple ayant à chaque fois trouvé le moyen de contrer cette compatibilité. L'exemple le plus parlant porte sur la société RealNetworks et son programme Harmony qui permettait de convertir le format de la musique téléchargée sur sa propre plateforme en un format non protégé et lisible sur l'iPod. Apple a répondu à cette attaque avec une mise à jour de iTunes qui empêchait cette interopérabilité[142]. Un an après, RealNetworks a programmé une nouvelle version de Harmony qui réinstaurait la compatibilité entre l'iPod et le contenu téléchargé

[134] JONES, SUFRIN, p. 486.
[135] Idem, p. 487.
[136] SHARPE, AREWA, p. 342.
[137] SHARPE, AREWA, p. 342 et la doctrine citée.
[138] GASSER, PALFREY, p. 17 et SHARPE, AREWA, p. 343.
[139] GASSER, BEGUE, p. 8.
[140] GASSER, PALFREY, p. 22 et la jurisprudence citée.
[141] GASSER, BEGUE, p. 9.
[142] Idem.

depuis la plateforme de RealNetworks. Apple a réitéré ses mises à jour et a menacé la société de poursuites judiciaires. Elle se fondait sur l'interdiction de contournement des mesures techniques efficaces prévue par le DMCA (§ 1201). Le comportement de RealNetworks été jugé similaire à celui d'un « *hacker* » qui diffuse un outil de contournement, dans ce cas le logiciel Harmony.

Certains auteurs s'interrogent sur l'applicabilité de l'exception de « *reverse engineering* » [ingénierie inversée] prévue à la section § 1201 (f) DMCA.
La doctrine apporte deux arguments qui tendent à la non-application de cette disposition. D'abord, les conditions générales d'utilisation d'un service excluent habituellement l'ingénierie inversée[143] - c'est le cas pour iTunes[144]. Ensuite, l'exception « *reverse ingineering* » accordée par le DMCA dispose d'un champ d'application relativement restreint puisqu'elle ne vise que l'interopérabilité entre logiciels[145] : « [s]ec. 1201 (f) applies, [...], only to software-to-software interoperability and does not allow reverse engineering to enable interoperation between software and the DRMS-ed content itself (software-to-data interoperability »[146]. Cet argument est particulièrement clair : effectuer une manipulation inversée d'un DRMS (FairPay) afin de comprendre son fonctionnement et créer un logiciel (Harmony) qui rende un certain contenu (les musiques téléchargées depuis la plateforme RealNetworks) compatible avec ce DRMS est interdit.

En résumé, les arguments de la doctrine amènent à la constatation suivante : d'une part, le DMCA et le droit des contrats (par les conditions générales d'utilisation) garantissent à Apple la protection technique de son DRMS FairPlay. D'autre part, le droit de la concurrence et la jurisprudence en la matière, ne permettent pas d'établir un abus de position dominante ni l'obligation de licencier la technologie.

Cette approche de la doctrine pourrait être infirmée par le tribunal californien en charge du procès dirigé contre Apple intenté le 2 décembre 2014. La société est accusée de concurrence déloyale et serait contrainte de payer plusieurs centaines de millions de dollars si sa culpabilité était retenue[147] : « [a]ttorneys representing as many as 8 million consumers and 500 retailers and resellers who bought iPods from 2006 to 2009 claim Apple modified iTunes software so music downloaded with RealNetworks software couldn't be played. Locking iPod owners into iTunes stifled competition for downloading services and enabled Apple to charge more for iPods, they claim »[148].
Les agissements de Apple en 2005 en réponse aux tentatives de RealNetworks de proposer des morceaux compatibles avec l'iPod seront donc examinés. Alors que la première mise à jour de iTunes avait été qualifiée de réelle amélioration du produit par les tribunaux, la deuxième n'avait pas été caractérisée de la sorte : la perspective d'un procès devenait alors possible[149]. Cette possibilité s'est concrétisée puisque le procès est actuellement pendant.

---

[143] GASSER, PALFREY, p. 21.

[144] Voir la dernière version des conditions générales de iTunes Store du 17 septembre 2014 sur le site Internet de Apple Inc. : http://www.apple.com/legal/internet-services/itunes/us/terms.html (consultation le 3 décembre 2014).

[145] GASSER, PALFREY, p. 21.

