Les protections techniques vues dans un contexte juridique plus large-Rapport général et rapport Belge

Dusollier, Séverine

Published in:
Régimes complémentaires et concurrentiels au droit d'auteur

Publication date:
2002

Document Version
le PDF de l'éditeur

Congrès de l'ALAI 2001, New York, 13-17 Juin 2001

Régimes complémentaires et concurrentiels au droit d'auteur

Séance I.C:

Les protections techniques vues dans un contexte juridique plus large

Rapport Général

Séverine Dusollier[*]

INTRODUCTION

Cela ne fait pas plus d'une dizaine d'années que la protection des mesures techniques a fait son entrée dans la propriété littéraire et artistique, suivant de très près le développement de l'ère numérique et des outils de sécurisation technique.

Si cette protection est une nouvelle venue en droit d'auteur, son objectif s'inscrit dans de nombreuses tentatives législatives de protéger la technologie et d'encadrer juridiquement l'érection de barrières techniques sécurisant les contenus informationnels et leur transmission. Ailleurs qu'en droit d'auteur, le législateur a réprimé les tentatives de déverrouillages de ces barrières et de ces sécurité techniques. L'objet de ce rapport est d'examiner les différents mécanismes juridiques, qui constituent des précédents aux dispositions de droit d'auteur relatives aux mesures techniques et pourraient servir de fondement à une action contre le contournement des mesures techniques de protection.

Cette mission nous[1] a entraînés dans des *terra incognita*, ou à tout le moins dans des chemins moins fréquentés par les juristes de droit d'auteur que nous sommes: droit de l'audiovisuel, droit des télécommunications, droit de la criminalité informatique, droit de la responsabilité, protection des secrets d'affaires ou du savoir-faire furent autant de continents visités par nos soins, sans compter les

---

[*] Séverine Dusollier est Maître de Conférences aux Facultés Universitaires Notre-Dame de la Paix de Namur et chargée de recherches au CRID (Centre de Recherche Informatique et Droit).

[1] Ce rapport n'aurait pu être rédigé sans l'aide des rapporteurs nationaux que je remercie ici: P. Wand (Allemagne), D. Lindsay (Australie), A. Cruquenaire et P.Y. Potelle (Belgique), N. Landry (Canada), P. Schønning (Danemark), N. Smith (Etats-Unis), R. Avilés Carceller (Espagne), K. Sorvari et T. Ryhänen (Finlande), G. Vercken (France), P.A. Koriatopoulou (Grèce), A. Pojaghi (Italie), Kentaro Endo et Hiroshi Saito (Japon), G. Larrea Richerand, M. Larrea Legorreta, R. Larrea Soltero, C. Peralta Casares, O. Lecona Morales et F. Campuzano Lamadrid (Mexique), N. Helberger, B. Hugenholtz, K. Koelman, J. Seignette, R. Stuyt et D. Visser (Pays-Bas), H. Best et R. Treagar (Royaume-Uni), P. Brügger (Suisse).

dispositions relativement accessoires, presque anecdotiques, multiples îles d'un cinquième continent de protection de la technique, que nous n'envisagerons pas ici[2].

Au cours de nos pérégrinations, la perspective était double. Il s'agissait de glaner dans chacun de ces paysages les dispositions auxquelles les auteurs peuvent recourir lorsqu'ils constatent soit que le système technique de protection ou de gestion de leurs œuvres a été désactivé et contourné, soit que des équipements facilitant ce déplombage sont diffusés dans le public. Nous avons suivi en cela la distinction classique dans les dispositions anti-contournement propres au droit d'auteur entre l'acte de neutralisation et les équipements permettant ce dernier[3]. Le parallèle n'est pas toujours si manifeste dans les autres régimes juridiques mais la distinction acte/équipement garde néanmoins tout son sens. Elle répond notamment à deux logiques et à deux types d'actes illicites très différents.

Dans une première partie de ce rapport, nous examinerons les différents régimes juridiques qui comportent en leur sein des dispositions pertinentes. Nous oublierons un instant le droit d'auteur pour mieux le retrouver dans la deuxième partie qui envisagera l'interaction entre la protection des mesures techniques telle que prescrite dans les Traités de l'OMPI de 1996 et la protection proche que l'on aura pu trouver dans ces autres corps législatifs.

1. LA PROTECTION DES MESURES TECHNIQUES HORS DU DROIT D'AUTEUR

1.1. Protection par le droit civil : responsabilité, tort law, concurrence déloyale.

a. Introduction

Le droit civil offre une protection protéiforme aux mesures techniques par le biais du recours au droit des contrats ou au droit de la responsabilité sous ses multiples aspects. L'image de cette protection est particulièrement fragmentée, d'autant plus que, sur ce terrain, les traditions juridiques divergent largement. Ce serait nous livrer à un exercice fastidieux de droit comparé que de les analyser en détail.

Une constante apparaît néanmoins dans les rapports nationaux: le fait de contourner une mesure technique ou de diffuser des équipements le permettant est susceptible de constituer une faute, une négligence, un acte illicite ou un *tort*, actes fondateurs selon les Etats d'une obligation de réparer le préjudice ainsi occasionné. Par exemple, la *Hoge Raad* néerlandaise a qualifié d'acte illicite la

[2] Les rapports nationaux mentionnent par exemple des dispositions en matière de protection des données personnelles ou d'enrichissement sans cause. On pourrait également songer à la fausse signature appliquée aux signatures digitales. Toutes ces dispositions devraient être examinées plus avant.

[3] En réalité, ce sont les actes de fabrication ou de diffusion d'équipements qui sont généralement réglementés et non les équipements eux-mêmes. Dans la suite de ce rapport, et dans un souci de concision, nous dénommerons toutefois cette distinction par l'opposition acte/équipement.

publication dans un magazine d'une méthode pour manipuler un décodeur afin de ne pas s'acquitter du paiement normalement dû[4].

Les rapports nationaux relèvent cependant quelques difficultés. Le rapport belge souligne que la preuve du préjudice sera, dans certains cas, difficile à établir ou à évaluer, notamment lorsque l'acte de contournement n'est suivi d'aucune diffusion des œuvres ainsi piratées. Le rapport australien explique que, dans les cas d'équipements de contournement, le préjudice sera généralement une *"pure economic loss"* qui ne donne pas naissance à une jurisprudence et à des principes très clairs.

Plus ardu sera l'établissement d'un lien de causalité entre la faute et le dommage, particulièrement en ce qui concerne les équipements de contournement[5]. Il pourrait être difficile, dans certaines hypothèses de prouver que la vente de dispositifs anti-contournement constitue la cause des contrefaçons que l'auteur avance comme préjudice.

Au contraire des régimes de responsabilité qui sanctionnent une norme générale de comportement, comme en France ou en Belgique, l'acte de contournement ou les activités préparatoires doivent, dans d'autres systèmes, pouvoir rentrer dans la définition d'actes générateurs de responsabilité. La notion anglo-saxonne de *negligence* implique généralement que l'acte illicite ait porté atteinte à un *duty of care*, condition qui ne sera pas forcément satisfaite en matière de mesures techniques. Le rapport américain mentionne de la jurisprudence qui a considéré que le fait de connaître l'usage probable d'équipements de neutralisation d'un procédé de protection établissait le *tort* dans le chef de celui qui les offre au public.

Autre acte fondateur de la responsabilité en droit anglo-saxon, le *trespass* qui peut être défini comme une interférence ou une atteinte illégitime à une personne ou à ses biens. En matière électronique, l'application du *trespass* peut susciter quelques difficultés[6], principalement en ce qui concerne la qualification de l'"information" en bien, objet de l'atteinte[7]. Une jurisprudence américaine récente semble s'être affranchie de cette difficulté conceptuelle pour qualifier de *trespass* l'accès et l'interférence portée à un site web pourtant librement accessible au public[8]. Cette institution pourrait donc connaître de beaux jours à l'ère des réseaux électroniques et peut-être constituer un recours utile en cas de contournement non autorisé d'une mesure technique.

La diversité des approches basées sur la responsabilité et les difficultés qui leurs sont inhérentes expliquent sans doute pourquoi la jurisprudence qui sanctionnerait des agissements de contournement sur base d'une responsabilité de droit commun est relativement absente. En revanche, on peut trouver

---

[4] Rapport néerlandais.

[5] Voir sur ce point les rapports belge et français.

[6] D. L. BURK, "The Trouble with Trespass", *Journal of Small and Emerging Business Law*, Vol.4, Spring 2000, n° 1, p.27-56.

[7] Rapport australien.

[8] *eBay, Inc. v. Bidder's Edge*, (N.D. Cal. 2000), no. c-99-21200 RMW ENE.

de nombreuses décisions qui appliquent aux actes d'atteinte aux mesures techniques un régime de responsabilité plus spécifique, par exemple la concurrence déloyale, ou la notion anglo-saxonne de *contributory infringement*.

b. *La concurrence déloyale*

La jurisprudence allemande regorge de décisions condamnant la distribution d'équipements de contournement d'une mesure technique protégeant des œuvres, surtout des logiciels, sur base de la concurrence déloyale[9]. Cette distribution constitue selon les jugements une atteinte au marché d'un concurrent, une entrave à la libre concurrence, une atteinte à l'organisation et à l'exploitation d'une entreprise. Ont ainsi été condamnés le fait de distribuer des équipements de contournement de protection contre les copies, la distribution de clés *hardware* imitant la clé originale d'accès au programme (ou *dongle*), ainsi que sa suppression. L'acte même du contournement a aussi été considéré comme un acte de concurrence déloyale s'il était suivi d'une distribution commerciale des logiciels ainsi "déprotégés"[10].

Ce type de protection est ouverte dans d'autres pays même si la jurisprudence existante n'a pas encore eu à connaître de cas de piratage relatifs à des protections techniques du droit d'auteur mais plutôt à des décodeurs de services de télévision cryptée ou payante[11]. Le principe ne fait pourtant pas de difficulté et pourrait être transposé aux mécanismes de protection des œuvres.

Le droit de la concurrence déloyale connaît néanmoins certaines limites importantes puisqu'il implique l'existence d'une pratique commerciale concurrente ou parasitaire. L'offre gratuite d'appareils pirates, notamment sur Internet, ne saurait être poursuivie sur cette base si elle ne se situe pas dans le cadre d'une pratique commerciale.

c. *Responsabilité indirecte*

Aux Etats-Unis, un *tort* peut constituer en la commission directe de l'acte préjudiciable, ou en une responsabilité indirecte soit pour *vicarious liability* soit pour *contributory liability*. Ce deuxième type de standard de responsabilité a parfois permis aux juges de sanctionner des équipements permettant de déverrouiller une entrave technique. Dans *Sega v. Maphia*, par exemple, la fabrication et la commercialisation d'équipements permettant de désactiver la protection des plates-

[9] Rapport allemand. Voir également LEHMANN M., "Droit d'auteur et protections techniques - rapport allemand", in *Droit d'auteur dans le cyberespace*, Journées d'étude de l'ALAI, Juin 1996, Amsterdam, ed. Otto Cramwinckel, 1997, p. 371-372; A. RAUBENHEIMER, "Increasing importance of hardware locks (dongles) in recent German case law", *Information & Communications Technology Law*, Vol.7, No. 1, 1998, p.51-70

[10] RAUBENHEIMER, op.cit.

[11] Voir rapport belge.

formes de jeux vidéos empêchant l'insertion de jeux pirates ont été qualifiées de *contributory infringement*[12].

Une limite importante existe toutefois. Elle découle de l'arrêt de la Cour Suprême dans l'affaire qui opposait l'entreprise de produits électroniques Sony aux studios hollywoodiens quant à la légalité des magnétoscopes permettant d'effectuer des reproductions d'œuvres soumises aux droits exclusifs des auteurs[13]. La question essentielle était de trouver un équilibre entre la protection d'un monopole et la liberté de commerce. De manière assez proche du droit de la concurrence, il s'agissait de déterminer dans quelle mesure des activités connexes et à première vue légitimes pouvaient au delà d'un certain point entraîner une responsabilité. La Cour Suprême a jugé que les équipements vendus par Sony, même s'ils constituaient des moyens permettant une violation du copyright, ne justifiaient pas la responsabilité de leur fabriquant s'ils étaient *"capable of substantial non-infringing uses"*. Ce critère général alors dégagé par la Cour Suprême, autrement appelé la doctrine du *"staple items of commerce"*, constitue le standard de la responsabilité pour des équipements dont on poursuit l'illicéité sur base d'un *contributory infringement*[14].

d. *La responsabilité contractuelle*

Lorsque le contournement ou la commercialisation d'équipements se réalise en violation d'une obligation contractuelle, la mise en cause de son auteur peut se révéler bien plus facile. Les auteurs pourraient par exemple inclure une clause dans les contrats de licence qui interdit la désactivation ou toute autre manipulation des mécanismes de protection et de gestion des droits. Une autre hypothèse vise les accords inter-entreprises entre titulaires des droits, fournisseurs des technologies et industrie électronique ou informatique qui intègrent à la licence de la technologie des obligations relatives à leur utilisation. Par exemple, l'accord qui lie les fournisseurs de la technologie de protection du DVD impose aux fabricants des appareils de lecture les conditions dans lesquelles le contenu peut être décrypté[15].

