LE CONTOURNEMENT DES MESURES TECHNIQUES DE PROTECTION, CONTREFAÇON OU CRIMINALITE INFORMATIQUE

- JUIN 2003 -

Par Isabelle Vaillant, juriste.

Introduction

1. Le développement des nouvelles techniques permet désormais de protéger les œuvres contre la copie ou l'accès non autorisé. Se pose alors la question de savoir quel mécanisme juridique appliquer lors du contournement de tels dispositifs.

2. La Directive 2001/29/CE du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (ci-après la Directive), qui doit être transposée en droit français, impose en son article 6 de sanctionner les actes de contournement des mesures techniques de protection. Ces dispositions ont soulevé bien des inquiétudes depuis lors, s'agissant notamment de la possibilité pour les utilisateurs de jouir librement de l'œuvre qu'ils ont acquise. Comment interpréter un tel acte de neutralisation d'une mesure technique de protection d'une œuvre ? Quelle répression doit alors s'imposer ? Le droit français ne permet-il pas déjà de réprimer de tels agissements ? Afin de savoir si la législation française existante est apte à s'appliquer dans ces circonstances, il faut tout d'abord déterminer dans quelle mesure les prescriptions de la Directive sont contraignantes et exigent ou non une transposition. En effet, le but d'une directive communautaire est d'assurer un certain objectif d'harmonisation, tout en réservant aux Etats membres les moyens d'y parvenir. Cependant, il faut, semble-t-il, malgré tout transposer obligatoirement la directive, dans son intégralité.

3. Ainsi a-t-il été jugé que « s'*il est constant que, en droit français, il existe des règles déjà anciennes* […]*, telles que celles prévues par la directive, il n'en demeure pas moins qu'il incombe aux autorités nationales responsables de la transposition de la directive de veiller à ce que de telles règles assurent effectivement, de manière suffisamment claire et précise, la pleine application de la disposition communautaire en cause* »[1].

Et ceci même si « *selon une jurisprudence constante de la Cour, la transposition en droit interne d'une directive n'exige pas nécessairement une reprise formelle et textuelle de ses dispositions dans une disposition légale ou réglementaire expresse et spécifique et peut se satisfaire d'un contexte juridique général, dès lors que celui-ci assure effectivement la pleine application de la directive d'une façon suffisamment claire et précise* »[2].

Le texte de transposition de l'article 6 de la Directive pourrait donc se contenter d'opérer un renvoi – s'agissant de la répression des actes de contournement de mesures techniques de protection – aux dispositions existantes du Code pénal en matière de fraude informatique. La création en France d'un mécanisme spécifique pour assurer la transposition de ces dispositions ne s'avère pas indispensable, dès lors qu'il existe déjà un cadre juridique général assurant ces objectifs.

4. Il apparaît en effet que les mesures techniques de protection sont déjà protégées par le droit français, tant d'un point de vue civil que pénal (1). Par ailleurs, la transposition de l'article 6 de la Directive a sa place, non dans le Code de la propriété intellectuelle, mais dans le Code pénal, l'assimilation du contournement des mesures techniques à de la contrefaçon étant impropre (2). Enfin, les incriminations actuelles – et futures – en matière de fraude

---

[1] CJCE, 6 avril 2000, Commission/République française, aff. C-256/98, n° 36, concernant la directive n° 92/43/CEE relative à la conservation des habitats naturels ainsi que de la faune et de la flore sauvages (JO L 206, p. 7).

[2] CJCE, 15 nov. 2001, Commission/Italie, aff. C-49/00, Rec. p. I-8575, point 21, concernant la directive n° 89/391/CEE relative à la mise en oeuvre de mesures visant à promouvoir l'amélioration de la sécurité et de la santé des travailleurs au travail (JO L 183, p. 1).

informatique permettent de répondre pleinement aux objectifs de l'article 6 de la Directive (3).

1. LES MESURES TECHNIQUES SONT D'ORES ET DEJA PROTEGEES PAR LE DROIT FRANÇAIS, A DEUX NIVEAUX

Les Traités de l'OMPI sur le droit d'auteur et sur les interprétations et exécutions et les phonogrammes du 20 décembre 1996, ainsi que la Directive européenne du 22 mai 2001, n'imposent pas d'introduire la protection des mesures techniques contre le contournement dans la législation sur la propriété intellectuelle. Or il s'avère que les mesures techniques de protection se trouvent être déjà protégées en droit français, d'une part par le droit civil (1.1), et d'autre part par le droit pénal (1.2).

1.1. La protection par le droit civil

Le droit civil permet la protection des mesures techniques par le biais de plusieurs mécanismes.

- Le droit civil protège les mesures techniques de protection tout d'abord par le biais du **contrat**[3].

Il est en effet possible d'établir des obligations contractuelles dans les contrats de licence, imposant à l'utilisateur l'obligation de ne pas contourner les mesures techniques ou de ne pas modifier des informations sur le régime des droits. En cas d'inexécution de ces obligations, l'utilisateur engagera sa **responsabilité contractuelle**.

Toutefois, il est évident que ces obligations contractuelles ne sauraient conférer aux titulaires plus de droits que la loi ne leur en confère. Ainsi, un contrat ne saurait protéger davantage une œuvre tombée dans le domaine public, ni interdire la décompilation de logiciels aux fins d'interopérabilité.

- Le droit civil protège également les mesures techniques par le biais de la **concurrence déloyale** et du **parasitisme**.

Le mécanisme de la **concurrence déloyale** peut permettre de sanctionner toute forme de fabrication ou de distribution de matériels de contournement des mesures techniques de protection. La concurrence déloyale sanctionne en effet le non-respect d'un devoir, par un acteur économique, dans l'exercice de la concurrence, de la liberté du commerce. Ce manquement est constitutif d'une faute dommageable engageant la responsabilité civile de son auteur sur le fondement des articles 1382 et 1383 du Code civil. Il s'agira alors de

[3] Christophe Caron, « *Brèves observations sur la protection des mesures techniques par le droit civil* », Actes du Congrès de l'ALAI, New York 13-17 juin 2001.

démontrer une faute (la commission d'actes déloyaux tels que dénigrement, risque de confusion, désorganisation interne de l'entreprise concurrente, désorganisation du marché…), un préjudice (confusion, trouble commercial…) et un lien de causalité entre les deux.

La situation requiert un rapport de concurrence - clientèle identique, produits similaires ou substituables - et des activités économiques. Tel sera le cas s'agissant des dispositifs de contournement de mesures techniques protégeant des logiciels.

➢ Ainsi, le 22 mai 1998, le Tribunal de grande instance de Paris[4] a reconnu coupable de **concurrence déloyale** celui qui avait **fourni les moyens de contourner une mesure technique protégeant un logiciel** encyclopédique, provoquant une perte de chiffre d'affaires pour la société éditrice dudit logiciel.