[146] Idem et la doctrine citée.

[147] *Steve Jobs' emails show how he wanted to smear competitor as hackers*, du 3 décembre 2014, disponible sur le site Internet de Business Insider : http://uk.businessinsider.com/steve-jobs-emails-in-real-networks-ipod-lawsuit-2014-12 (consulté le 3 décembre 2014).

[148] *Apple in the dock : $ 1 billion antitrust claim casts Steve Jobs as conspirator*, du 2 décembre 2014 disponible sur le site Internet de Bloomberg : https://www.bloomberg.com/news/2014-12-02/apple-1-billion-antitrust-case-revisits-ipod-dominance.html (consultation le 3 décembre 2014).

[149] *Apple iPod iTunes antitrust litigation ruling on summary judgment*, du 26 septembre 2014, disponible sur le site Internet Scribd. : http://www.scribd.com/doc/241844346/Apple-iPod-ITunes-Antitrust-Litigation-Ruling (consultation le 3 décembre 2014).

3.2.3. Selon la perspective des consommateurs

Lorsqu'on analyse son impact sur la situation des consommateurs, le « phénomène iPod » révèle deux facettes diamétralement opposées.

En premier lieu, il est important de mettre en lumière les points forts du système Apple et les raisons pour lesquelles il a séduit le public. L'iPod plaît car il permet aux consommateurs de vivre une nouvelle expérience musicale, il est muni de fonctionnalités dépassant largement les possibilités offertes par les supports physiques tels que les CD ou les cassettes audio par exemple. Lors de son lancement, son caractère innovateur a tout de suite conquis le public : aucun lecteur de petit format ne permettait jusqu'alors de stocker des dizaines de gigas de musique, de faire des listes de lecture ou de lire des vidéos.
Malgré les critiques à propos du binôme iTunes/iPod, il faut reconnaître que Apple a apporté une solution appréciable aux inconvénients des CD. Via la distribution des supports physiques, l'industrie musicale pratiquait déjà une sorte de regroupement qui limitait lui aussi les choix des consommateurs. En effet, ceux-ci étaient contraints d'acheter le CD en entier – donc des titres dont ils ne voulaient pas - pour pouvoir profiter de la musique qu'ils souhaitaient. L'iPod a alors offert la possibilité d'acquérir les titres de manière séparée, sans perte de qualité audio[150].
La plateforme iTunes a particulièrement contribué au succès de l'iPod, notamment parce qu'elle dispose d'un catalogue musical de plusieurs millions de titres[151] et qu'elle est supportée par les producteurs majors. Les consommateurs peuvent ainsi acquérir les chansons qu'ils désirent réellement à des prix abordables, sans pour autant débourser pour de la musique qu'ils n'écouteront pas.

Malgré de nombreux avantages, le système Apple a été vivement dénoncé par les consommateurs et leurs associations. En effet, le DRMS FairPlay a subi plusieurs accusations, notamment celle qui limiterait de manière trop restrictive le choix des consommateurs, spécialement en ce qui concerne l'impossibilité de lire sur l'iPod d'autres morceaux de musique que ceux acquis sur iTunes[152].
Une fois de plus, l'absence d'interopérabilité se retrouve au cœur des critiques.

L'avis général est que les consommateurs devraient pouvoir transférer la musique acquise légalement sur iTunes vers n'importe quel lecteur et, à l'inverse, pouvoir télécharger de la musique sur d'autres plateformes tout en pouvant la lire sur l'iPod. Le DRMS FairPlay a donc pour effet de bloquer les utilisateurs des produits Apple dans un système unique, dans lequel le billet de sortie se paye au prix fort. En effet, les coûts de transfert (*switching costs*) sont particulièrement élevés pour un client Apple lorsqu'il décide de passer à un autre fournisseur. Ces coûts incluent la recherche d'une autre source de téléchargement, la sélection et l'acquisition d'un nouvel équipement, le choix d'abandonner un produit familier et apprécié pour ses fonctionnalités et enfin, la potentielle perte de données qui ne pourront pas être transférées sur le nouvel appareil[153]. De ce fait, il convient de remarquer que certains utilisateurs d'iPod ne changent pas de lecteur par souci de fidélité, mais aussi parce que cela serait trop contraignant.