Cette protection, simple et évidente, même si elle est limitée aux parties au contrat, peut se révéler assez efficace, particulièrement dans le cadre de conventions entre entreprises. Les rapports nationaux ne font pourtant pas état d'une pratique contractuelle bien établie en la matière. A l'exception du rapport français qui rappelle que les contrats de licence avec certains sociétés de gestion collective

---

[12] *Sega v. MAPHIA*, (857 F. Supp. 679, 685 (N.D. Cal. 1994)).

[13] *Sony Corporation of America et al. v. Universal City Studios, Inc., et al.*,464 U.S. 417, 104 S. Ct., 774, 78 L. Ed. 2d 574 (1984).

[14] Cette doctrine a notamment été utilisée comme moyen de défense dans l'affaire Napster.

[15] M. S. DEAN & B. H.TURNBULL, "Technical protection measures : the intersection of technology, law and commercial practices", *E.I.P.R.*, 2000, n°5, p. 207.

pour l'utilisation en ligne d'œuvres imposent la diffusion en format de *streaming*, qui , sans constituer une réelle mesure technique, empêche toutefois la copie des œuvres.

1.2. La protection des réseaux de communications - Le droit des télécommunications, de l'audiovisuel et des services cryptés

a. Introduction

Les infrastructures des télécommunications et de la radio et télédiffusion ont ouvert l'ère des réseaux de communication et d'information. Les réglementations de ces infrastructures sont riches en dispositions protégeant les transmissions, les contenus et les services qui en font l'objet. Il est d'ailleurs difficile d'en dresser un tableau exhaustif tant les législations foisonnent et s'interpénètrent, sans nécessairement qu'une distinction très claire soit effectuée entre réseaux de télécommunications et réseaux de diffusion hertzienne, par câble ou satellite.

Nous avons malgré tout choisi de présenter ces dispositions légales selon cette distinction classique entre télécommunications et radiodiffusion, tout en étant conscients que les limites de cette distinction sont en réalité relativement floues et que la convergence de ces réseaux dans la société de l'information brouillera davantage les pistes.

b. L'interception et la réception non autorisée de données de télécommunications

La plupart des Etats connaissent le délit d'interception illégale de données de télécommunications. Prenant leur source dans le principe fondamental du secret des correspondances, ces dispositions, généralement pénales, transposent, à l'ère des communications téléphoniques et autres, l'inviolabilité des lettres. La majorité des rapports nationaux font état d'un tel délit, soit relevant d'une loi spécifique aux télécommunications[16], soit du Code Pénal[17].

En vertu de ces législations, il est interdit d'intercepter sans autorisation des communications. L'Espagne vise particulièrement l'interception du courrier électronique. Outre l'interception, sont également visées la communication du contenu à un tiers (Australie), sa divulgation (Finlande, Belgique, Etats-Unis, France, Japon), sa publication (Etats-Unis, Pays-Bas[18]), son utilisation (Australie, Belgique, Finlande, France), son enregistrement (Australie, Belgique, Pays-Bas), la transformation des données (Belgique), leur suppression (Belgique), leur détention (Belgique), l'installation d'un appareil d'écoute (Belgique, France), l'utilisation frauduleuse d'un enregistrement

[16] C'est le cas de l'Australie, de la Belgique, des Etats-Unis, de la Finlande, du Japon.

[17] C'est le cas de la France, du Canada, des Pays-Bas et de la Suisse.

[18] W. GROSHEIDE, "Droit d'auteur et protections techniques – Rapport néerlandais", in *Droit d'auteur dans le cyberespace*, Journées d'étude de l'ALAI, Juin 1996, Amsterdam, ed. Otto Cramwinckel, 1997, p. 408

légalement effectué (Belgique, France), l'usage frauduleux d'un service de télécommunications (Grande-Bretagne[19]).

Dans la mesure où l'objectif de la protection est de garantir le secret des télécommunications, l'acte décisif est l'interception du contenu de la communication. Peu importe que celle-ci soit cryptée ou autrement protégée. Ce n'est donc ni l'existence ni le contournement d'une quelconque barrière technique qui déclenche l'incrimination, à l'exception notable de la Suisse qui protège les services cryptés.

En outre, si la majorité des dispositions législatives vise l'acte d'interception et de divulgation des données, seule une minorité prohibe également les équipements permettant une telle interception. C'est le cas notamment du *Crimes Acts* australien, de l'*Electronic Communications Privacy Act* américain, du Code pénal suisse. Sont généralement interdites la fabrication, la vente, la possession, l'offre et la mise sur le marché d'appareils ou moyens destinés à l'interception non autorisée des données de télécommunications. Le Code Criminel canadien pénalise pareillement la possession de moyens permettant d'utiliser des installations ou d'obtenir un service en matière de télécommunications[20]. Ici aussi, comme dans la loi pénale suisse, on vise les services plus que les données de télécommunications[21], ce qui rapproche ces dispositions de la protection des services cryptés de l'audiovisuel dont nous parlerons au point suivant.

c. *La protection des services de radio et télédiffusion*

La plupart des pays ont instauré une protection des services de radio et télédiffusion payants en criminalisant les équipements permettant de décoder sans autorisation les programmes, autrement appelés "décodeurs pirates".

Ces lois prohibent généralement les actes de commercialisation, de distribution ou de détention relatifs à des équipements de décodage ou de décryptage illicites. Certaines lois s'étendent également au fait de décoder ou décrypter les signaux télévisés ou de transmettre à un tiers les programmes décodés. Certains Etats, tels la Belgique (Communauté Française) ou le Japon, se contentent d'interdire les actes liés au décryptage sans se préoccuper des équipements de décodage. Dans ce cas, le droit de la concurrence déloyale vient généralement combler cette lacune en interdisant tout acte commercial relatif aux décodeurs pirates[22].

---

[19] Selon le rapport anglais, l'interception d'une télécommunications n'est interdite que si elle est effectuée par un opérateur. Par contre le droit anglais sanctionne l'usage frauduleux et l'accès à un service de télécommunications.

[20] E.FRANCHI et P.E. MOYSE, "Droit d'auteur et protections techniques - Rapport canadien", in *Droit d'auteur dans le cyberespace*, Journées d'étude de l'ALAI, Juin 1996, Amsterdam, ed. Otto Cramwinckel, 1997, p.376.

[21] C'est également le cas de l'article 18 U.S.C. 1029 relatif à la fraude en matière d'équipements d'accès qui prohibe la commercialisation et l'usage d'un instrument de télécommunications modifié dans le but d'obtenir l'usage non autorisé de services de télécommunications.

[22] Rapport belge.

En outre, ces législations ne protègent souvent que les programmes audiovisuels payants. C'est en effet l'objectif de garantir la rémunération des services de télévision qui a inspiré les législateurs anglais, belge, français, japonais et néerlandais. Or, ce ne sont pas seulement les télévision payantes, qu'elles fonctionnent sur un modèle de "péage" ou de "pay-per-view", qui recourent au cryptage de leur signal. Des stations "gratuites" limitent de manière similaire leur audience potentielle soit pour réduire les droits de diffusion des œuvres cinématographiques, soit pour répondre à des conditions légales ou économiques de diffusion[23]. Il s'agit souvent de stations qui émettent par satellite, pour des raisons techniques, mais qui souhaitent toutefois restreindre leur audience à un public national ou régional. Certains pays, tels l'Australie, le Danemark, la Finlande, le Mexique, la Suisse et certains Etats américains, ont rencontré ces préoccupations en ne faisant pas du critère de rémunération une condition de la protection contre les agissements de décodage illicites. Dans certains cas, il suffit que les programmes soient brouillés ou cryptés pour entraîner la protection, dans d'autres, le simple accès aux programmes sans autorisation, ce qui présuppose un régime conditionnel d'accès, normalement mis en place par une technique de codage, déclenche la sanction.

La protection ressort généralement du droit pénal, mais les rapports nationaux indiquent à de nombreuses reprises qu'une action civile reste ouverte au diffuseur dont les programmes ont ainsi été piratés. C'est particulièrement le cas en Grande Bretagne qui insère cette protection des télévisions cryptées dans la Copyright Act, le droit des radiodiffuseurs n'étant pas dans ce pays, un droit voisin, mais bien un copyright[24]. Lorsque la loi permet une action de toute personne lésée, on peut imaginer que le titulaire de droits d'auteur ou de droits voisins sur les programmes codés puisse intervenir[25].

La technique de diffusion des programmes importe assez peu, si ce n'est aux Etats-Unis qui disposent de lois fédérales distinctes pour la transmission des programmes par câble ou par satellite. La diffusion des programmes par Internet ou webcasting n'est que rarement mentionnée dans les textes mais rien n'indique que ces programmes, payants ou cryptés, ne puissent être protégés par des textes technologiquement neutres. L'irruption de la notion d'accès conditionnel et de services de la société de l'information dans la matière pourra donc se faire directement dans ces textes non limités à l'environnement analogique ou par des textes qui les mentionnent expressément, telle la directive européenne sur la protection de l'accès conditionnel, vers laquelle nous nous tournons maintenant.

---

[23] A. CHAUBEAU, "Le décodage illicite des signaux de télévision cryptée et la protection des auteurs et producteurs d'œuvres audiovisuelles", *Droit d'Auteur*, Décembre 1990, p. 385.

[24] K.J. KOELMAN & N. HELBERGER , "Protection of technological measures", in *Copyright and electronic commerce*, B. HUGENHOLTZ (ed.), Kluwer Law International, Information Law Series 8, 2000, p. 165-227.

[25] telle la loi canadienne, voir FRANCHI et MOYSE, op.cit., p. 377; ou le Cable Communications Policy Act américain, voir rapport américain.

d. *La protection des services à accès conditionnel: la directive européenne et la convention du Conseil de l'Europe*

Les textes relatifs aux services à accès conditionnel sont les descendants logiques de la protection des télévisions payantes des années 80. Mais le marché pour les services cryptés a connu un fort développement à la faveur de l'augmentation des fréquences de diffusion disponibles, du développement du numérique et de la baisse du coût du cryptage. Ce ne sont plus désormais les seules télévisions qui conditionnent l'accès à leurs programmes. Le glissement sémantique de "programmes" à "services" l'indique. Opérateurs de télécommunications, fournisseurs de services Internet, entrent maintenant dans la danse.

Dans l'environnement électronique, de nombreux services sont désormais fournis sur base d'un accès conditionnel: services professionnels en ligne tels que services financiers et bancaires, services de consultance, enseignement à distance, fourniture d'informations, accès à des bases de données en ligne, musique ou vidéo sur demande ou fourniture électronique de journaux et magazines.

Le législateur européen s'est très tôt intéressé à ce marché en pleine expansion marqué par ces nouveaux entrants. En 1996, un Livre Vert sur la protection des services cryptés dans le Marché Intérieur[26] pose les questions du débat et relève les disparités des législations dans les Etats membres[27]. La directive sur la protection des services à accès conditionnel et des services d'accès conditionnel suit de très près ce premier texte et sera finalement adoptée en 1998[28].

Plus récemment, le Conseil de l'Europe a enclenché le pas et adopté une convention[29] sur le même thème et issue du même moule, à quelques mots près, que le texte communautaire. La similarité entre les deux textes est telle que, dans la suite de ce rapport, nous envisagerons la protection qu'ils instaurent de manière globale, ne distinguant l'un par rapport à l'autre qu'en cas de nécessité.