➢ Le 22 mai 1991, un arrêt de la chambre commerciale de la Cour de cassation[5] a rejeté le pourvoi formé contre une décision condamnant une société sur le fondement de la **concurrence déloyale**, pour avoir commercialisé des **programmes de « *déplombage* »** de logiciels, ces actes étant source de perte de chiffre d'affaires pour l'entreprise.

➢ L'arrêt de la Cour d'appel de Paris du 20 octobre 1988[6] a quant à lui déclaré que la **mise en vente de copies obtenues par le biais de programmes permettant d'annihiler l'efficacité d'un dispositif anti-copie d'un logiciel** était constitutive de **concurrence déloyale**, dont il était établi que toutes les conditions étaient réunies :

- Les auteurs des mesures de contournement étaient des concurrents des auteurs du logiciel : leurs produits avaient le même objet que le produit d'origine, la clientèle visée était identique.
- La faute consistait dans la commercialisation de copies illégales du produit en question, sans droit.
- Le dommage consistait dans la mise en vente des copies, constituant une « *source de perte de chiffre d'affaires* » pour l'entreprise, qui subissait un « *acte de concurrence déloyale par désorganisation de l'entreprise* ».
- Dès lors, le lien de causalité entre cette faute et le dommage était démontré.

Par conséquent, la société était « *fondée, par référence à l'article 1382 du Code civil, à réclamer réparation de tout acte fautif de nature à entraver la commercialisation de* [ses] *logiciels* ».

➢ De même, de nombreuses décisions ont pu condamner, en **Allemagne**, sur le fondement de la concurrence déloyale, la distribution d'équipements de contournement d'une mesure technique protégeant des œuvres, ainsi que le contournement lui-même s'il était suivi d'une distribution commerciale des logiciels ainsi « *déprotégés* »[7]. La

---

[4] TGI Paris, 22 mai 1998, Expertises, juillet 1998, p. 211.

[5] Cass. com., 22 mai 1991, Artware, PC Mart / La Commande Electronique et autres, Bull. civ. IV, n° 172 ; JCP 1992, éd. G, II, 21792, obs. J. Huet.

[6] CA Paris, 20 oct. 1988, JCP G 1989 n° 10, II, 21188, note X. Linant de Bellefonds ; JCP E, 1990, n° 16-17, II, 15751, p.265, note M. Vivant et A. Lucas.

[7] Séverine Dusollier, Actes du Congrès de l'ALAI, New York 13-17 juin 2001, p. 158 ; p. 1284.
OLG Stuttgart, CR 5 (1989), 685-688 "*Feilhalten von Hardlock-Entfernern*" [Offering of Hardlock Removing Devices]; OLG Düsseldorf, GRUR 91 (1989), 535-536 "*Hardware-Zusatz*" [Matériel auxiliaire]; LG München, CR 11 (1995), 669-671 "*Dongle*", *aff'd*, OLG München, CR 12 (1996), 11-18 "*Dongle*", *aff'd*, BGH GRUR 98 (1996), 78-79; OLG München, CR 11 (1995), 663-665 "*UNPROTECT*"; OLG München, CR 9 (1993), 31 "*Multifilter*"; OLG Frankfurt am Main, NJW 49 (1996), 264-265 "*Piratenkarte*" [Carte Pirate].

distribution de dispositifs de contournement des mesures de protection contre la copie, de clefs physiques imitant la clef originale d'accès au programme, ainsi que sa suppression, ont ainsi été réprimées.

Le **parasitisme**, quant à lui, permet de sanctionner le fait, pour un acteur économique, de vivre dans le sillage économique d'un autre, de tirer indûment profit de ses investissements financiers, intellectuels ou humains, de ses efforts, de son travail à valeur économique, sans bourse délier. Ce comportement est lui aussi sanctionné sur le fondement des articles 1382 et 1383 du Code civil relatifs à la responsabilité civile[8], indépendamment de toute situation de concurrence entre les acteurs en cause.

La faute sera caractérisée par l'usurpation de la notoriété ou des efforts d'autrui, soit par le biais d'un comportement destructeur de son avantage concurrentiel (désorganisation de l'entreprise, dénigrement…), soit par un comportement assimilateur de ce même avantage (utilisation de la réputation d'un concurrent, ou de ses efforts intellectuels ou investissements).

- Dans une décision de la Cour d'appel de Paris en date du 20 octobre 1988[9], la **fabrication et** la **commercialisation de dispositifs de contournement ont ainsi été réprimées par le biais** de la **concurrence parasitaire**, car profitant indûment des « *investissements intellectuels* », matériels et économiques d'autrui (« *utilisation sans droit du travail intellectuel d'autrui* »).

La théorie des agissements parasitaires permet de ce fait de condamner toute personne physique ou morale pour avoir imité ou usurpé la réputation ou la notoriété d'autrui, ses efforts intellectuels ou ses investissements (« *se placer indûment, sans bourse délier, dans le sillage d'autrui* »), même s'il n'existe pas de risque de confusion.

Ainsi en irait-il de la **commercialisation de programmes permettant d'effectuer des copies**.

[8] Il est cependant intéressant de noter que la faute (et par là même le lien de causalité) n'est pas toujours recherchée, le fait de se placer dans le sillage d'autrui pouvant parfois suffire pour caractériser le parasitisme. V. en ce sens Trib. com. Paris, 10 août 1978, RIPIA 1979, p. 248.

[9] CA Paris, 20 oct. 1988, JCP G 1989 n° 10, II, 21188, note X. Linant de Bellefonds ; JCP E, 1990, n° 16-17, II, 15751, p.265, note M. Vivant et A. Lucas.

1.2. **La protection par le droit pénal**

Le droit pénal français permet également de protéger les mesures techniques de protection contre leur contournement, à plusieurs niveaux : par le biais des dispositions relatives à la fraude informatique (1.2.1), par le biais de celles relatives à la protection juridique des logiciels (1.2.2), et enfin par le biais de la protection juridique des services à accès conditionnel (1.2.3).

1.2.1. ***Les dispositions relatives à la fraude informatique***

1. La loi n° 88-19 du 5 janvier 1988 dite loi « *Godfrain* », introduite dans le Code pénal aux articles 323-1 à 323-7, institue un certain nombre d'incriminations en matière de fraude informatique.

- Le fait de **s'introduire illégalement dans un système**, et de **s'y maintenir**, est puni par l'**article 323-1 du Code pénal** d'un an d'emprisonnement et de 15 000 euros d'amende.

Est donc réprimé l'accès frauduleux rendu possible par le fait « *de décrypter du contenu crypté sans autorisation : **ainsi en irait-il du contournement d'une mesure technique protégeant un CD ou un DVD contre la copie*** »[10].