Certains usages licites, tels que le *fair use*, sont compromis par la combinaison de plusieurs éléments : un DRMS fermé, en l'occurrence FairPlay, l'interdiction légale de contourner les mesures techniques efficaces et des conditions générales d'utilisation restrictives[154]. A terme, l'équilibre entre les intérêts des titulaires de droits d'une part et les intérêts des utilisateurs de l'autre risque de ne plus être atteint[155].

---

[150] SHARPE, AREWA, p. 336.
[151] Apple indique un catalogue riche de 43 millions de titres sur son site Internet Apple Inc. : https://www.apple.com/itunes/music/ (voir note de bas de page n°1, consultation le 3 décembre 2014).
[152] SHARPE, AREWA, p. 335.
[153] SHARPE, AREWA, p. 344.
[154] GASSER, BEGUE, p. 9 et la doctrine citée.
[155] GASSER. BEGUE, p. 9.

3.3. Le dénouement

3.3.1. La lettre ouverte de Steve Jobs « *Thoughts on Music* »

En février 2007, Steve Jobs (fondateur de Apple) répond aux diverses critiques en publiant une lettre ouverte intitulée « *Thoughts on music* »[156]. En voici un résumé.

Il faut tout d'abord remarquer que dans la situation actuelle, le choix des consommateurs n'est pas aussi limité que ce qu'ils prétendent. Ces derniers ont en effet la possibilité de transférer sur leur iPod de la musique non protégée par un DRMS, au format MP3 ou AAC, mais aussi d'importer des CD dans leur librairie iTunes.
L'argument selon lequel les utilisateurs sont emprisonnés pour toujours dans un seul système a quant à lui été rapidement réfuté sur la base d'un rapide calcul. En se reposant sur les ventes d'iPods et le nombre de musiques achetées sur iTunes, il résulte qu'un iPod contient seulement 22 chansons achetées sur cette plateforme. Les iPods les plus populaires ont une capacité de 1000 chansons et la majorité d'entre eux sont pleins, ce qui signifie que sur un iPod contenant 1000 chansons, il n'y en a que 22 qui proviennent de iTunes, c'est-à-dire moins de 3%. Steve Jobs démontre ainsi objectivement que les dénonciations des associations de consommateurs sont injustifiées.

Ensuite, les critiques relatives à l'absence d'interopérabilité sont selon lui infondées. Apple n'a pas développé FairPlay pour des raisons de stratégie commerciale, mais uniquement pour remplir ses obligations contractuelles vis-à-vis des producteurs majors. En effet, ceux-ci exigeaient que la musique distribuée par iTunes soit protégée techniquement, afin d'en contrôler l'utilisation. Apple encourt une responsabilité dans les cas où de la musique téléchargée depuis iTunes est transférée sur un lecteur non autorisé, risquant ainsi de perdre les licences avec les majors.
La protection de FairPlay s'apparente au jeu du « chat et de la souris » contre les *hackers,* dans la mesure où Apple doit constamment être à l'affût de toute infraction.

De plus, une obligation d'octroyer une licence pour le DRMS résoudrait les problèmes d'interopérabilité, mais ne ferait qu'augmenter les risques de perdre les licences conclues avec les majors. Selon Steve Jobs, accorder des licences pour FairPlay impliquerait la divulgation de sa composition, tenue secrète jusqu'ici. L'expérience de la vie rappelle que les secrets le ne demeurent jamais longtemps dès le moment où un trop grand nombre de personnes sont impliquées, ce qui serait le cas avec les licences : Apple ne serait plus apte à protéger adéquatement le contenu proposé sur iTunes et les majors résilieraient leur accord.

Enfin, il aboutit à la conclusion que la solution la plus efficace serait d'abolir les DRMS. En effet, ces derniers ne peuvent pas empêcher le piratage, qui existera toujours du moment qu'il est possible de transférer un CD sur un ordinateur, puis sur Internet.

La lettre de Steve Jobs tient sur deux pages mais suffit à contrer la plupart des arguments de ses détracteurs. Le fondateur de Apple a fait son travail, c'est-à-dire défendre son entreprise contre des allégations parfois exagérées et mal fondées. Bien que le but était de défendre FairPlay, il ne défend pourtant pas les DRMS puisqu'il appelle l'industrie musicale à les supprimer… Ce qui n'est pas forcément surprenant lorsque l'on accepte la réalité : l'inefficacité des DRMS.