Si ces textes ont une importance qui mérite que nous nous y attardions, c'est non seulement parce qu'ils instaurent la première protection large des services électroniques et des barrières techniques protégeant ceux-ci, mais également parce que leur rapport avec les dispositions anti-contournement

---

[26]Commission Européenne, Livre Vert sur la protection légale des services cryptés dans le marché intérieur, 6 mars 1996, COM (96) 76.,

[27] N. HELBERGER, "Hacking BskyB: The legal protection of conditional access services under European law", *Entertainment Law Review*, 1999-5, p. 88, disponible sur <http://www.ivir.nl/Publicaties/helberger/HackingBskyB.html>

[28] Directive 98/84/CE du Parlement européen et du Conseil du 20 novembre 1998 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel, J.O. n° L 320 du 28/11/1998 p. 0054 – 0057.

[29] Convention Européenne sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel, STE n° : 178, 24 janvier 2001.

spécifiques au droit d'auteur a été, bien que sous-estimé dans un premier temps, régulièrement commenté depuis[30].

La directive sur l'accès conditionnel vise à accorder une protection aux services de radiodiffusion télévisuelle ou sonore, ainsi qu'aux services de la société de l'information, traditionnellement définis en droit européen comme "*tout service presté, normalement contre rémunération, à distance, par voie électronique et à la demande individuelle du destinataire des services*"[31].

Les deux conditions de la protection sont d'une part que le service doit être presté sur base d'un accès conditionnel et d'autre part, que le but de cet accès est de garantir le versement de la rémunération du service. L'accès conditionnel consiste en "*toute mesure et/ou tout dispositif techniques subordonnant l'accès au service protégé sous une forme intelligible à une autorisation individuelle préalable*". La directive précise en outre que le dispositif garantissant l'accès conditionnel est considéré comme un service protégé en soi. La protection s'étend donc à la fois sur la technique d'accès et sur l'objet de cette dernière.

Le service doit être un service payant et la protection de cette rémunération l'objectif de la sécurisation technique, pour que la directive s'applique. Cette exigence a suscité de nombreuses critiques. Qu'en est-il des télévisions gratuites qui recourent au cryptage notamment pour limiter géographiquement leur audience et de la sorte la négociation des licences sur les programmes ? Peut-on songer à une rémunération indirecte et non monétaire, notamment au transfert d'une autre valeur économique, tels que des biens ou des informations[32] ?

La technique de limitation de l'accès est indifférente. Il n'est plus question uniquement des services cryptés qui fondaient la genèse de la directive mais bien de toute technique conditionnant l'accès au service. Il peut donc s'agir des mots de passe[33], du cryptage, des techniques biométriques ou de toute

---

[30] TH. HEIDE, "Access Control and Innovation under the Emerging EU Electronic Commerce Framework", (2000) *B.T.L.J.*, Vol. 15, No. 3, p. 993-1048; K.J. KOELMAN & N. HELBERGER, op.cit.; S. DUSOLLIER, "Incidences et réalités d'un droit de contrôler l'accès en droit européen", in *Le Droit d'auteur : un contrôle de l'accès aux œuvres?*, Cahiers du CRID n°18, Bruylant, 2000, p. 25-52."

[31] Voyez l'article 1 (2) de la Directive du Conseil et du Parlement Européen 98/34/EC du 29 juin 1998 établissant une procédure pour la fourniture d'information dans le domaine des standards techniques et des régulations, JO L 204, 21.07.1998, modifiée par la Directive 98/48/EC, 20 Juillet 1998, JO L 217, 05.08.1998, <http://europa.eu.int/eur-lex/en/lif/dat/1998/en_398L0048.html>

[32] N. HELBERGER, op.cit.. Ces critiques n'ont pas échappé au Parlement européen qui a commandé, par l'intermédiaire de la Commission, la réalisation d'une étude sur les services dont l'accès conditionnel poursuit d'autres motifs que le versement d'une rémunération et sur la nécessité d'une protection juridique de ceux-ci. Cette étude est disponible sur le site de l'IVIR, Université d'Amsterdam, qui fut en charge de l'étude, Voyez *Study on the use of conditional access systems for reasons other than the protection of remuneration,* .<http://www.ivir.nl>.

[33] L'inclusion des mots de passe n'est toutefois pas certaine, à tout le moins dans la directive européenne qui n'interdit que les équipements ou logiciels illicites. Le mot de passe ne consistant qu'en de l'information destinée à obtenir un accès, il ne devrait pas pouvoir être sanctionné en vertu de la directive, sauf si les législateurs nationaux, en transposant la directive, en décident autrement. C'est notamment le cas du Code pénal néerlandais qui interdit l'usage de mots de passe pour recevoir des signaux non autorisés par des moyens techniques ou un

autre technique de brouillage ou d'identification, cette neutralité technologique étant un gage pour un vieillissement serein de ces textes.

La protection de l'accès conditionnel, à l'instar de ses textes fondateurs en matière d'audiovisuel, tend plus à réglementer l'offre d'équipements de contournement que l'acte de déverrouillage même. Ni la convention du Conseil de l'Europe ni la directive communautaire ne sanctionnent l'accès non autorisé au service protégé. Sont par contre visés la fabrication, l'importation, la distribution, la vente, la location, la détention à des fins commerciales, l'installation, l'entretien, le remplacement ou toutes activités visant à promouvoir commercialement des dispositifs *"conçus ou adaptés pour permettre l'accès à un service protégé sous une forme intelligible sans l'autorisation du prestataire de services*". Offrir la clé de décryptage sur un site web gratuitement, ainsi que toutes autres offres non commerciales, ne sont donc pas inclus dans la liste des activités illicites, ce qui constitue sans doute une grave lacune du texte[34].

Le choix des sanctions est laissé aux législateurs nationaux. Elles doivent en tout cas êtres *"effectives, dissuasives et proportionnées à l'incidence potentielle de l'activité illicite"*, ce qui incitera certainement les Etats à sanctionner pénalement les activités illicites. Les prestataires de services à accès conditionnels et les prestataires de services d'accès conditionnel (fournisseurs de la technologie ou prestataires du service d'accès conditionnel pour des services fournis par des tiers) doivent pouvoir bénéficier d'une action en dommages et intérêts ainsi que d'une action en cessation ou injonction. L'inclusion des titulaires de droit d'auteur avait été suggérée lors de l'élaboration de la directive[35] mais a finalement été rejetée dans l'optique de réserver la protection de la future directive sur le droit d'auteur aux intérêts des titulaires de droits d'auteur ou droits voisins. Ceci souligne une fois de plus quel est l'intérêt protégé par la directive : c'est la rémunération du service qui justifie la réglementation et non la protection de son contenu.

Les Etats de l'Union européenne n'ont pas tous transposé la directive, même si le délai est déjà dépassé depuis un an. Les rapports nationaux indiquent que le Danemark, la Grande Bretagne[36] et l'Italie font figure de bons élèves. Des transpositions sont en cours en Allemagne, en France, en Espagne et en Finlande. Dans ce dernier pays, ainsi qu'aux Pays-Bas, la protection des services cryptés incluait déjà les services de la société de l'information.

---

faux signal. Cette formulation d' "équipements et logiciels" dénote la généalogie de la directive conçue à l'origine pour les services cryptés. Voir K.J. KOELMAN & N. HELBERGER, op.cit., p. 47.

[34] N. HELBERGER, op.cit.

[35] L'Avis du Comité Economique et social proposait d'ouvrir l'action à tout intéressé (J.O.C.E., No. C 129, 27.04.1998, p. 16); le Comité des affaires juridiques et des droits des citoyens suggérait d'inclure explicitement le titulaire de droits d'auteurs sur les œuvres (Rapport A4-0136/98).

[36] Le cas anglais est intéressant puisqu'il insère la directive au Copyright, Designs and Patents Act (1988) qui régit déjà la protection des radiodiffuseurs.

e. *Avantages et inconvénients de ce type de protection*

En matière d'audiovisuel, la protection ne vise parfois que les services de radio, télédiffusion ou les services de la société de l'information qui sont fournis contre rémunération. Cette condition a d'ailleurs déjà été dénoncée par les milieux des radiodiffuseurs bénéficiaires de cette protection[37]. C'est également le cas pour la directive accès conditionnel.

Ce point est essentiel car la protection technique des œuvres notamment par un contrôle de l'accès, ne se réalise pas forcément pour garantir le paiement d'une rémunération.

Un autre inconvénient de cette protection est le fait qu'elle s'ouvre à l'organisme de radio-télédiffusion ou de télécommunications et non au titulaire des droits sur les programmes diffusés[38]. La directive européenne protège les prestataires de services dont l'accès est conditionnel ainsi que les fournisseurs de la technique elle-même. Pour ce dernier texte, l'objection n'est pas décisive. Lorsque les titulaires de droits distribueront leurs œuvres sur Internet sur base d'un accès conditionnel, ils revêtiront dans la majorité des cas la qualité de prestataires de services[39]. D'autre part, la distribution d'œuvres sera généralement effectuée par des prestataires qui disposeront des droits. Ce seront par exemple les firmes de disques, les sociétés cinématographiques, les producteurs de bases de données.

1.3. Le droit pénal et la criminalité informatique

a. *Introduction*

Faisant suite au développement de l'informatique et des actes criminels qui l'ont rapidement prise pour cible, les Etats se sont dotés de législations spécifiques à ce nouveau genre de criminalité édictant en infractions nouvelles, les atteintes à l'intégrité, à la sécurité ou à la confidentialité des systèmes et données informatiques.

Outre les dispositions nationales en la matière, de nombreux textes internationaux ont été récemment adoptés pour tenter d'offrir une approche harmonisée contre les actes criminels qui mettent en péril la sécurité des réseaux, par essence internationaux. Nous évoquerons particulièrement un projet de Convention du Conseil de l'Europe sur la cybercriminalité[40] qui impose aux Etats des modifications et

---

[37] A. CHAUBEAU, op.cit., p. 385 qui explique l'intérêt de crypter leurs émissions dans d'autres situations, notamment pour restreindre le public ayant accès à leurs programmes pour des raisons techniques ou économiques.

[38] A. CHAUBEAU, op.cit., p. 388; Voir cependant le rapport espagnol qui mentionne une décision où une personne qui avait décodé sans autorisation des programmes télévisés et les avait transmis à d'autres personnes a été condamnée sur base de la propriété intellectuelle.

[39] Voir pour une explication plus détaillée de cette question, S. DUSOLLIER, op.cit., p.49.

[40] Projet de convention sur la cybercriminalité (N°27 Rév.), disponible sur <http://conventions.coe.int>. Le texte de cette nouvelle version du projet de convention n'est disponible qu'en anglais. Les articles cités se réfèrent à

adaptations de la procédure pénale et des règles de coopération internationale en matière de la poursuite des infractions. Le texte préconise également d'ériger en délits une liste de comportements dont certains pourraient servir à poursuivre un acte de contournement d'une protection technique.

b. *L'accès non autorisé aux systèmes informatiques et infractions similaires*

L'accès illégal constitue une infraction clé du projet du Conseil de l'Europe. Doit être considéré comme une infraction pénale dans les droits nationaux, "*l'accès intentionnel et sans droit à tout ou partie d'un système informatique*". Ce n'est donc pas le fait de désactiver une barrière technique qui est en cause même si la convention autorise les Etats à requérir, comme condition d'incrimination, une violation des mesures de sécurité. Ce n'est toutefois pas le choix de la majorité des législations nationales existantes[41].

L'article 3 du texte en projet incrimine l'interception illégale, définie comme «*l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non-publiques, à destination, en provenance ou à l'intérieur d'un système informatique, ainsi que des émissions électromagnétiques en provenance d'un système informatique transportant de telles données informatiques*».

Une même condition apparaît dans ces deux infractions: l'accès ou l'interception doit être effectué "sans droit", élément qui ne sera peut-être pas sans incidence sur l'utilisation de ces incriminations en matière de protection des œuvres. Selon les notes, "sans droit" réfère soit à des comportements ne reposant sur aucune compétence, qu'elle soit législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle, soit à un comportement "non justifié par des exceptions légales, excuses et faits justificatifs établis ou des principes de droit national pertinents". Cette expression pourrait-elle justifier l'accès lorsqu'il s'effectue dans le but d'accomplir une exception au droit d'auteur ?