D'autre part, « *le fait d'outrepasser le nombre d'utilisateurs ou le temps d'accès autorisés, ou d'outrepasser le nombre de copies autorisées ou une mesure technique empêchant la réalisation de copies* [est réprimé par l'article 323-1] *: **ces derniers actes sont considérés comme équivalant à un maintien frauduleux dans un système de traitement automatisé de données ("STAD")*** »[11].

Est également réprimé le fait d'accéder sans autorisation à un système informatique techniquement sécurisé ou à du contenu protégé, rendu possible par l'utilisation d'un faux nom ou d'un mot de passe usurpé, de fausses données financières, d'une fausse adresse IP…

- Le 22 mai 1998, le Tribunal de grande instance de Paris a déclaré coupable d'accès frauduleux à un « *STAD* » le prévenu qui avait procuré aux utilisateurs des instructions nécessaires à l'accès frauduleux à un fond encyclopédique contenu sur un CDRom[12]. L'éditeur du CDRom avait en effet protégé son produit avec un « *dongle* », sorte de clef électronique qui interdit la consultation à toute personne non autorisée par une licence.

- Un jugement du Tribunal de grande instance de Paris du 26 juin 1995[13] a déclaré le prévenu coupable du délit d'accès frauduleux à un « *STAD* », en ayant introduit des **données (numéro de carte et code confidentiel) usurpées** à une tierce personne et en utilisant l'identité de celle-ci.

---

[10] Gilles Vercken, « *Les protections techniques vues dans un contexte plus large* », Actes du Congrès de l'ALAI, New York 13-17 juin 2001. En effet, la jurisprudence a pu assimiler des CDs à des systèmes, v. *infra* §. 3.1, point 2.
[11] Gilles Vercken, *op. cit.*
[12] TGI Paris, 22 mai 1998, Expertises, juillet 1998, p. 211.
[13] TGI Paris, 26 juin 1995, Petites Affiches, 1er mars 1996, n° 27 p. 4, obs. Valérie Alvarez.

➢ Une décision du Tribunal de grande instance de Paris du 14 juin 1994[14] a pu réprimer un délit d'accès ou de maintien frauduleux dans un « *STAD* » qui s'était effectué à l'aide d'un **mot de passe usurpé**.

Les prévenus avaient en effet « *agi en ayant conscience qu'ils faisaient* ***usage, sans droit, d'un mot de passe usurpé*** *à un abonné bien individualisé », et « se sont pourtant introduits ou maintenus dans des* "STAD". » Du fait de l'usurpation des prérogatives attribuées à un tiers, la conscience d'agir était révélée, permettant d'établir le caractère **frauduleux** de l'accès et du maintien.

Une telle situation peut se rencontrer dans le cas d'une mesure technique protégeant un service ou une œuvre en ligne.

Les actes interdits par l'article 321-1 du Code pénal sont donc définis largement : comme l'a bien souvent confirmé la jurisprudence, c'est le simple fait d'accéder frauduleusement à un système qui est réprimé, peu importe le moyen que le contrevenant a employé.

De même, la **conscience** de l'absence de droit à accéder ou à se maintenir dans un système permet de retenir l'infraction.

➢ Dans l'espèce jugée par le Tribunal de grande instance de Paris le 14 juin 1994[15], sanctionnant un délit d'accès ou de maintien frauduleux dans un « *STAD* » qui s'était effectué à l'aide d'un mot de passe usurpé, les prévenus avaient eu **conscience** d'agir sans droit afin de s'introduire dans les systèmes. Ils s'étaient servi des mots de passe à l'insu, et donc sans l'autorisation, du titulaire pour s'introduire dans les « *STAD* ». La **conscience d'agir** était donc établie, permettant de caractériser l'élément moral du délit de l'article 323-1 du Code pénal.

- L'article 323-2 du Code pénal punit de trois ans d'emprisonnement et de 45 000 euros d'amende le fait d'entraver ou de fausser le fonctionnement d'un « STAD ».

➢ Par un arrêt du 15 mars 1994 de la Cour d'appel de Paris[16], le prévenu a été condamné pour entrave au fonctionnement d'un « STAD », pour avoir introduit une « bombe logique » dans le système, entraînant la paralysie de celui-ci.

Sans penser nécessairement à une « bombe logique » paralysant un système, le contournement d'une mesure technique de protection peut entraver le bon fonctionnement d'un « STAD ». En effet, une telle neutralisation rendrait possibles des actes non autorisés au départ et empêchés par la mesure technique, ce qui perturberait incontestablement le système.

- L'article 323-3 du Code pénal réprime l'altération de fichiers, soit l'introduction ou la suppression ou la modification frauduleuse de données dans un « STAD », par trois ans d'emprisonnement et 45 000 euros d'amende.

Les travaux préparatoires de la loi « *Godfrain* »[17] révèlent que la **modification frauduleuse de données** « *peut être réalisée soit directement, soit indirectement, au moyen d'une* ***action sur*** *les modes de traitement de ces données – c'est-à-dire* ***les logiciels*** *– ou encore au moyen d'une* ***action sur les moyens de transmission de ces données*** *– c'est-à-dire les lignes de*

[14] TGI Paris, 14 juin 1994, Expertises, novembre 1994, p. 395, note J.P. Sala-Martin.
[15] TGI Paris, 14 juin 1994, *op. cit.*.
[16] CA Paris, 9e ch., 15 mars 1994, Juris-Data n° 20887 ; JCP (E) 1995, I, n° 461, n° 21, obs. Vivant et Le Stanc.
[17] Rapport de M. Jacques Thyraud devant le Sénat, n° 214 1ère SE 1987-1988.

communication reliant entre eux les différents éléments du système et qui font partie de ce système ».

Une œuvre sous format numérique peut contenir des signaux ou des données cryptées. Seule l'œuvre originale sera ainsi reconnue par l'appareil de lecture, intégrant un programme décryptant ces données, quand bien même l'utilisateur aurait réussi à effectuer une copie numérique. **L'œuvre se trouve ainsi protégée par un tel processus de cryptage ou de brouillage. La neutralisation de ce système, entraînant nécessairement modification des données cryptées, pourrait donc être sanctionnée par l'article 323-3 du Code pénal pour modification frauduleuse de données.**

> ➢ Le délit d'introduction frauduleuse de données de l'article 323-3 du Code pénal a été reconnu s'agissant de l'**introduction d'un virus dans un logiciel**, par un arrêt du 12 décembre 1996 de la chambre criminelle de la Cour de cassation[18].
>
> ➢ Un arrêt de la Cour d'appel de Paris du 5 octobre 1994[19] a condamné le prévenu pour introduction frauduleuse de données dans un « *STAD* » car il avait **modifié le programme des clefs d'accès au système**.
>
> ➢ Par un jugement du Tribunal de grande instance de Paris du 16 décembre 1997[20], les juges ont reconnu les délits d'accès frauduleux dans un « *STAD* » et d'introduction frauduleuse de données, du fait de la **mise en œuvre d'un programme « *sniffer* » à l'intérieur d'un serveur.** Un tel programme a pour fonction de capturer des données, et suppose donc au préalable un accès frauduleux.