[156] Lettre ouverte de Steve Jobs « *Thoughts on music : calls for DRM-free music* », February 6 2007, disponible sur le site Internet de Mac Daily News: http://macdailynews.com/2007/02/06/apple_ceo_steve_jobs_posts_rare_open_letter_thoughts_on_music (consultation le 1er décembre 2014).

3.3.2. La réponse de l'industrie musicale

Quelques mois après la lettre de Steve Jobs, Apple annonçait que les morceaux musique du producteur EMI seraient désormais également disponibles sans DRMS[157].
Il faudra deux ans supplémentaires pour que les trois autres majors offrent également leur catalogue sans protection[158]. Ainsi, dès 2009, iTunes pouvait définitivement abandonner les DRMS.

3.3.3. Les remarques finales

Dès leur lancement, la plateforme iTunes et l'iPod ont dominé leurs marchés respectifs. Or, cette performance a été vivement remise en question et fait l'objet d'un procès actuellement pendant. Hormis ce procès, Apple a su saisir l'opportunité du marché pour proposer un service et un produit novateurs. Il est incontesté que la société a gagné sa position de leader sur le marché de manière légitime. Les reproches portent uniquement sur les pratiques qui ont permis à Apple de maintenir son monopole pendant de nombreuses années, au détriment des consommateurs.

La clé du succès de Apple a un nom : FairPlay. C'est un élément essentiel des contrats de licence avec les producteurs majors car il constitue un argument acceptable pour refuser d'octroyer des licences.
Le refus d'accorder l'interopérabilité a parfois été défendu de manière agressive : le DRMS a semblé intouchable durant plusieurs années - quitte à entraver la concurrence - mais ceci n'était qu'une apparence, comme le confirme la lettre de Steve Jobs, qui ne demandait pas moins que l'abolition des DRMS.

L'objectif souhaité par le fondateur de Apple a été atteint puisque depuis 2009, iTunes offre un catalogue « DRMS-free ». Toutefois, l'utilisation abusive de DRMS et surtout l'obsession de sa protection pourraient coûter cher à la société, accusée de concurrence déloyale pour des actes remontant à 2006.

[157] Voir Apple Hotnews du 2 avril 2007, disponible sur le site Internet d'Apple Inc. : http://www.apple.com/pr/library/2007/04/02Apple-Unveils-Higher-Quality-DRMS-Free-Music-on-the-iTunes-Store.html.

[158] Voir Apple Hotnews du 6 janvier 2009, disponible sur le site Internet d'Apple Inc. : http://www.apple.com/pr/library/2009/01/06Changes-Coming-to-the-iTunes-Store.html.

CONCLUSION

Nous étions partis du postulat que le droit d'auteur survivrait difficilement dans l'univers numérique sans l'aide des mesures techniques de protection. Les titulaires de droits étaient armés pour contrôler l'utilisation de leurs œuvres et lutter contre le piratage. Le privilège des exceptions en faveur du public, en tant que gardien de l'équilibre des intérêts, pouvait ainsi perdurer.

De ce fait, la communauté internationale a adopté les « Traités Internet », qui prévoient spécifiquement la protection des mesures techniques. La réalisation de l'objectif d'harmonisation reste discutable. Les législateurs ont certes introduit les règles s'y référant dans leur droit national et se sont dotés d'une définition « technologiquement neutre », mais ils ne peuvent pas prétendre avoir adopté une interprétation et un système de sanctions communs, ce qui entraîne de flagrantes disparités de protection selon les pays.
L'existence de la règle juridique est une chose, mais ce qu'en fait l'Etat en est une autre. Il suffit de comparer le texte du DMCA avec celui de la LDA pour constater que le premier est beaucoup plus complexe et répressif que le second. De plus, le DMCA et la Directive sur le droit d'auteur accordent à l'ayant droit un réel droit de contrôle, alors que la LDA n'est pas aussi radicale. La Suisse a encore une fois prouvé ses sens de neutralité et d'équilibre qui lui sont reconnus.