Il faut d'abord souligner que l'accès ne sera pas sans droit uniquement lorsqu'une compétence, une exception, excuse ou autre fait justificatif autorise l'accès même et non l'acte accompli postérieurement à celui-ci. Ce ne sont donc pas les actes relatifs aux données accédées par un acte de hacking qui devront être justifiés légalement mais bien l'acte de hacking lui-même. De telles hypothèses ne sont pas nombreuses. Il s'agit par exemple, et selon les lois nationales, des intrusions justifiées par la recherche d'infractions, par la mise à l'épreuve de la sécurité des systèmes ou pour des raisons de sécurité publique. En ce qui concerne le droit d'auteur, l'exercice d'une exception ne justifiera pas nécessairement l'accès à l'œuvre. Mais ceci est l'objet d 'un autre rapport. Cela pourrait toutefois être le cas lorsque le législateur impose à l'auteur la fourniture d'un accès libre à l'œuvre ou à tout le moins un effacement de la mesure technique, pour garantir le bénéfice des limites de la protection. On songe notamment à la transposition des mesures prescrites par l'article 6 (4) de la directive européenne sur le

---

une version précédente du projet de convention. Sur les points cités, le texte en projet n'a toutefois pas été modifié.

[41] S. SCHJOLBERG, "The legal framework – Unauthorized access to computer systems, Penal legislation in 37 countries", <http://www.mossbyrett.of.no/info/legal.html>

droit d'auteur dans la société de l'information[42]. Si un Etat membre impose une circulation libre de l'œuvre, entendez dénuée de toute barrière technique, au profit de certains utilisateurs, le passage d'une barrière éventuelle ou le simple accès aux données par ces derniers ne pourrait être qualifié d'accès non autorisé au sens du projet de Convention.

Ce texte international ne modifiera pas en profondeur les législations de nombreux Etats qui comportent déjà une telle infraction d'accès non autorisé, ce que nous confirment tous les rapports.

En revanche, les conditions d'incrimination de l'accès non autorisé diffèrent légèrement. Certains Etats, tels que la Suisse, l'Italie, la Norvège, la Finlande ou l'Allemagne[43], requièrent que le système soit spécialement protégé pour qualifier l'accès de non autorisé. L'existence de mesures techniques de protection sera donc indispensable pour que l'infraction soit établie. Dans d'autres Etats, l'absence d'autorisation suffit à l'incrimination, bien que celle-ci puisse être prouvée par la présence d'une barrière technique. La loi fédérale américaine[44] en la matière requiert en sus de l'accès illicite, l'obtention, la modification ou la destruction d'informations.

La France, la Belgique, la Grande-Bretagne et les Etats-Unis pénalisent en outre le maintien non autorisé dans un système informatique ou l'abus d'une autorisation d'accès, ce qui pourrait permettre de sanctionner la neutralisation des mesures techniques relatives à l'utilisation des œuvres protégées même si l'accès lui-même a été autorisé par le titulaire du droit. Par exemple, une personne souscrit un abonnement à un service de vidéo à la demande dont chaque utilisation lui est facturée par la suite. Elle parvient à neutraliser les mesures techniques qui enregistrent et facturent ces utilisations. Rien ne pourrait empêcher qu'on considère que ces utilisations hors du système technique constituent un maintien indu dans le système de traitement des données punissable par la loi française. Cela pourrait également être le cas pour le fait d'excéder le nombre d'utilisateurs légitimes d'une œuvre ou le fait de déjouer des systèmes de *pay-per-view* ou *pay-per-time*[45].

Souvent l'usage, l'altération ou la suppression des données postérieurement à un accès illégitime constituera une circonstance aggravante de l'infraction. Le rapport belge précise à cet égard que *"reproduire ou communiquer au public les données et œuvres auxquelles le pirate aura accédées illicitement, réutiliser les éléments d'un programme d'ordinateur dont la décompilation aura nécessité la violation des dispositifs de sécurité, consulter ou utiliser les bases de données ou le système informatique une fois les barrières déverrouillées, seront autant de circonstances aggravant la peine pouvant être prononcée à l'encontre du hacker"*. On peut y ajouter la suppression de données constituant le mécanisme de protection ou la manipulation de ce mécanisme afin qu'il devienne inactif.

---

[42] 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 (JOCE L167, 22/06/2001).

[43] S. SCHJOLBERG, op.cit.

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

[45] rapport belge.

c. *Les dispositifs facilitant l'accès non autorisé ou hacker tools*

Sport solitaire, dont les adversaires poussaient surtout à la surenchère, le hacking est devenu depuis quelques années, et avec l'apparition des réseaux, un sport d'équipe dont les membres se partagent astuces et équipements.

Rencontrant cette réalité, les textes récents de criminalité informatique ne se contentent pas du délit d'accès non autorisé mais répriment désormais les outils permettant ou facilitant la commission d'une infraction de hacking. On parle généralement de «*hacker tools*». Rentreront dans cette définition les clés de décryptage, les logiciels permettant de "craquer" des codes d'accès ou autres dispositifs de sécurité, les mots de passe, etc…

Ainsi, l'article 6 du projet de Convention du Conseil de l'Europe prescrit :

> « *Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'il est commis intentionnellement et sans droit:*
>
> *a) la production, la vente, l'obtention pour utilisation, l'importation, la diffusion, ou d'autres formes de mise à disposition,*
>
> *1) d'un dispositif, y compris un programme informatique, [spécialement] [principalement] conçu [en particulier] pour permettre la commission de l'une des infractions établies conformément aux articles 2 – 5 ci-dessus ;*
>
> *2) d'un mot de passe, d'un code d'accès ou des données informatiques similaires permettant d'accéder à l'ensemble ou à une partie d'un système informatique*
>
> *dans l'intention qu'il soit utilisé afin de commettre l'une des infractions visées par les articles 2 – 5 [accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité du système];*
>
> *b) La possession d'un article visé aux paragraphes (a) (1) et (2) ci-dessus dans l'intention qu'il soit utilisé afin de commettre l'une des infractions visées par les articles 2 – 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces articles soit détenu pour que la responsabilité soit engagée.*»

Les rapports suisse, belge, italien et grec font état d'une répression des *hacker tools.* Le rapport américain mentionne des réglementations qui interdisent soit le commerce de mots de passe soit la fraude en matière de dispositifs d'accès. Le mot de passe fait également l'objet d'une disposition pénale japonaise. Le rapport français précise que la poursuite des personnes faisant commerce de *hacker tools* pourra se faire sur base des textes généraux relatifs à la complicité.

d. *Autres délits informatiques*

Les rapports nationaux indiquent que d'autres infractions spécifiques à la criminalité informatique pourraient incriminer le contournement d'une mesure technique protégeant une œuvre.

Les rapports belge, américain, finlandais, grec, espagnol, suisse[46] et danois estiment que la fraude informatique peut également être utile à cet égard. Le Conseil de l'Europe définit la fraude comme " *le fait de causer intentionnellement et sans droit un préjudice patrimonial à autrui par l'introduction, l'altération, l'effacement ou la suppression de données informatiques, ou toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui".*

Cette infraction pourrait trouver à s'appliquer à certains actes relatifs aux dispositifs techniques de protection mentionnés dans les rapports: l'introduction dans un programme informatique piraté d'une liste de numéros de licence trouvés sur Internet, l'introduction d'un programme permettant le contournement d'une mesure technique ou d'une clé de décryptage illicitement acquise. Le bénéficie économique obtenu sans droit consisterait en l'utilisation et la copie d'une œuvre sans autorisation de l'auteur.

Outre ces deux grands pans de la criminalité informatique, accès non autorisé et fraude, d'autres délits qui pourraient poursuivre un contournement sont invoqués dans les rapports nationaux: le faux et la modification de matériel informatique en droit anglais, l'altération ou la détérioration de données en droit suisse et espagnol, allemand et mexicain, l'utilisation frauduleuse d'un ordinateur en droit espagnol et suisse, l'escroquerie en droit suisse, l'obtention de données sans autorisation et le sabotage d'un traitement de données en droit allemand.

e. *Avantages et inconvénients de ce type de protection*

Les dispositions de la cybercriminalité permettront vraisemblablement d'incriminer un grand nombre d'actes de contournement de dispositifs de protection, en raison déjà de la largesse de la notion d'accès non autorisé qui pourra couvrir de nombreux cas. Toutefois, l'exemplaire d'une œuvre ne sera pas toujours facilement qualifié de système informatique[47]. Si l'œuvre est hébergée sur un système informatique, tel qu'un serveur ou un site web, son accès impliquera l'accès au système[48].On pourrait également considérer qu'un répertoire d'œuvres accessible en réseau, par exemple des vidéos à la demande, pourra constituer un système informatique. Il n'en sera pas de même pour les œuvres stockées sur des supports, tels que CD Rom, DVD, qui ne pourront être considérés comme des systèmes informatiques. L'accès non autorisé à ces œuvres ne pourra en conséquence constituer une

[46] Le droit pénal suisse parle d'obtention frauduleuse d'une prestation.

[47] K.J. KOELMAN & N. HELBERGER, op.cit., p. 35

[48] rapport néerlandais.

infraction que si la législation pénale parle à la fois de système et de données informatiques. C'est parfois le cas dans des lois plus récentes.

La notion de système informatique ne couvrira pas non plus les mesures d'accès placées chez l'utilisateur, par exemple le décryptage d'un signal codé réalisé par l'ordinateur ou l'appareil de lecture. Si l'utilisateur utilise une clé de décryptage qu'il a trouvée sur Internet pour décoder et pouvoir visionner un contenu qu'il a légitimement acquis, par exemple un DVD ou un jeu vidéo, on pourra difficilement qualifier cet accès à un contenu sur son propre système informatique d'accès non autorisé.

Il existe en outre deux inconvénients inhérents au droit pénal. Le premier est que sa mise en œuvre est souvent plus lourde et consiste à laisser l'action aux mains du ministère public [49]. Le deuxième est que l'interprétation des dispositions pénales doit s'effectuer de manière restrictive ce qui ne permet pas les approximations. Si un acte de contournement d'un dispositif technique n'entre pas clairement dans le champ d'application de la norme pénale, il n'est pas punissable.

1.4. Droits intellectuels sur la technique

a. *Introduction*

Le fait de contourner ou de désactiver un dispositif technique nécessite bien souvent une manipulation de ce dernier, qui est susceptible de constituer une atteinte à des droits privatifs portant sur cette technique même. Ceci nous ramène à des contrées plus voisines de la propriété intellectuelle. Droit d'auteur, brevet, protection du savoir-faire et des secrets d'affaires sont autant de domaines qui peuvent dans certains cas offrir des recours utiles, ce que confirme une jurisprudence qui est loin d'être éparse.

b. *Le droit d'auteur sur le logiciel*

Lorsque le dispositif technique utilisé par l'auteur pour protéger son œuvre, en contrôler l'accès, en empêcher la copie ou en garantir l'authenticité, est un logiciel, certains actes visant à le déplomber peuvent constituer des atteintes au droit d'auteur portant sur celui-ci. Il est en effet difficile d'imaginer qu'une manipulation de la mesure technique ne nécessite pas un acte de reproduction , même fugace, du programme d'ordinateur[50].

---

[49] Voir le rapport anglais.

[50] Ceci implique toutefois que cet acte de reproduction, lorsqu'il n'est que temporaire, soit soumis à l'autorisation du titulaire de droits . Sur cette question, voir Y. GENDREAU , "Le droit de reproduction et l'Internet", *R.I.D.A.*, octobre 1999, n°178, p. 2-81

C'est particulièrement vrai pour l'élaboration d'un anti-programme, d'un dispositif permettant soit de réduire à néant l'objectif de protection du logiciel, soit d'en simuler l'action[51]. Concevoir un tel système pirate requiert en premier lieu une décompilation du programme de protection et dans un second stade de nombreux tests de son fonctionnement. Souvent, le pirate effectuera une copie complète et permanente du logiciel[52]. Chacun de ces actes constitue une reproduction, permanente ou provisoire, soumise à l'autorisation du titulaire de droits. Ce dernier pourrait donc s'opposer à la conception d'outils de neutralisation ou d'émulation de son logiciel. Toutefois, il ne sera pas en mesure de poursuivre sur cette base celui qui offre ou met sur le marché de tels outils, cette commercialisation n'impliquant en principe aucun acte de reproduction du logiciel originel.

L'utilisation des équipements, et donc l'acte de neutralisation, pourraient pareillement être poursuivis s'ils nécessitent des actes de reproduction du logiciel de protection.