- Il est à noter que l'entente ou la participation à un groupement en vue de commettre ces délits est punie des mêmes peines par l'article 323-4 du Code pénal.

- De même, la seule tentative de ces délits est punie des mêmes peines que les délits eux-mêmes par l'article 323-7 du Code pénal.

> ➢ Dans un jugement du Tribunal de grande instance de Limoges du 14 mars 1994[21], des individus ont été condamnés pour accès ou maintien frauduleux dans un « *STAD* », **tentative d'accès frauduleux**, introduction de données dans un système informatique ou suppression ou modification de données, pour avoir piraté les systèmes informatiques de diverses entreprises.

2. D'autre part, le droit pénal général permet de sanctionner des actes de fabrication et de distribution de dispositifs de contournement par le biais de la **complicité (article 121-7 du Code pénal)**. Les instructions données et la fourniture de moyens (services ou matériels) en relation avec la commission d'une infraction sont donc réprimées à ce titre.

> ➢ Le 9 novembre 1999, la chambre criminelle de la Cour de cassation[22] a approuvé une décision de la Cour d'appel de Paris qui avait condamné pour **complicité** de contrefaçon

---

[18] Cass. crim., 12 déc. 1996, Bull. crim., n° 465 ; Expertises mars 1997, p. 114, obs. Beaujard ; JCP (E), 1998, I, 849, obs. Vivant et Le Stanc.
[19] CA Paris, 5 oct. 1994, Juris-Data n° 023667 ; JCP E, 1995, I, 461, obs. Vivant et Le Stanc.
[20] TGI Paris, 16 déc. 1997, Gaz. Pal. du 29 au 30 juillet 1998, p. 34, note Cyril Rojinsky.
[21] TGI Limoges, 14 mars 1994, Expertises, juin 1994, p. 238, note Corinne Teboul.
[22] Cass. crim., 9 nov. 1999, pourvoi n° 98-87.275, arrêt n° 6980, *Légifrance*.

le **fournisseur de logiciels de « *craquage* »** dans la mesure où il « *savait parfaitement que les copieurs servaient largement à autre chose que sauvegarder des jeux* ». Il ne pouvait donc « *valablement arguer de sa bonne foi dans la mesure où il savait, ayant parfaitement compris le mécanisme de "craquage" du code et l'absence de protection en résultant sur les copies, que les appareils par lui vendus permettaient de contourner le dispositif de sécurité* […] *et d'en copier le programme de jeu sur une disquette* […] *; que la notion de complicité par fourniture de moyens* […] *est établie* ».

Une telle jurisprudence pourrait parfaitement s'appliquer dans le cas de contournement de mesures techniques de protection de CD ou de DVD réprimé par le biais de la fraude informatique.

3. Enfin, il est intéressant de préciser que, à l'image des infractions instituées par le Code pénal en ce qui concerne la fraude informatique et la complicité, l'article 6 de la Directive requiert un élément moral (« *que la personne effectue en sachant, ou en ayant des raisons valables de penser* ») ainsi qu'un élément matériel (le contournement, la fourniture de moyens). L'**élément moral** est le plus souvent constitué par la connaissance de la fonction de contournement du dispositif technique.

- L'arrêt de la Cour d'appel de Paris du 14 janvier 1997[23] précise que, « *pour être punissable, un accès ou un maintien doit être fait sans droit et* ***en pleine connaissance de cause*** […]. »

Dès lors, les délits de maintien frauduleux dans un « *STAD* » et d'entrave au fonctionnement d'un « *STAD* » ont pu être caractérisés au préjudice de services télématiques.

- De même, « *la notion de complicité par fourniture de moyens* […] *suppose que celui qui fournit le moyen sait, lors de la livraison de celui-ci, que l'utilisateur en fera un usage frauduleux* »[24].

Une fois encore, les incriminations relatives à la fraude informatique peuvent être appliquées au contournement de mesures techniques de protection.

4. Il apparaît donc que la législation française relative à la criminalité informatique est dès à présent apte à protéger les mesures techniques de protection.

Ainsi, « ***l'accès à un service ou un objet verrouillé techniquement est déjà protégé par le droit pénal de l'informatique*** », constate Gilles Vercken[25].

De même, Antoine Latreille[26] considère que la législation pénale sur la fraude informatique a vocation à protéger les mesures techniques de protection : « *Sans constituer précisément un instrument réservé à la sanction des contournements des dispositifs techniques de protection des propriétés intellectuelles, il est évident que la plupart* [des comportements incriminés par la Directive] *sont ou seront réprimés par* [la loi « *Godfrain* »] *dans la mesure où la notion de* "système de traitement automatisé" *s'applique à tous les*

---

[23] CA Paris, 11e ch., 14 janv. 1997, Juris-Data n° 020128.
[24] Cass. crim., 9 nov. 1999, pourvoi n° 98-87.275, arrêt n° 6980, Légifrance.
[25] Gilles Vercken, « *Mesures techniques et copie privée : round 1 ?* », Légipresse n° 198, janvier-février 2003, p. 17.
[26] Antoine Latreille, « *L'étendue de l'interdiction de contournement des dispositifs techniques de protection des droits – Exceptions* », Actes du Congrès de l'ALAI, New York 13-17 juin 2001.

réseaux télématiques et notamment à Internet. Or c'est précisément via Internet que seront communiquées à l'avenir la plupart des œuvres de l'esprit et donc là que seront présents la plupart des dispositifs techniques de protection. » « ***La plupart des contournements des dispositifs techniques de protection des propriétés intellectuelles sont ou seront réprimés par ladite loi*** [loi « *Godfrain* »] *dans la mesure où la notion de système de traitement automatisé est largement définie.* »[27]

1.2.2. *La protection juridique des mesures techniques par le droit des logiciels*

La législation relative à la protection des logiciels – insérée dans le Code de la propriété intellectuelle – pourrait s'appliquer dès lors que la mesure technique de protection met en œuvre un logiciel.