La protection juridique des mesures techniques était déjà contestée avant son entrée en vigueur. Les parties concernées ont fait part de leurs préoccupations quant aux risques d'abus qui pourraient avoir des effets dommageables importants. Ces inquiétudes semblent s'être concrétisées, particulièrement aux Etats-Unis. Les rapports de l'EFF et de INDICARE, appuyés par les affaires Sony Rootkit et Apple iTunes/iPod, mettent en évidence les dérives des DRMS. A la lumière de ces affaires, nous remarquons que ce n'est pas le DRMS en tant que tel qui est problématique, mais l'alliance « fonctionnalités du DRMS et interdiction légale de contournement ». Dans la plupart des cas, les utilisateurs d'un contenu protégé ne sont pas autorisés à neutraliser la mesure technique qui leur porte préjudice, sous peine de commettre une violation du droit d'auteur, plus spécifiquement la violation de l'interdiction de contournement ou des actes préparatoires.

Premièrement, les DRMS peuvent menacer la sécurité des consommateurs qui ne sont ni conscients, ni informés que leur contenu numérique est protégé par une mesure technique. Le *rootkit* installé par les CD de Sony était capable de récolter des informations relatives aux habitudes des consommateurs ou leur adresse IP, mais il contenait également des failles permettant l'intrusion de virus et logiciels malveillants.
Deuxièmement, le *fair use* – cher aux consommateurs - apparaît fortement compromis par des DRMS contrôlant l'accès à l'œuvre. A l'image du FairPlay de Apple, les utilisateurs de iTunes n'avaient plus le choix : l'iPod était le seul appareil compatible avec la plateforme. En outre, la légitimité des dispositifs anti-copie est discutable puisque le droit de faire des copies pour un usage privé est reconnu dans la plupart des législations.
Troisièmement, certaines sociétés ont développé une stratégie commerciale fondée sur un DRMS. Apple a en effet refusé l'interopérabilité de ses produits au détriment de la concurrence, soit en n'accordant pas de licence, soit en contrant les tentatives de déjouer FairPlay (comme dans l'affaire RealNetworks). Bien que Steve Jobs ait essayé de justifier les choix de sa société, il faut reconnaître que certaines pratiques frôlaient l'anti-concurrence. Selon le fondateur, pour des raisons d'obligations contractuelles, Apple aurait le droit d'évincer ses concurrents. La supériorité du tandem iTunes/iPod a certes été reconnue lors de leur lancement respectif, mais le maintien de cette position de leader du marché est quant à elle plus discutable.
Finalement, le domaine de la recherche dénonce l'interdiction des actes préparatoires qui porte préjudice à la diffusion du savoir. Un chercheur ne peut communiquer le résultat de ses recherches lorsqu'elles portent sur les failles d'une mesure technique sans être accusé de fournir des informations permettant de contourner celle-ci. Or, c'est un acte répréhensible dans la plupart des législations.

Ces exemples démontrent que les mesures techniques sont munies de fonctionnalités qui vont trop souvent au-delà de ce qui est nécessaire pour protéger le droit d'auteur. Ces mesures avaient en effet perdu leur caractéristique principale - soit celle de protection - pour servir des fins étrangères et particulièrement nuisibles. C'est la raison pour laquelle les DRMS sont rapidement devenus très impopulaires parmi les différents acteurs. La renonciation des producteurs majors à les utiliser marque d'ailleurs le début d'une prise de conscience.

Pour les raisons présentées ci-dessus, il faut admettre que les DRMS ont constitué de « faux espoirs »[159]. Il ne s'agit pas de remettre en cause leur capacité à protéger les titulaires de droit, mais plutôt de dénoncer les utilisations qui ont été faites de ces dispositifs et leurs effets sur la société. La technologie doit servir au bien-être de la collectivité en favorisant la communication et les échanges. C'est en effet un domaine extrêmement dynamique, contrairement au droit qui, lui, évolue de manière plus lente. Les législateurs se doivent de rester dans la course à l'évolution technologique, même si cela implique une vitesse accélérée - le droit doit correspondre à la réalité.

Il s'agit à présent de voir si les différents systèmes juridiques parviendront à faire face aux défis lancés par l'esprit d'innovation. La réponse sera peut-être bientôt apportée. Apple, comme des millions de consommateurs, retiennent leur souffle...

[159] Pr. Vincent Salvadé, lors d'un cours intitulé « Droit de la propriété intellectuelle et technologies de l'information et de la communication » relatif au chapitre des mesures techniques de protection, dispensé à l'Université de Neuchâtel durant le semestre de printemps 2014.