Les rapports nationaux indiquent de nombreux cas de jurisprudence qui ont adopté cette solution de protection. En Allemagne, plusieurs décisions ont estimé que le contournement d'un logiciel de sécurité nécessitait son altération et à ce titre portait atteinte au droit d'adaptation portant sur le programme[53]. Un juge australien a également considéré que le fonctionnement d'un *dongle*, routine de vérification d'un accès légitime au logiciel, constituait une part substantielle du programme protégé et que sa neutralisation impliquait un acte de reproduction. Dans ce cas, toutefois, ce n'est pas la mesure technique seule qui est considérée comme un programme d'ordinateur mais son interaction avec le logiciel qu'elle protège. En ce sens, le juge opère une sorte de fusion entre le dispositif technique et son objet. Une autre décision australienne a qualifié une protection technique de logiciel protégeable à la condition qu'elle présente une originalité suffisante. La question s'était également posée quant à savoir si les données traitées par la routine de vérification ne constituaient pas une compilation protégée selon la loi australienne[54].

Aux Etats-Unis, à l'ère pré-DMCA, le concepteur d'un dispositif de protection anti-copie a poursuivi un concurrent qui proposait sur le marché un système de déplombage[55]. Le demandeur, la société Vault Corp., invoquait les copies que son adversaire avait effectuées à la fois pour tester le logiciel de protection et pour le décompiler. Le juge a toutefois estimé que ces copies étaient des usages permis

---

[51] Par exemple, les programmes d'émulation qui simulent l'action d'un logiciel certifiant que la copie du logiciel est originale.

[52] X. LINANT DE BELLEFONDS, obs. sous Paris, 4ème ch., 20 octobre 1988, *Sem. Jur.*, 1989, éd. G, Jurisprudence, n°21188.

[53] voir J. KAESTNER, "Law and technology convergence: copyright", in I. WALDEN & J. HÖRNLE (ed.), *E-commerce law and practice in Europe*, ECLIP Publications, Woodhead Publishing, 2001, Chap. 2, p. 8, et la jurisprudence qui y est citée; A. RAUBENHEIMER, op.cit.

[54] Voir le rapport australien.

[55] *Vault Corp. v. Quaid Software*, Inc., 655 F. Supp. 750 (E.D. la. 19870, aff'd, 847 F.2d 255 (5th Cir. 1988).

par la licence d'utilisation dont disposait la société ayant développé l'équipement illicite[56]. Un autre argument de Vault se fondait sur le droit de créer une œuvre dérivée dans la mesure où l'intervention du logiciel pirate altérait l'opération du programme de protection. De manière générale, la Cour d'appel a rejeté l'action au motif que l'utilisation du logiciel de contournement développé pouvait également poursuivre des buts légitimes, tels que la réalisation d'une copie de sauvegarde des logiciels protégés par la mesure technique.

A l'instar de cette affaire américaine, les décisions évoquées dans les rapports nationaux ont parfois eu à connaître d'exceptions susceptibles de s'opposer à une telle action. En France[57], un plaideur a tenté de justifier le contournement d'une protection anti-copie d'un logiciel par l'objectif d'en réaliser une copie de sauvegarde. Ce type de copie reçoit toutefois une interprétation très stricte de la jurisprudence française qui l'autorise à la seule condition que l'éditeur de logiciels ne l'ait pas fournie à l'utilisateur. En outre, elle ne consiste qu'en une faculté et certainement pas en un droit, ce qui signifie, bien que le juge ne l'ait confirmé qu'implicitement, qu'elle ne peut certainement pas être invoquée à l'encontre d'une mesure technique[58].

Une autre exception largement invoquée par les défendeurs est celle de la décompilation. Toutefois, ses conditions ne seront que rarement rencontrées. L'objectif de la décompilation doit être la conception d'un programme intéropérable. Or, dans les cas de décompilation des mesures de sécurité, le but poursuivi est la neutralisation du mécanisme et non la création d'un programme compatible[59].

Le rapport belge relève également qu'une difficulté de protéger la mesure technique par le droit d'auteur dont elle fait l'objet réside dans le fait que seul le titulaire de droits sur le logiciel-mesure technique pourra invoquer l'atteinte à ses droits, et non l'auteur du contenu ainsi protégé. Cette difficulté pourra être résolue lorsqu'une voie de recours s'offre à tout intéressé, notion qui pourrait comprendre le titulaire d'une licence d'utilisation de la mesure technique pour protéger ses œuvres[60].

a. *Le droit des brevets*

Le procédé technique de protection peut faire l'objet d'un brevet. Qu'il s'agisse d'un logiciel ne présente en outre plus tellement de difficultés. Toutefois la protection accordée par le brevet ne constituera pas un recours très utile en cas de contournement ou d'actes préparatoires. Le brevet octroie un droit

---

[56] P. SAMUELSON, "Intellectual property and the digital economy: why the anti-circumvention regulations need to be revised", *Berkeley Technology Law Journal*, Vol. 14:1 (1999).

[57] Paris, 4ème ch., 20 octobre 1988, *Sem. Jur.*, 1989, éd. G, Jurisprudence, n°21188.

[58] X. LINANT DE BELLEFONDS, op.cit..

[59] Voir en matière de dispositions anti-contournement en droit d'auteur, *Universal City Studios, Inc. v. Reimerdes*, 2000 WL 48514 *2 (S.D.N.Y. 2000); JANE C.GINSBURG, "Copyright use and excuse on the Internet", 24 *Columbia-VLA J.L. & the Arts*, 2000.

[60] Rapport belge.

exclusif de fabriquer, d'utiliser, de vendre et de mettre sur le marché les produits brevetés[61]. Lorsque l'invention consiste en un procédé, les législations diffèrent: soit le titulaire du brevet a seul le droit de fabriquer des produits basés sur ce procédé, soit aucun droit n'est accordé relativement à ces produits.

Un contournement d'une mesure technique ou la vente d'équipements à cet effet ne constitueront pas un acte de fabrication ou de commercialisation de ce dispositif breveté. Le contournement aura peut-être pour but de fabriquer des équipements basés sur le procédé breveté mais c'est cette fabrication qui pourra alors faire l'objet d'une action en contrefaçon. De manière générale, les équipements de contournement ne reproduisent pas le procédé technique mais le désactivent.

b. *Le secret et le savoir-faire*

De nombreux Etats réglementent les secrets de fabrique ou secrets d'affaires et en interdisent la divulgation. La technique législative est variée, soit par une incrimination pénale, soit par une action civile, en concurrence déloyale, soit encore par le droit du travail.

Les accord ADPIC imposent aux Etats une protection des renseignements non divulgués, définis comme les renseignements *"qui sont secrets en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exact de leurs éléments, ils ne sont pas généralement connus de personnes appartenant aux milieux qui s'occupent normalement du genre de renseignements en question ou ne leur sont pas aisément accessibles; ont une valeur commerciale parce qu'ils sont secrets, et ont fait l'objet, de la part de la personne qui en a licitement le contrôle, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrets"*[62]. Ce texte préconise le recours au droit de la concurrence déloyale si le renseignement est divulgué à un tiers, ou acquis par ce tiers, ou encore utilisé par lui.

A notre connaissance, au moins une décision judiciaire a fait appel au secret d'affaires pour sanctionner une offre au public d'un dispositif de contournement. Il s'agit du premier épisode de l'affaire américaine du décryptage du DVD dans lequel les concepteurs de la technologie de protection ont poursuivi les personnes diffusant la clé de décryptage sur base de la divulgation d'un secret[63]. Le juge a considéré que la clé de cryptage constituait bien un *trade secret*, le fait que quelqu'un puisse le décrypter n'empêchant pas que le cryptage reste un secret pour le public général. La valeur économique du procédé de cryptage des DVD tient d'ailleurs dans son secret. L'atteinte au secret nécessite que les informations aient été obtenues de manière illégitime. Dans cette affaire, le secret

---

[61] S. LADAS, *Patents, Trademarks and Related Rights : National and International Protection*, Harvard University Press, Cambridge, 1975, T. I, p. 396, § 232A.

[62] Article 39 §2 ADPIC.

[63] *DVD Copy Control Association, Inc. v. Andrew Thomas McLaughlin et al.*CV-786804 (Ca. Super. Ct filed Dec. 28, 1999).

avait été obtenu par décompilation, ce qui constitue un mode d'obtention licite pour autant que la licence du produit faisant l'objet du secret ne l'interdise pas.

A ces conditions, la divulgation d'informations secrètes liées à la protection techniques des œuvres pourrait être considéré comme une violation punissable d'un secret. Cette protection ne s'étend toutefois pas au contournement de la protection, ni à la fabrication d'équipements.

Le savoir-faire ou *know-how* est un ensemble de connaissances techniques, transmissibles, non immédiatement accessibles au public et non brevetées[64] qui ne bénéficie que d'une protection contractuelle [65]. Nous renvoyons donc à ce qui a été dit sur ce point.

1.5. Comparaison des régimes de protection

a. Critères de protection des mesures techniques en droit d'auteur

Les autres sessions de ce congrès démontreront combien les dispositions anti-contournement spécifiques au droit d'auteur diffèrent d'un Etat à un autre. Il est donc difficile de trouver des règles communes de protection qui pourraient servir de base à une comparaison avec les dispositions hors du droit d'auteur. Prendre les Traités de l'OMPI comme dénominateur commun ne proposerait qu'une base très minimale de protection, les Traités n'imposant aux Etats que la prohibition de l'acte de contournement et non celle des équipements.

On sait toutefois que l'intention première de la Conférence Diplomatique de 1996 était d'englober les équipements dans le champ de la réglementation. On peut donc supposer qu'une protection communément admise des dispositifs techniques comprend tant l'acte de neutralisation que les actes préparatoires[66].

La définition des mesures techniques protégées varie également largement. Le droit d'auteur englobe toute mesure technique mises en œuvre par les auteurs dans le cadre de l'exercice de leurs droits ce qui a permis au législateur et à la jurisprudence de faire bénéficier de la protection une série de dispositifs qui, de près ou de loin, étaient utilisés par les auteurs. Ont ainsi pu être protégés:

- les mécanismes de protection contre la copie;

---

[64] M. BUYDENS, *Le droit des brevets d'invention*, Larcier, Bruxelles, 1999, p. 291.

[65] K.J. KOELMAN & N. HELBERGER, op.cit., p. 36

[66] Ceci n'est toutefois qu'une hypothèse de travail. L'opportunité de viser l'acte et les équipements ou la réalité de cette protection bicéphale dans les Etats reste en dehors de cette discussion.

- les systèmes contrôlant l'accès de l'utilisateur à l'œuvre, soit par mot de passe, par insertion d'un dispositif hardware ou software, ou par une clé de décryptage;

- les procédures d'authentification qui assurent que l'œuvre constitue bien un original[67];

- le watermarking et toute autre technique consistant à apposer sur l'œuvre des sceaux électroniques ou toute autre information;

- le cryptage de l'œuvre dont le but est de garder l'œuvre confidentielle lors de sa transmission sur les réseaux;

- les outils de contrôle des utilisations de l'œuvre, notamment utilisés pour la facturation des services de *pay-per-view*;

Les régimes juridiques en dehors du droit d'auteur ne seront pas toujours appropriés pour couvrir une gamme aussi large de technologies. Nous le verrons.

Une protection efficace dépend en outre des sanctions et voies de recours offertes. Ce qui constituera notre troisième point de comparaison entre les différents régimes.

b. *Acte de neutralisation / équipements de neutralisation*

Il a souvent été dit que le vrai danger pour les mesures techniques et la protection des oeuvres résidait dans la naissance d'un marché de clés de décryptage, mots de passe, décodeurs, outils d'émulation et autres outils pirates. Les Traités OMPI n'ont pourtant pas pu obtenir un consensus sur ce point et se contentent de viser l'acte de contournement. Une protection strictement équivalente à ces textes internationaux pourrait donc se limiter à la condamnation de la neutralisation d'un dispositif de protection. De nombreux régimes juridiques le permettent. Ils visent soit un acte de contournement tel que défini en droit d'auteur, à savoir le fait d'enjamber une barrière de protection, de la désactiver. Le vocabulaire de ce déplombage diffère selon les régimes qui parlent d'interférence, de décryptage , de décodage, de l'utilisation d'une contre-mesure[68], etc… Tous ces termes renvoient à l'existence d'une barrière entre le contenu et l'utilisateur. La rencontre de l'utilisateur et de la barrière de protection

[67] Ces processus ont constitué l'objet de la majorité des décisions américaines sur base du DMCA. Ces mesures techniques de vérification sont notamment utilisées dans les DVD ou dans les formats Realmedia, ainsi que dans les jeux vidéos. Le principe consiste à ce que l'appareil ou le logiciel de lecture de l'œuvre ne s'enclenche que si le contenu est original et non piraté. Ces procédures permettent également d'effectuer un codage régional, comme dans le cas du DVD.