« *Lorsque la désactivation d'un contrôle d'accès* […] *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.* »[28]

Bien entendu, la mise en cause du droit de l'auteur sur le logiciel - constituant la mesure technique de protection contournée - suppose que la décompilation ne soit pas effectuée dans les termes prévus à l'article L. 122-6-1 du Code de la propriété intellectuelle, c'est-à-dire « *lorsque la reproduction du code du logiciel ou la traduction de la forme de ce code est indispensable pour obtenir les informations nécessaires à l'interopérabilité d'un logiciel créé de façon indépendante avec d'autres logiciels, sous réserve que soient réunies les conditions suivantes :*

1° Ces actes sont accomplis par la personne ayant le droit d'utiliser un exemplaire du logiciel ou pour son compte par une personne habilitée à cette fin ;

2° Les informations nécessaires à l'interopérabilité n'ont pas déjà été rendues facilement et rapidement accessibles aux personnes mentionnées au 1° ci-dessus ;

3° Et ces actes sont limités aux parties du logiciel d'origine nécessaires à cette interopérabilité. »

---

[27] Antoine Latreille, « *La protection des dispositifs techniques (I) – Entre suspicion et sacralisation* », Propriétés intellectuelles, janvier 2002, n° 2, p. 35.

[28] Séverine Dusollier, « *Régimes complémentaires et concurrentiels au droit d'auteur – Les protections techniques vues dans un contexte juridique plus large* », Rapport général, Actes du Congrès de l'ALAI, New York 13-17 juin 2001, p. 180.

1.2.3. *La protection juridique des mesures techniques par le droit des services à accès conditionnel*

1. Le contournement de dispositifs contrôlant l'accès à des œuvres pourra être sanctionné par le biais de la législation sur les **services à accès conditionnel**.

2. L'article 2 alinéa 1er de la **loi n° 86-1067 du 30 septembre 1986** relative à la liberté de communication, modifiée par la **loi n° 92-1336 du 16 décembre 1992**, définit la notion de « *télécommunication* » comme « *toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature, par fil, optique, radio-électricité ou autres systèmes électromagnétiques* ».

L'article 2 alinéa 2 de la loi de 1986 définit la notion de « *communication audiovisuelle* » comme « *toute mise à disposition du public, par un procédé de télécommunication, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée* ».

Or Internet est un « *réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destinés à l'échange* […] *d'informations multimédias et de fichiers.* […] »[29]. Il apparaît donc qu'une mise à disposition d'œuvres sur Internet pourrait être concernée par cette législation.

En effet, les sites Web sont à ce jour fréquemment assimilés à des services de communication audiovisuelle[30].

3. Or la loi de 1986 permet d'**interdire les équipements de décryptage ou de neutralisation**. Les activités prohibées sont énoncées en ses articles 79-1 à 79-4 : il s'agit de la fabrication, l'importation en vue de la vente ou de la location, la vente ou l'installation d'un équipement, matériel, dispositif ou instrument conçu, en tout ou en partie, pour capter frauduleusement des programmes télédiffusés ; le fait de commander, de concevoir, d'organiser ou de diffuser une publicité faisant, directement ou indirectement la promotion de l'un de ces équipements ; l'acquisition ou la détention, en vue de son utilisation, de l'un de ces équipements. Il s'agit donc d'**actes préparatoires**, envisagés de façon large.

4. De même, la **loi n° 2000-719 du 1er août 2000** relative à la liberté de communication, modifiant la loi du 30 septembre 1986, prévoit le régime applicable aux exploitants de systèmes d'accès sous condition : « *Au sens du présent article, les mots :* "système d'accès sous condition" *désignent tout dispositif technique permettant, quel que soit le mode de transmission utilisé, de restreindre l'accès à tout ou partie d'un ou plusieurs services de télévision ou de radiodiffusion sonore transmis par voie de signaux numériques au seul public autorisé à les recevoir, et les mots :* "exploitants de systèmes d'accès sous condition" *désignent toute personne, physique ou morale, exploitant ou fournissant un système d'accès sous condition* » (article 95 I de la loi de 1986 modifiée).

---

[29] M. Vivant *et alii*, Lamy « *Droit de l'Informatique et des Réseaux* », éd. 2003, n° 3531.
[30] Antoine Latreille, « *L'étendue de l'interdiction de contournement des dispositifs techniques de protection des droits – exceptions* », Actes du Congrès de l'ALAI, New York 13-17 juin 2001.

5. Dès lors, la loi de 1986 sur la liberté de communication, modifiée en 1992 et 2000, pourrait aussi contribuer à sanctionner efficacement le contournement de mesures techniques de protection des services de télédiffusion et de radiodiffusion en ligne.

D'une manière générale, et pour conclure sur la protection des mesures techniques par le droit pénal, il est possible de considérer que la législation pénale française permet déjà de sanctionner les actes de contournement des mesures techniques de protection. M. Vercken estime d'ailleurs que « ***la réglementation du droit pénal de l'informatique est particulièrement efficace pour assurer la protection des mesures techniques*** »[31]**.**

Ainsi, à titre d'exemple, le décryptage non autorisé d'une œuvre cryptée disponible en ligne peut être réprimé « *pour interception de données de télécommunications et de données cryptées, accès non autorisé, fraude informatique, altération de données, et décryptage non autorisé de signaux de télédiffusion si la transmission s'effectue par ce mode* »[32]. De même, la commercialisation de clefs de décryptage peut être sanctionnée sur le fondement de la concurrence déloyale.

Mais à ce jour, il est vrai que tous les actes visés à l'article 6 de la Directive ne sont pas expressément visés par les textes internes.

En effet, les articles 323-1 à 323-7 du Code pénal ne pénalisent que le fait d'**accéder** ou de se **maintenir**, **frauduleusement**, dans tout ou partie d'un « *STAD* », d'**altérer**, d'**entraver** ou de **fausser** son fonctionnement, d'y **introduire**, **supprimer** ou **modifier frauduleusement des données**, la tentative de ces délits, la participation à un groupement formé ou à une entente établie en vue de la préparation de ces infractions. Ces articles sont, concernant ces infractions, conformes à l'article 6.1 de la Directive qui évoque le « ***contournement*** *de toute mesure technique efficace, que la personne effectue* ***en sachant, ou en ayant des raisons valables de penser****, qu'elle poursuit cet objectif* ».

En revanche, l'article 6.2 de la Directive ne trouve pour l'instant pas d'écho dans la législation française actuelle, notamment en ce qui concerne **la promotion et la distribution de moyens de contournement**, ce qui ne sera plus le cas avec la rédaction future des dispositions relatives à la fraude informatique[33].

Dès lors, le droit pénal français ainsi que certains mécanismes du droit civil étant d'ores et déjà aptes à protéger les mesures techniques, cette protection n'a pas lieu de figurer au sein du Code de la propriété intellectuelle.

---

[31] Gilles Vercken, « *Les protections techniques vues dans un contexte plus large* », Actes du Congrès de l'ALAI, New York 13-17 juin 2001.

[32] Séverine Dusollier, « *Régimes complémentaires et concurrentiels au droit d'auteur – Les protections techniques vues dans un contexte juridique plus large* », Rapport général, Actes du Congrès de l'ALAI, New York 13-17 juin 2001, p. 181.