[68] On trouve également dans les textes anglais les termes descrambling, interfering, breaking, countermeasure, removal.

constitue en conséquence le moment décisif de l'incrimination[69]. Ce qui compte est la méthode utilisée pour avoir accès aux données.

Dans d'autres textes, l'élément déterminant est le fait d'avoir accès au contenu ou aux données de manière non autorisée. Peu importe qu'un dispositif de protection soit violé. Peu importe même dans certains régimes que le contenu soit techniquement protégé. L'incrimination est dès lors plus large que le contournement[70]. On parle alors d'interception, de réception ou d'accès.

Après ce point de vocabulaire, venons-en à la comparaison des différents régime de protection sur base de la distinction acte/équipement. La désactivation d'une mesure technique peut être considérée, dans les limites que nous avons vues plus haut, comme une faute ou une *negligence* et entraîner la responsabilité de son auteur. Il en va de même de la conception et de la commercialisation d'équipements de neutralisation qui soit constituent une faute, soit contribuent à la violation du droit d'auteur (*contributory infringement*).

Le droit de la concurrence déloyale, là où il existe, se révèle d'un moindre secours car il permet surtout de sanctionner les actes commerciaux posés au regard d'équipements désactivant un outil d'un concurrent.

En revanche, l'interception non autorisée est criminalisée par les réglementations relatives aux télécommunications. Certaines lois étendent ce délit à toute réception non autorisée d'un signal ou de données, qu'il s'agisse d'une communication sur une infrastructure de télécommunications ou de signaux de radio ou télédiffusion. Certains Etats exigent que ces signaux soient cryptés, d'autre que leur réception se fasse normalement contre rémunération. Parfois, et c'est souvent le cas en matière de télédiffusion, la protection est hybride et vise également les équipements d'interception. Dans certaines législations, seule la distribution d'équipements est illicite. C'est notamment le cas du texte européen sur la protection de l'accès conditionnel dans les services de radio, télévision ou services de la société de l'information. Seuls les équipements déjouant ces systèmes conditionnant l'accès aux services y sont visés.

Les nouveaux délits ressortissant au droit de la criminalité informatique pénalisent des actes d'accès non autorisés, de contournement d'une mesure technique, ou de manipulation de données informatiques. De plus en plus, ces infractions ne requièrent pas la violation de dispositifs de sécurité, bien que l'existence de ceux-ci prouvera l'absence d'autorisation de l'accès.

La criminalité informatique est donc traditionnellement un régime qui sanctionne l'acte d'accès ou le contournement. La criminalisation des équipements permettant de commettre ces délits a pourtant fait son entrée dans ces dispositions, mouvement qui ne pourra que s'amplifier suite à l'adoption de la

---

[69] G.T. WILLIAMSON, "Domestic provisions analoguous to the anti-circumvention provisions of the DMCA", Draft, 2000, p. 17

[70] ibidem.

Convention du Conseil de l'Europe, premier texte international qui inscrit au titre des infractions informatiques la conception, détention ou diffusion de *hacker tools*.

Lorsque l'acte de neutralisation ou de conception d'un moyen de contournement implique une duplication ou une reproduction du logiciel qui constitue la protection technique, le droit d'auteur sur le logiciel permettra de poursuivre ces agissements. On se trouve ici dans une sanction de la conception des équipements, non de leur commercialisation et dans certains cas, de leur utilisation. La protection par le biais du secret d'affaires ou du savoir faire n'interdira que la diffusion des informations, éléments de la technique de protection.

On peut donc dresser le tableau suivant[71]:

	Neutralisation	Interception/ accès	Equipements
Responsabilité	X	X	X
Concurrence déloyale			X
Criminalité informatique	(X)	X	(X)
Interception de données de télécommunications		X	
Droit de la radio et télédiffusion	(X)	(X)	X
Directive européenne sur l'accès conditionnel			X
Protection par le logiciel			X (conception)
Secret d'affaires			X (divulgation)

[71] Une croix dans le tableau indique qu'une majorité de législations dans ce domaine permettent de sanctionner l'acte en question. Une croix entre parenthèses indique que cette possibilité est prévue dans certaines législations.

c. *Type de mesures techniques*

Les mesures techniques anti-copie seront rarement protégées comme logiciel car elles ne consistent souvent qu'en des signaux insérés dans le support de l'œuvre et reconnus par le lecteur. Par contre, la désactivation de ce signal ou la fabrication et l'offre d'éléments le désactivant pourraient entraîner la responsabilité de son auteur. Si l'offre d'équipements s'effectue dans la vie des affaires, la concurrence déloyale pourra également sanctionner ces pratiques.

Les dispositions relatives aux télécommunications ou à l'audiovisuel ne seront en revanche pas d'un grand secours à moins que le mécanisme empêchant la copie fonctionne lors de la transmission de l'œuvre. Les textes sur l'accès conditionnel ne le seront pas plus. La protection technique ne pourra pas être qualifiée de système d'accès conditionnel. Généralement, l'accès à l'œuvre est déjà licitement obtenu, le système anti-copie n'en restreignant que les usages ultérieurs. En outre, dans la mesure où les contenus dans lesquels sont insérés ces systèmes sont offerts au public, il est difficile de considérer la copie comme une interception non autorisée.

En matière de criminalité informatique, seule l'infraction de fraude pourrait sanctionner la manipulation du mécanisme pour obtenir une copie, avantage patrimonial illicitement obtenu. Par contre, la désactivation du dispositif anti-copie ne pourra être qualifiée d'accès ou de maintien non autorisé, ni d'usage non autorisé d'un ordinateur.

La protection des dispositifs contrôlant l'accès ne manque par contre pas. Législations sur l'accès conditionnel, responsabilité et concurrence déloyale, droit de l'audiovisuel ainsi que la plupart des infractions propres à la criminalité informatique mettront l'auteur en mesure de poursuivre les actes de contournement ou l'offre d'équipements. Par exemple, l'insertion de mots de passe ou de numéros de série obtenus illégitimement sera une fraude informatique. L'infraction d'interception de données de télécommunications fera pareillement l'affaire si le mécanisme d'accès se réalise pendant la transmission des données.

La protection du logiciel ne sera utile que dans certaines hypothèses dans la mesure où de nombreux dispositifs d'accès ne sont que des mots de passe, des codes d'accès ou des procédés de décryptage et non des logiciels. En revanche, lorsque la désactivation d'un contrôle d'accès tel qu'un *dongle* requiert une décompilation ou une altération du logiciel, qui fait l'objet du mécanisme d'accès, le droit de l'auteur sur le logiciel pourra être mis en cause[72]. Une autre hypothèse où le droit sur le logiciel sanctionnera l'acte de contournement est celle où l'accès s'effectue par l'application d'une routine de vérification de la clé d'accès insérée dans le *hardware*, cette routine pouvant être qualifiée de programme d'ordinateur[73].

---

[72] J. KAESTNER, op.cit., p. 6.

[73] Ibidem, p. 7 et la jurisprudence citée en notes 25 à 27.

Le code ou procédé d'accès seront généralement secrets et bénéficieront de la protection des secrets d'affaires. Certains pays connaissent également des infractions spécifiques pour le commerce de mots de passe.

On peut également insérer des signaux dans les œuvres ou crypter les données de telle manière que seul l'original soit reconnu par l'appareil de lecture. La jurisprudence américaine a admis que ces procédés d'authentification jouissaient de la protection du DMCA. Peu d'autres régimes juridiques, à l'exception de la responsabilité et de la concurrence déloyale, dont les limites sont toutefois assez strictes, peuvent également les protéger. Ce processus d'authentification, autrement appelé une "poignée de mains secrète"[74] par une décision américaine, n'est en effet ni un logiciel ni un mécanisme d'accès conditionnel. En effet, si accès il y a, c'est au bien que constitue le support, DVD ou jeu vidéo, et non à un service. En outre, cet accès n'a pas pour objectif de garantir la perception de la rémunération, condition posée par les textes sur l'accès conditionnel, mais d'éviter le piratage.

En outre, à moins de considérer que la tentative d'insérer un disque pirate dans une plate-forme propriétaire est un accès ou un usage non autorisé à celle-ci, les infractions de la criminalité informatique ne seront pas d'un grand secours.

Le watermarking a pour but d'insérer dans l'œuvre des informations sur celle-ci, sur l'auteur ou sur l'utilisation autorisée. Il ne s'agit pas d'un logiciel ni d'un dispositif d'accès. Le seul recours légal contre une suppression de ces informations ou une désactivation du marquage, outre la mise en cause de la responsabilité du pirate, sera l'infraction d'altération ou de suppression des données informatiques là où elle existe. En outre, si l'acte de piratage consiste non à supprimer les données mais à rendre le logiciel de lecture de ces données inactif, il pourra s'agir d'une altération ou d'une décompilation non autorisée du programme[75].

Lorsque l'œuvre est cryptée lors de la transmission sur les réseaux, son décryptage non autorisé est passible de poursuites pour interception de données de télécommunications et de données cryptées, accès non autorisé, fraude informatique, altération de données informatique et de décryptage non autorisé de signaux de télédiffusion si la transmission s'effectue par ce mode. La commercialisation de clés de décryptage pourra constituer un acte de concurrence déloyale ou une violation du secret d'affaires.

Enfin la désactivation des mécanismes de contrôle des utilisations, notamment dans les systèmes de *pay-per-view*, pourrait être considérée comme un délit de suppression ou d'altération des données informatiques ou comme un cas de fraude informatique. L'infraction de maintien non autorisé dans un système informatique, telle qu'elle existe en droit belge et français, serait particulièrement adaptée à la répression de ce type de manipulations. Dans un autre contexte, un tribunal français[76] a condamné sur

---

[74] J. GINSBURG, op.cit.

[75] J. KAESTNER , op.cit., p. 26.

[76] Trib. Corr. Paris, 5 novembre 1996, *Expertises*, n° 202, fév. 1997, p. 81.

cette base des personnes qui se connectaient en toute légalité à des jeux télématiques dans le seul but de bénéficier de jetons de présence qui leur ouvraient le droit à certains cadeaux. Ces jetons n'étaient toutefois comptabilisés au crédit de l'utilisateur qu'en fonction de la durée de la connexion, durant laquelle l'utilisateur devait pratiquer le jeu à défaut de quoi le système se déconnectait automatiquement. Pour gagner ces jetons sans avoir à jouer durant de longues heures, ils désactivaient le système de déconnexion automatique grâce à un mécanisme de rafraîchissement d'écran.

Ces mécanismes de monitoring pourront en outre être qualifiés de logiciel dans certaines hypothèses et bénéficier de la protection qui s'ensuit.

	Anti-copie	Contrôle d'accès	Authentifi-cation	Watermar-king	Cryptage	Monitoring
Responsabilité	X	X	X	X	X	X
Concurrence déloyale	X	X	X	X	X	X
Accès non autorisé		X			X	
Maintien non autorisé		X				X
Fraude informatique	X	X			X	X
Suppression de données informatiques	X		X	X	X	X
Interception de données de télécommunications					X	
Droit de la radio et télédiffusion		X			X	
Directive européenne sur l'accès conditionnel		X				
Protection par le logiciel		(X)	X			X
Secret d'affaires		X			X	

d. *Sanctions et titulaire de l'action*

La majorité des textes que nous avons abordés sont des dispositions pénales. Intercepter des données, accéder à un système informatique, manipuler ou supprimer des données, décrypter un signal de télédiffusion, offrir des mécanismes permettant de déjouer un système d'accès conditionnel constituent dans bien des pays des infractions passibles d'amendes et de peines d'emprisonnement.

Si cette qualification pénale revêt un caractère dissuasif non négligeable, cela ne doit toutefois pas occulter le fait que la procédure pénale est une lourde et lente machine dans de nombreux systèmes judiciaires. L'auteur a souvent plus intérêt à pouvoir stopper les agissements illicites, plus particulièrement lorsqu'il assiste au développement d'un marché illicites de décodeurs, décrypteurs ou autres machines pirates qui ont tôt fait de réduire l'effectivité de sa protection technique à néant. Il est donc essentiel que des actions en cessation, des injonctions et autres actions sur requête rapides et répondant à l'urgence soient ouvertes aux parties lésées, ainsi que des actions en dommages et intérêts.

Les rapports nationaux ne nous ont toutefois pas mis en mesure de nous former une idée d'ensemble sur cette question mais il est probable qu'une telle action en urgence et susceptible d'aboutir à l'arrêt immédiat des activités illicites et à la saisie des équipements pirates soit ouverte sur base de la concurrence déloyale, de droit de la responsabilité, du droit de l'audiovisuel ou des dispositions relatives à l'accès conditionnel, du droit d'auteur sur le logiciel et du secret d'affaires.

Quant à la possibilité pour l'auteur d'intenter une action, cela ne fait certainement pas de difficulté en matière de concurrence déloyale ou de droit de la responsabilité. Le droit de l'audiovisuel prévoit dans certaines législations cette faculté, dans d'autres, réserve l'action au télédiffuseur. Les voies de recours dans les dispositions européennes sur l'accès conditionnel bénéficient au prestataire de service, mais nous avons vu que ce dernier pourra être dans de nombreuses hypothèses le titulaire de droits sur le contenu.

Si la protection est recherchée par le droit sur le logiciel de protection technique, à première vue seul l'auteur de ce programme, soit le fournisseur de la technologie, pourra intenter l'action en contrefaçon, à moins que la législation sur les logiciels n'ouvre les voies de recours à tout intéressé. En matière de secret d'affaires, seule la personne à l'origine du secret pourra en attaquer la divulgation. Il s'agira principalement du fournisseur de la technologie de protection, détenteur des secrets liés à sa conception et à son fonctionnement.

2. UNE PROTECTION ADEQUATE DES MESURES TECHNIQUES

2.1. La place des régimes juridiques alternatifs dans la protection des mesures techniques : un rôle de figuration ou un premier rôle ?

Nous venons de voir combien la protection des mesures techniques sous le prisme de régimes juridiques autres que le droit d'auteur faisait figure de kaléidoscope. Le rapport australien parle de patchwork dont la protection ne présente pas une vue d'ensemble cohérente. Nous ne pouvons que souscrire à ce point de vue.

Si ces régimes alternatifs peuvent toutefois être d'un quelconque secours aux auteurs, c'est essentiellement sur deux plans. D'une part, ils peuvent combler des lacunes des dispositions du droit d'auteur en matière de mesures techniques, par exemple parce qu'ils permettent de poursuivre l'acte de contournement dans les pays où ce dernier n'est pas visé en droit d'auteur[77], ou parce qu'ils englobent des dispositifs techniques utilisés par les auteurs mais qui peuvent être difficilement qualifiés de mesures techniques protégeant leurs droits.

Dans ces hypothèses, la criminalité informatique, le droit des télécommunications ou de l'audiovisuel, l'accès conditionnel, le secret d'affaires peuvent certainement constituer des adjuvants salutaires à la protection anti-contournement du droit d'auteur. Le tableau de comparaison que nous avons dressé, si on le met en perspective avec les dispositions du droit d'auteur, permet d'ailleurs de déceler très vite là où une disposition juridique comble un manque.

Mais ces institutions juridiques peuvent prendre une place bien plus importante dans un régime de protection des mesures techniques. Les Etats peuvent en effet décider que ces régimes remplissent l'objectif de protection des Traités OMPI[78]. En conséquence, la criminalité informatique, la protection des services d'accès conditionnels, le droit de la concurrence déloyale hébergeraient les sanctions contre la neutralisation des mesures techniques destinées à protéger les droits des auteurs. Les Traités OMPI ne l'interdisent pas[79]. Seule exigence : que la protection soit appropriée et comporte des sanctions efficaces.

---

[77] C'est le cas de l'Australie dont le rapport soulève l'utilité de régimes alternatifs de protection dans ce cas.

[78] Dans le chœur des critiques contre la protection des mesures techniques en droit d'auteur, quelques voix se sont élevées et ont dénoncé l'inutilité d'une protection spécifique et nouvelle, estimant soit que le droit existant répondait déjà suffisamment aux craintes des titulaires de droits, soit que d'autres régimes juridiques étaient plus à même de le faire. Certains voyaient cette protection dans la criminalité informatique, d'autres dans la concurrence déloyale ou dans la législation européenne sur l'accès conditionnel. Selon ces auteurs, la protection conférée par ces régimes juridiques soutiendrait la comparaison avec celle envisagée par les Traités OMPI ou à tout le moins, accorderaient une réponse adéquate aux risques de piraterie. Voir M. LEDGER & J.P. TRIAILLE, "Dispositions contre le contournement des dispositifs de protection technique", Rapport belge pour les Journées d'Etude de l'ALAI, *Le Droit d'auteur dans le Cyberespace*, Amsterdam, Juin 1996. Texte non inclus dans la publication des actes, p. 12; W. GROSHEIDE, op.cit., p. 403; K.J. KOELMAN & N. HELBERGER, op.cit., p. 222.

[79] Intervention de KURT KEMPER, Atelier sur la mise en œuvre des Traités OMPI, 6-7 décembre 1999, Genève.

De multiples options s'offrent donc au législateur national. La satisfaction de l'objectif de protection peut se réaliser par une transposition spécifique dans le corpus du droit d'auteur –option classique préférée par de nombreux Etats–, ou dans un régime juridique autre, que les dispositions visent particulièrement les atteintes aux moyens techniques utilisés contre la contrefaçon ou englobent de manière plus générale, dans une optique de sécurité informatique, tout type d'atteintes portées aux barrières techniques. La transposition peut être exclusive à un domaine juridique, droit d'auteur ou autre, ou être hybride. Dans cette dernière hypothèse, la protection peut être cumulative, l'application des dispositions juridiques différentes s'additionnant, ou distributive, certains dispositifs étant protégés par le droit d'auteur, d'autres par une autre institution. C'est le cas du Japon qui a partagé les sanctions pour les équipements de neutralisation entre le droit d'auteur et la loi sur la concurrence déloyale, à la logique du dispositif technique répondant la logique différente de l'une et l'autre protection.

Les Etats peuvent en outre garantir que leur arsenal législatif accorde déjà une protection appropriée et effective, que ce soit par le droit d'auteur ou non. C'est la réponse qu'avait donnée la France aux autorités communautaires chargées de contrôler la transposition de la directive de 1991 sur la protection des programmes d'ordinateur. La France, qui n'avait pas introduit de dispositions spécifiques à l'interdiction des équipements de neutralisation des dispositifs de sécurité des logiciels, si ce n'est une réglementation de la publicité de ces équipements, estimait que le régime de la complicité pour contrefaçon, en vertu d'une jurisprudence claire[80], permettait de poursuivre de manière satisfaisante les vendeurs de tels équipements[81].

La directive européenne sur le droit d'auteur et les droits voisins dans la société de l'information laisse, à notre avis, une liberté semblable aux Etats membres, puisqu'elle n'impose, dans la droite ligne des textes de Genève, qu'une protection juridique appropriée. Rien n'indique une obligation pour les Etats de l'Union d'intégrer l'interdiction du contournement et des équipements destinés à cet effet dans l'arsenal législatif du droit d'auteur. A première vue, l'éventail des possibilités de transposition, ouvert par l'OMPI, subsiste, sous réserve du respect des autres obligations communautaires. Une limite s'impose toutefois. L'article 8 du texte européen prescrit des sanctions et des voies de recours appropriées contre les atteintes aux droits et obligations prévues par la directive, ceci incluant les dispositions relatives aux mesures techniques. Les Etats doivent notamment faire en sorte que les titulaires de droit puissent intenter une action en dommages et intérêts et demander qu'une ordonnance sur requête soit rendue. Les équipements de neutralisation doivent également pouvoir faire l'objet d'une saisie. Il est donc indispensable que le régime choisi pour la transposition de l'article 6 relatif aux mesures techniques comporte de telles voies de recours. Le droit pénal informatique ne pourra par exemple pas remplir l'ensemble de ces exigences.

---

[80] Paris, 4ème ch., 20 octobre 1988, *Sem. Jur.*, 1989, éd. G, Jurisprudence, n°21188.

[81] A. LUCAS, *Droit d'auteur et Numérique*, Droit@Litec, Paris, 1999, p. 269 et suiv.

2.2. Les conditions d'une protection appropriée

a. L'objectif de la protection

C'est certainement sur ce critère que l'adéquation du régime juridique aura le plus de mal à se faire une raison. L'objectif de chaque domaine de protection justifie son paradigme, son étendue et ses limites qui risquent de ne pas faire bon ménage avec une préoccupation générale de protection des droits des auteurs. Seules les dispositions anti-contournement propres au droit d'auteur embrassent un objectif large de protection des œuvres. Cela va de soi. En conséquence si l'on souhaite juger de l'adéquation d'un autre type de protection au seul regard de la lutte contre la piraterie et la contrefaçon, le choix d'un régime spécifique au droit d'auteur semble s'imposer. Mais si l'on examine d'un peu plus près les justifications des autres institutions légales, on verra qu'elles ne sont pas toujours étrangères à des préoccupations soulevées lors des discussions relatives aux mesures techniques.

L'arsenal répressif de la criminalité informatique ne se préoccupe que de la sécurité des réseaux et systèmes dont les dispositifs techniques, quels qu'ils soient, ne sont qu'un élément. Ce sont donc les agissements qui portent atteinte à cet idéal de sécurité et de confiance qui sont la cible de la répression. Il s'agit d'une vision très extensive puisque toute violation d'un système ou d'une architecture informatique est punissable quel qu'en soit le contenu.

La protection des données qui transitent par les réseaux de télécommunications vise à garantir le secret des communications et la sécurité des transmissions. Ce qui explique que l'interception, voire la divulgation, des données, constitue l'acte répréhensible et non l'atteinte à une protection technique.

Le droit de l'audiovisuel, ainsi que la protection récente de l'accès conditionnel, ont pour ambition d'assurer la rémunération des services ainsi prestés à distance contre condition de paiement ou autre. La justification de cette protection est de garantir les intérêts économiques des prestataires de ces services, préoccupation assez proche des intérêts des titulaires de droits, producteurs et diffuseurs relativement à la distribution des œuvres.

Le régime de la concurrence déloyale ou de manière assez proche, la doctrine américaine du *staple articles of commerce*, permet de réglementer un marché et d'assurer une saine concurrence entre des activités économiques parallèles. L'usage d'une mesure technique pour protéger un contenu est alors un exercice de la liberté d'entreprise qui ne peut *a priori* empêcher un exercice parallèle de la liberté d'un autre acteur du marché. Ce paradigme explique la limitations des sanctions aux seules activités commerciales et l'instauration de moyens d'action généralement rapides.

Si la protection des mesures techniques répond également à ces objectifs, elle pourrait trouver sa place dans un régime autre que le droit d'auteur.

b. *La définition des mesures techniques protégées*

Les Traités OMPI n'évoquent que les *"mesures techniques efficaces qui sont mises en œuvre par les auteurs dans le cadre de l'exercice de leurs droits et qui restreignent l'accomplissement d'actes qui ne sont pas autorisés par les auteurs concernés ou permis par la loi*". Il ne s'agit donc que de protéger les dispositifs qui assurent l'effectivité des droits des auteurs et titulaires de droits voisins. La plupart des transpositions de ce texte vont bien au-delà et protègent également tout dispositif technique qui contrôle l'accès aux œuvres, ainsi que d'autres techniques qui n'ont pas pour objectif premier d'empêcher la reproduction, la communication au public et autres actes soumis au monopole de l'auteur. Nous en avons vu des exemples précédemment. Qu'on juge cette extension adéquate ou non, est une question essentielle à l'instauration d'une protection des mesures techniques. La réponse qu'on donnera à cette question fera en sorte d'exclure certaines institutions légales du choix d'un régime de protection. Les régimes de protection institués dans d'autres dispositifs légaux ne couvrent en effet pas expressément les mécanismes empêchant les droits des auteurs. Cela va de soi. L'objet de ces protections est plutôt relatif à une technique particulière, par exemple le cryptage, quelle qu'en soit la fonction, ou à des actes d'accès spécifiques.