[33] V. *infra* §. 3.2.

2. LA PROTECTION JURIDIQUE DES MESURES TECHNIQUES NE DEVRAIT PAS FIGURER AU SEIN DU CODE DE LA PROPRIETE INTELLECTUELLE

Lors de la transposition de la protection juridique des mesures techniques en droit français, le législateur sera vraisemblablement amené à choisir d'introduire ces dispositions dans une législation particulière. Cependant, leur insertion ne doit pas intervenir dans le Code de la propriété intellectuelle (CPI), et ceci pour trois raisons particulières. Tout d'abord, ni la Directive du 22 mai 2001, ni les Traités de l'OMPI de 1996, n'assimilent le contournement de mesures techniques de protection à de la contrefaçon (2.1). Ensuite, la protection des mesures techniques est d'une logique absolument distincte de la protection accordée par le CPI aux auteurs et aux titulaires de droits voisins (2.2). Enfin, l'insertion de cette protection au sein du CPI serait inopportune (2.3).

2.1. Ni la Directive du 22 mai 2001, ni les Traités de l'OMPI de 1996, n'assimilent le contournement de mesures techniques de protection à de la contrefaçon, et n'imposent en aucune manière de procéder à une telle assimilation

1. Le Traité de l'OMPI sur le droit d'auteur du 20 décembre 1996, en son article 11, ainsi que le Traité de l'OMPI sur les droits voisins de la même date, en son article 18, n'imposent qu'« *une protection juridique appropriée et des sanctions juridiques efficaces contre la neutralisation des mesures techniques* » de protection, sans autre précision. Cette formulation appelle une protection « *classique* » à défaut de référence à un quelconque élément relevant du droit d'auteur. Ce sont les droits que les mesures techniques doivent protéger qui relèvent du droit d'auteur ; les mesures techniques elles-mêmes ne sont pas appréhendées comme faisant partie du monopole de l'auteur. Ce n'est pas une *maîtrise de l'œuvre* qui est en cause. Dès lors, il n'apparaît pas judicieux d'assimiler de tels actes de contournement à de la contrefaçon, à plus forte raison en l'absence d'une telle obligation imposée par les Traités eux-mêmes.

2. De même, la Directive du 22 mai 2001 ne procède pas à une telle assimilation du contournement d'une mesure technique de protection à de la contrefaçon. Au contraire, les termes dans lesquels la répression de cet acte est présentée (article 6.1[34]) rappellent davantage la répression de la fraude informatique : exigence d'un élément moral, actes interdits, etc. Dès lors, le contournement d'une mesure technique de protection ne s'apparente pas à de la contrefaçon, mais bien plutôt à de la fraude informatique telle que réprimée aux articles 323-1 à 323-7 du Code pénal.

[34] Article 6 : « *Obligations relatives aux mesures techniques : 1. Les Etats membres prévoient une protection juridique appropriée contre le contournement de toute mesure technique efficace, que la personne effectue en sachant, ou en ayant des raisons valables de penser, qu'elle poursuit cet objectif.* »

3. La plupart des pays de l'Union européenne, qui ont déjà transposé ou ont prévu un projet de loi de transposition de la Directive, ont d'ailleurs choisi d'adopter des mesures qui n'assimilent pas le contournement des dispositifs techniques de protection à de la contrefaçon.

L'**Allemagne** prévoit de transposer l'article 6 de la Directive dans la section 95a de sa loi sur la propriété intellectuelle[35]. Le contournement de mesures techniques de protection est réprimé par les dispositions de droit pénal prévues à la section 108b de la loi allemande, sans assimilation à de la contrefaçon. Le contrevenant encourre jusqu'à un an de prison si l'infraction n'a pas été commise pour son usage exclusivement privé. Si le contournement a été effectué pour son usage privé, le titulaire des droits peut simplement le poursuivre afin d'engager sa responsabilité civile. En ce qui concerne les actes parallèles de fourniture de moyens de contournement de mesures techniques, les peines peuvent aller jusqu'à trois ans d'emprisonnement si l'infraction a été commise dans un but commercial. Il n'y a donc en aucun cas assimilation à de la contrefaçon, et la répression de ces actes se fait par le biais du droit pénal et du droit de la responsabilité civile.

L'**Autriche** a intégré la protection des mesures techniques dans sa « *loi sur l'omission et l'élimination de l'état conflictuel* », et non dans une loi sur la propriété intellectuelle, sans assimilation à de la contrefaçon[36].

En ce qui concerne la **Belgique**[37], un projet de nouvel article 79 bis, § 1er de la loi belge du 28 novembre 2000 sur la **criminalité informatique** prévoirait une sanction pénale du contournement illicite de toute mesure technique efficace en vue d'empêcher ou de limiter des actes non autorisés par les ayants droits. Un tel élément n'est donc pas assimilé à de la contrefaçon.

Au **Danemark**, l'article 6 de la Directive a été transposé par l'article 75 de la loi du 17 décembre 2002 modifiant la législation danoise sur la propriété intellectuelle[38]. Cet article interdit le contournement des mesures techniques de protection efficaces, à moins qu'il ne soit autorisé par le titulaire des droits. La loi de transposition précise que tout contournement sera sanctionné par les règles générales de la responsabilité (article 75c et 75e), et non par le régime spécial de responsabilité en cas d'atteinte à un droit d'auteur (article 78 de la loi).

La **Grèce**, quant à elle, dans l'article 66A de sa loi de transposition de la Directive[39], ne fait que prévoir des sanctions pénales au contournement de mesures techniques de protection, sans procéder à une quelconque assimilation à de la contrefaçon.

Le 28 mars 2003, le Conseil des ministres italien a approuvé la loi de transposition de la Directive[40], qui vient modifier la loi italienne sur le droit d'auteur. Ainsi, l'**Italie** sanctionne le contournement de mesures techniques de protection, en ses articles 26, 27 et 28[41] de la loi de transposition, par le biais du droit pénal (article 173-bis de la loi n° 663 du 22 avril 1941). De tels contournements ne sont pas assimilés à de la contrefaçon, bien que ces mesures soient introduites dans sa législation relative à la propriété intellectuelle. De tels actes de contournement sont passibles d'une peine d'emprisonnement de six mois à trois ans, d'une peine d'amende pouvant aller de 2 500 à 15 000 euros et d'une suspension de certains droits.