L'adéquation de la protection au regard des techniques que l'on souhaite atteindre doit donc se poser en deux étapes. En premier lieu il est indispensable de déterminer quels types de mécanismes et quelles fonctions sont dignes d'une protection. Ensuite, si le choix de la protection se porte, en partie ou en totalité, sur un régime autre que la propriété littéraire et artistique, dans quelle mesure ces dispositions recouvrent ces mesures techniques jugées essentielles.

C'est sans doute sur ce critère que l'élection d'une protection adéquate se révélera la plus ardue tant nous avons vu qu'en dehors des dispositions anti-contournement du droit d'auteur, la couverture légale des multiples types de systèmes techniques utilisées par les auteurs montrait une image fragmentée.

Toutefois, le choix du type de mesures techniques méritant une protection peut de manière pertinente trancher en faveur d'une couverture distributive. Par exemple, les mesures techniques protégeant strictement les droits des auteurs feraient l'objet de dispositions en droit d'auteur. Quant aux dispositifs contrôlant l'accès aux œuvres ou aux services, ils s'intégreraient mieux dans un autre régime juridique. Une telle approche présenterait l'avantage d'évacuer la délicate question du contrôle de l'accès aux œuvres en droit d'auteur.

c. *L'étendue de la protection : acte ou équipement*

Il suffit de voir les différences de transposition des Traités de 1996 sur le seul critère déjà de l'objet de l'interdiction (acte et/ou équipement) pour juger de la difficulté d'une acception uniforme du terme de "protection appropriée". L'Australie a par exemple jugé que la seule réglementation des équipements de neutralisation constituait une réponse suffisante. Le Japon limite l'acte de neutralisation illicite aux agissements accomplis dans un but commercial[82].

[82] TERUO DOI, "WIPO Copyright Treaty and Japanese Copyright Law: A comparative analysis", *R.I.D.A.*, n°186, Octobre 2000, p. 203.

Ce critère peut donc déjà à lui seul faire pencher la balance en faveur d'un régime juridique ou d'un autre.

d. Les limitations de la protection

La protection des mesures techniques ne peut faire l'économie d'une réflexion sur ses propres limites. Le choix du terme "approprié" n'est pas neutre dans les Traités de l'OMPI. Il ne s'agit pas seulement d'édicter une protection effective et forte mais aussi de l'inscrire dans la philosophie générale du droit d'auteur, dans l'équilibre nécessaire qui y préside, et ce même si cette protection peut en définitive trouver abri dans un autre domaine juridique. Les dispositions anti-contournement doivent être proportionnées, cela est répété à l'envi dans les travaux préparatoires des Traités OMPI ou de la directive européenne.

En conséquence, la question des limites à la protection se doit d'être posée dans l'examen de l'adéquation de la protection. Sans doute, est-ce une question fort délicate. Elle l'est déjà lorsqu'on opte pour une protection des mesures techniques dans le champ du droit d'auteur. Elle l'est davantage si l'on se tourne vers un autre régime. Sans parler de la question subsidiaire de la validité des exceptions aux droits des auteurs en tant que limites à la protection des mesures techniques en dehors de la propriété littéraire et artistique.

Thomas Heide[83] plaide en tout cas pour que les exceptions, lorsqu'elles sont déclarées impératives, et c'est le cas pour certaines exceptions de l'acquis communautaire européen, s'imposent à tout acte contractuel qu'il se situe dans un schéma de droit d'auteur ou non, par exemple en matière d'accès conditionnel. De là à ce qu'une exception mette en échec une barrière et la sanction de son ouverture hors du droit d'auteur, il y a un large pas qu'on ne saurait franchir si aisément. A moins de militer clairement en faveur d'une limitation expresse de certains régimes par les exceptions du droit d'auteur[84].

Les exceptions en droit d'auteur ne sont pas des atomes libres. Si elles constituent des pans essentiels de la propriété littéraire et artistique, elles n'en sont pas moins indissociables de l'exercice des droits exclusifs et de la philosophie fondatrice du droit d'auteur. Elles ne pourront donc être transposées telles quelles aux autres régimes juridiques, dont les objectifs sont d'ailleurs très différents.

La cybercriminalité garantit la sécurité des réseaux et systèmes informatiques. L'exception au droit d'auteur n'y a pas sa place. Ce qui importe est que la barrière de protection ait été enfreinte, quelle qu'en soit la raison. Un bémol toutefois à cette affirmation: l'exception qui justifierait un acte de contournement ou un accès non autorisé pourrait intervenir dans l'appréciation de l'élément moral de l'infraction, fraude ou autre élément intentionnel.

---

[83] TH. HEIDE, "The approach to innovation under the proposed copyright directive: Time for mandatory exceptions ?", [2000] *I.P.Q.*, No 3, p. 228

[84] Pour un exemple en matière d'accès conditionnel, TH. HEIDE, "Access Control and Innovation under the Emerging EU Electronic Commerce Framework", (2000) *B.T.L.J.*, Vol. 15, No. 3, p.1046.

S'agissant de la protection des services cryptés ou à accès conditionnel, l'objectif est ici d'assurer la rémunération ou toutes autres conditions mises à l'octroi du service. En pareille hypothèse, l'exception du droit d'auteur ne peut avoir aucune incidence puisqu'elle ne s'exerce qu'une fois la prestation du service accomplie.

Si l'on poursuit les équipements de contournement par le droit de la concurrence déloyale, la situation pourrait se présenter de manière légèrement différente. L'objectif de la protection est de réglementer les activités concurrentes sur un marché dans la seule mesure où certains actes iraient au-delà de la liberté d'entreprise. En toute hypothèse, des exceptions qui, en droit d'auteur, traduisent le souci de préserver la concurrence[85], telle que l'exception de décompilation relative aux logiciels, devraient pouvoir être accueillies puisqu'elles justifient la légitimité de l'acte posé au regard de la concurrence saine.

Ce dernier exemple montre que ce ne sont pas réellement les exceptions telles que prescrites par le droit d'auteur qui sont susceptibles d'être transposées à d'autres domaines juridiques mais bien plutôt les considérations fondamentales qui les sous-tendent, liberté d'expression, liberté de recevoir de l'information, liberté d'entreprise, qui peuvent justifier une défense similaire face à une action pour contournement d'un dispositif technique.

En Europe, par exemple, la liberté de recevoir des informations justifie dans certains pays l'exception pour les comptes-rendus d'actualité. Le même fondement est reconnu aux dispositions de la directive Télévision Sans Frontières[86] qui imposent d'émettre en clair certains événements d'importance majeure[87]. Aux Etats-Unis, le Premier amendement, qui justifie de nombreuses tentatives de défense face aux dispositions du DMCA, peut également être invoqué à l'encontre d'autres régimes.

Ces hypothèses resteront rares et aléatoires puisqu'elles dépendront de l'interprétation du juge. Par exemple, dans une affaire néerlandaise en matière de décodeurs pirates, la *Hoge Raad* n'a pas accepté l'argument selon lequel la fourniture d'informations permettant de concevoir des décodeurs était immunisée en vertu de la liberté de recevoir de l'information qui justifiait la réception libre de programmes de télévision cryptés[88].

Dès lors, l'admissibilité de limites à la protection des mesures techniques, en ce compris des limites basées sur des droits fondamentaux tels qu'en matière d'exceptions au droit d'auteur, devrait être un critère essentiel de l'adéquation de celle-ci. Opter pour un régime juridique qui n'accepte que peu ou prou des limitations, qu'elles résultent des libertés fondamentales, d'intérêts publics ou des exceptions au droit d'auteur, est un choix politique non dépourvu de conséquences. Le rapporteur australien en

---

[85] TH. HEIDE, "The approach to innovation …" , op.cit.

[86] Directive du Conseil et du Parlement européens 97/36/CE du 30 juin 1997, modifiant la Directive du Conseil 89/552/CEE sur la .

[87] N. HELBERGER, op.cit.

[88] W. GROSHEIDE, op.cit., p. 408

convient et dénonce le risque d'une protection hors du droit d'auteur qui ferait fi de ses limites. En revanche, le rapport français y voit un avantage non négligeable pour les auteurs qui pourraient fonder une action anti-contournement sur une autre base que le droit d'auteur, sans crainte de s'en voir opposer les exceptions[89]. Ces deux points de vue opposés soulignent la nécessité d'une réflexion sur cette question, pourtant généralement absente des discussions en dehors du droit d'auteur. Le démontre l'adoption de la directive européenne sur la protection de l'accès conditionnel qui s'est effectuée de manière rapide et presque inaperçue, sans que jamais la question de la possible mainmise sur des éléments du domaine public ou le verrouillage d'actes autorisés en droit dauteur n'ait déchaîné les passions qu'a suscitées en revanche la directive sur le droit d'auteur. Or, si la protection d'une mesure technique est en butte à une exception au droit d'auteur[90], qu'est-ce qui empêche les auteurs de fonder l'action sur la protection des services à accès conditionnel qui ne connaît pas de telles limites ?

3. CONCLUSION

Notre tour d'horizon des dispositions anti-contournement est désormais terminé. Il aura en tous cas permis, il nous semble, de réhabiliter le droit d'auteur en tant que régime de protection approprié. Car si la sanction des actes de contournement ou des activités préparatoires est généralement possible dans chacun des territoires juridiques que nous avons traversés, de nombreuses difficultés et approximations subsistent. Au premier chef de ces approximations se trouve la pertinence de la démarche qui consiste à glaner de ci, de là, des éléments de protection dont l'objectif et les modalités sont très éloignées du droit d'auteur et surtout de tenter de les conformer à une toute autre logique. Les outils qu'on appelle ainsi à la rescousse ne peuvent qu'en être dénaturés et affaiblis. A force de tordre les concepts juridiques, on ne devra pas s'étonner qu'on arrive à des solutions tordues.

Une deuxième difficulté est la quasi-absence de limitations dans ces autres régimes, ou à tout le moins le manque de réflexion à cet égard. Le choix de ces institutions juridiques pour une protection contre le contournement ne pourra toutefois satisfaire le critère des Traités OMPI, soit la protection appropriée, que si l'équilibre inhérent au droit d'auteur s'y retrouve. Sur ce point, la balance penche facilement en faveur d'une transposition des dispositions anti-contournement en droit d'auteur. C'est en effet le seul lieu où des débats ont été menés sur le sort des exceptions, que les résultats de ces débats puissent être jugés décevants ou encourageants.

Ceci révèle combien le problème des exceptions face aux mesures techniques et aux dispositions anti-contournement constitue une question clé. Question qui trouve tout naturellement en droit d'auteur son épicentre, dont les vagues devraient pourtant se ressentir dans les autres domaines. Car s'il suffisait, pour sanctionner un contournement, de se tourner vers une autre technique de protection pour éviter les difficultés relatives à l'admission d'exceptions, à quoi serviraient donc tous ces efforts législatifs

---

[89] voir également, A. LUCAS, *Droit d'auteur et Numérique*, Droit@Litec, Paris, 1999, p.274.

[90] dans l'hypothèse où les exceptions ont un tel pouvoir, ce qui est loin d'être évident dans le texte européen.

pour régler le sort des limitations au droit d'auteur dans un monde de verrouillage technique? Il faut reconnaître que c'est une question particulièrement complexe dont la considération en dehors de la propriété littéraire et artistique peut paraître malvenue. Mais si les régimes juridiques s'enchevêtrent, leurs justes limites en feront tout autant.

La protection en droit d'auteur semble en conséquence un choix judicieux et équilibré. Toutefois, cela n'empêche que les dispositions anti-contournement propres au droit d'auteur puissent être limitées à leur objectif légitime: la protection des droits des auteurs. Et que les mesures techniques qui poursuivent une autre fonction, même si indirectement la sécurité des œuvres y trouve son compte, trouvent une protection dans des législations plus aptes à rencontrer ces autres préoccupations. Ce pourrait par exemple être le cas des systèmes qui contrôlent l'accès aux œuvres.

L'objectif de protection des œuvres, particulièrement à l'ère des réseaux, autorise donc des allées et venues entre dispositions de droit d'auteur et autres régimes juridiques. Ce va-et-vient pourrait combler des lacunes de protection, couvrir différents outils techniques ou permettre à d'autres personnes que le titulaire de droits d'agir. Il ne doit toutefois pas aboutir à une surprotection qui rendrait les dispositifs de protection technique plus impopulaires qu'ils ne le sont déjà aujourd'hui.