---

[35] http://dip.bundestag.de/btd/15/000/1500038.pdf
[36] http://www.justiz.gv.at/gesetzes/download/urheberrecht2002.pdf
[37] http://www.ael.be/docs/eucd/704-4.pdf
[38] http://www.fipr.org/copyright/guide/denmark.rtf
[39] http://www.culture.gr/8/84/e8401.html
[40] http://softwarelibero.org/progetti/eucd/bozza-legge-italiana.shtml
[41] http://www.fipr.org/copyright/guide/italy.rtf

Enfin, le **Portugal** prévoit dans son projet de loi de transposition de la Directive[42] que le contournement de mesures techniques de protection « *est puni d'une peine d'arrestation pouvant aller jusqu'à trois ans ou d'une peine d'amende* ». Il n'est, encore une fois, procédé à aucune assimilation à de la contrefaçon.

Il est donc intéressant de relever qu'actuellement, aucune législation d'un pays européen n'envisage de qualifier de contrefaçon le contournement d'une mesure technique de protection, pas plus que ne l'imposaient les Traités de l'OMPI ni la Directive du 22 mai 2001. **Une telle assimilation, lors de la transposition, à de la contrefaçon aurait alors pour résultat de s'éloigner de l'objectif premier de la Directive, c'est-à-dire l'objectif d'harmonisation.** Il est en effet nécessaire de prendre en compte le choix des autres Etats membres lors de la transposition de l'article 6 de la Directive dans le droit français.

2.2. La protection des mesures techniques est d'une logique distincte de la protection accordée par le CPI aux auteurs et aux titulaires de droits voisins

1. « *Il est loin d'être évident que les mesures techniques doivent être protégées par le droit d'auteur* » estime le professeur Christophe Caron[43], ajoutant qu'« *il est peut-être artificiel d'inclure la protection des mesures techniques dans le monopole de l'auteur : ce qui permet de rendre efficace le monopole ne relève pas forcément du monopole lui-même* ».

En effet, ce sont les mesures techniques de protection qu'il s'agit de protéger par le biais d'un mécanisme juridique. Ce dernier n'a donc pas pour but de protéger les œuvres elles-mêmes, mais au contraire de réprimer des actes qui portent atteinte aux mesures techniques de protection, actes qui permettent l'accès frauduleux aux œuvres par la neutralisation des mesures techniques. La protection de ces mesures ne relève donc pas de la protection de l'œuvre par le droit d'auteur, ni par-là même du monopole de l'auteur. Une telle neutralisation procède d'une toute autre démarche. Ce comportement relève bien plutôt de la notion de **fraude**, d'**accès indu**, ce qui permet donc de rattacher son régime juridique de préférence à la fraude informatique intégrée au Code pénal.

2. L'on pourrait parler de contrefaçon des mesures techniques de protection uniquement dans le cas d'une reproduction et d'une exploitation de celles-ci. Or, pour les cas visés dans cette étude, **la neutralisation de ces mesures n'a aucunement pour but de les exploiter, mais d'accéder à l'œuvre protégée. L'assimilation du contournement des mesures techniques de protection à de la contrefaçon est donc impropre. Le droit d'auteur, la notion de contrefaçon ainsi que les prescriptions de la Directive risquent de se trouver dénaturés par une telle assimilation.**

3. L'insertion de cette protection au sein du Code de la propriété intellectuelle serait par ailleurs inopportune au regard de ses effets et de sa signification.

---

[42] http://www.ansol.org/politica/eucd-texto.pt.html

[43] Christophe Caron, « *Brèves observations sur la protection des mesures techniques par le droit civil* », Actes du Congrès de l'ALAI, New York 13-17 juin 2001.

2.3. **L'insertion de cette protection au sein du CPI est inopportune**

1. Il semblerait que le gouvernement français ait pour l'heure fait le choix d'une assimilation des actes de neutralisation de mesures techniques, de fabrication, vente, etc., de matériels permettant de tels actes de contournement, à un délit de contrefaçon.

Le **délit de contrefaçon** est défini par l'article L. 122-4 du Code de la propriété intellectuelle, qui précise que : « *toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite* ». Il s'agit donc du fait pour un autre que le titulaire de droits de propriété intellectuelle d'exploiter les prérogatives patrimoniales ou morales de celui-ci, portant ainsi atteinte à ses droits (article L. 335-2 du Code de la propriété intellectuelle).

Or le contournement de mesures techniques de protection, couramment qualifié de « ***piratage*** », relève naturellement de la fraude informatique – au sens générique du terme. Le piratage est en effet entendu comme une **atteinte abusive à la technique**, et non comme une atteinte aux droits patrimoniaux (ou moraux) de l'auteur. Il s'agit du « *craquage* », du cassage d'une protection, et non de la reproduction ou de la représentation de l'œuvre en cause. Une insertion éventuelle dans le Code de la propriété intellectuelle est donc impropre notamment pour cette raison.

En effet, si l'on admet, comme cela est souvent soutenu[44], que l'acte de contrefaçon est un acte d'empiètement, d'emprise indue sur la propriété d'autrui, l'atteinte aux mesures techniques ne serait au mieux qu'un bris de clôture.

Par ailleurs, selon Michel Vivant et les auteurs du Lamy « *Droit de l'informatique et des réseaux* »[45], le piratage est le fait de « *s'introduire dans un système, s'y promener, prendre connaissance de l'information qu'il recèle : tout cela renvoie au phénomène d'intrusion* ».

Enfin, une grande partie des hypothèses de fraude informatique est déjà appréhendée par le Code pénal. Or, comme l'a affirmé M. Latreille, s'agissant de la transposition de la Directive, « *si la possibilité de légiférer hors de la propriété intellectuelle dans un texte général n'est pas suivie, la propriété littéraire et artistique y perdra sûrement en clarté, d'autant plus qu'en France d'autres dispositifs juridiques permettent déjà de sanctionner les contournements* »[46].

Dès lors, dans un souci de cohérence du système juridique français, il conviendrait d'insérer la répression de la neutralisation des mesures techniques de protection dans le Code pénal à la suite des dispositions relatives à la fraude informatique.

2. L'**assimilation du contournement des mesures techniques de protection à de la contrefaçon** présente par ailleurs un **effet pervers** de taille. En effet, **la mauvaise foi est**

---

[44] Michel Vivant, « *Les créations immatérielles et le droit* », Le droit en questions, Ellipses, éd. 1997, p. 26.
[45] M. Vivant *et alii*, Lamy « *Droit de l'informatique et des réseaux* », éd. 2003, n° 3487.
[46] Antoine Latreille, « *La protection des dispositifs techniques – Entre suspicion et sacralisation* », Propriétés Intellectuelles, janvier 2002, n° 2, p. 35.

présumée en matière de contrefaçon[47] : « *la contrefaçon est caractérisée, indépendamment de toute faute ou mauvaise foi, par la reproduction, la représentation ou l'exploitation d'une œuvre de l'esprit, en violation des droits de propriété intellectuelle qui y sont attachés* »[48]. Or, selon les termes de l'article 6.1 de la Directive, un contournement de mesure technique, pour être réprimé, suppose que la personne « *effectue* [le contournement] *en sachant, ou en ayant des raisons valables de penser qu'elle poursuit cet objectif* ». Il s'agit donc de **caractériser un élément intentionnel**. Même si le ministère de la Culture et de la Communication estime que « *seules les personnes qui ont agi en connaissance de cause pour contourner un système de protection seront coupables de contrefaçon* »[49], assimiler un tel contournement à de la contrefaçon sera contraire à la jurisprudence précitée en matière de présomption de mauvaise foi. Cette assimilation pourra en outre faire disparaître à terme l'élément intentionnel, et sera donc contraire à la Directive.

A titre d'exemple, les travaux des **chercheurs en cryptologie** nécessitent de tels actes de contournement de mesures techniques, afin de faire avancer la recherche dans ce domaine. Ces chercheurs tomberaient dès lors *de facto* sous le coup de la loi réprimant le contournement des mesures techniques par la contrefaçon, sans que leur bonne foi n'ait un quelconque rôle à jouer dans la qualification de l'infraction.

Assimiler le contournement de ces mesures techniques à de la contrefaçon **limite par conséquent les moyens de preuve**, dispensant le titulaire des droits d'apporter la preuve de la mauvaise foi du contrevenant. Une telle assimilation est dès lors contraire aux objectifs de la Directive, qui requiert une réelle intentionnalité.

3. Enfin, au vu des débats à l'Assemblée Nationale au sujet de la loi dite « *Godfrain* »[50], il apparaît clairement que celle-ci envisage la question de la fraude informatique dans son ensemble : « *elle réalise dans le Code pénal une ouverture sur l'avenir par la création d'un chapitre spécifique sur la répression des fraudes liées directement à la chose informatique* ». Il apparaît dès lors que le but de cette loi est d'englober l'ensemble des infractions relatives à l'informatique. En toute logique, la répression des actes de neutralisation des mesures techniques de protection doit donc être insérée à la suite de la répression des atteintes aux systèmes de traitement automatisé de données.

4. L'insertion de cette protection au sein du Code de la propriété intellectuelle serait donc inopportune, d'autant plus que la législation française possède un arsenal législatif permettant de répondre pleinement aux objectifs de l'article 6 de la Directive en matière de fraude informatique.

---

[47] Cass. civ. 1ère, 29 mai 2001, D. 2001, n° 1, p. 71, obs. critiques P. Sirinelli ; Cass. civ. 1ère, 15 oct. 1996, D. affaires 1997, p. 80 ; CA Paris, 4e ch. B, 2 fév. 1989, Expertises 1989, p. 69, Cahiers Lamy Droit de l'Informatique, mai 1989 (C), p. 23.

[48] Cass. civ. 1ère, 29 mai 2001, précit.

[49] Monique Ciprut, « *Copie privée : le gouvernement durcit le projet de loi* », Les Echos, 26 mai 2003.

[50] Débats à l'Assemblée Nationale, n° 39 du 16-06-1987 p. 2384-2388, M. Albin Chalandon, ministre de la Justice.

3. LES INCRIMINATIONS ACTUELLES – ET FUTURES – EN MATIERE DE FRAUDE INFORMATIQUE PERMETTENT DE REPONDRE PLEINEMENT AUX OBJECTIFS DE L'ARTICLE 6 DE LA DIRECTIVE

1. M. René André, dans son rapport devant l'Assemblée Nationale concernant la future loi « *Godfrain* »[51], précise que le **champ d'application** de l'incrimination d'« ***accès frauduleux*** » concerne « *non seulement les systèmes eux-mêmes (mémoires vives, mémoires de masse : disquettes, bandes, etc.), les terminaux d'accès à distance, mais aussi les réseaux assurant la communication entre les différents éléments d'un système ou encore entre systèmes* ».

Par conséquent, il apparaît clairement que les CD et DVD sont concernés par ces dispositions, mais également tous types de serveurs et de réseaux, dont le réseau Internet. Ainsi, le contournement d'une mesure technique protégeant un CD ou un DVD contre la copie, ou encore une œuvre sur Internet, peut être sanctionné par les articles 323-1 à 323-7 du Code pénal.

2. Dès lors, il est possible d'affirmer qu'une mesure technique – au sens de l'article 6 de la Directive – permet toujours de protéger un système de traitement automatisé de données (« *STAD* ») (3.1). De plus, l'article 34 du projet de loi pour la confiance dans l'économie numérique (« *LCEN* ») vient étendre les incriminations en matière de fraude informatique (3.2). Les objectifs de l'article 6 de la Directive seront ainsi pleinement satisfaits par la législation française sur la fraude informatique.

3.1. Une mesure technique, au sens de l'article 6 de la Directive, permet toujours de protéger un système de traitement automatisé de données

1. Un « *STAD* » peut être protégé techniquement contre tout accès ou maintien frauduleux. Une décision de la Cour d'appel de Paris du 30 octobre 2002[52] énonce deux critères principaux cumulatifs qui, en cas d'atteinte à un « *STAD* » par le biais d'un logiciel grand public de navigation, rendent possible l'application des dispositions pénales relatives à l'accès frauduleux : la mention du caractère confidentiel de l'ensemble de données concerné, et l'existence d'un obstacle à l'accès.

Une mesure technique de protection remplit un tel rôle de protection d'un « *STAD* ». Selon la Directive du 22 mai 2001, la mesure technique de protection doit en effet être efficace afin de bénéficier de la protection instituée. Son article 6.1 énonce à ce titre qu'une mesure technique est réputée efficace « *lorsque l'utilisation d'une œuvre protégée, ou celle d'un autre objet protégé, est contrôlée par les titulaires du droit grâce à l'application d'un code d'accès ou d'un procédé de protection, tel que le cryptage, le brouillage ou toute autre transformation de l'œuvre ou de l'objet protégé ou d'un mécanisme de contrôle de copie qui atteint cet objectif de protection* ».

---

[51] Rapport de M. René André devant l'Assemblée Nationale, n° 744 1ère SO 1986-1987.
[52] CA Paris, 30 oct. 2002, Expertises, janvier 2003, p. 36 ; note C. Morel p. 27, « *affaire Kitetoa* ».

Illustration technique :

Le « *Content Scramble System* » (CSS), par exemple, est une mesure technique protégeant les DVD. Ce système s'appuie sur le principe du cryptage. Il s'agit d'un algorithme de « *mélangeage* » (cryptage) qui est appliqué aux données d'un DVD. Pour pouvoir lire un DVD, un appareil de lecture (lecteur DVD de salon, logiciel de lecture de DVD sur ordinateur…) doit donc en décrypter (remettre en ordre) les données avant de pouvoir les traiter par des algorithmes qui permettent de visualiser à l'écran le contenu du DVD. Il suffit pour cela de connaître un algorithme de décryptage et de l'implémenter au sein de ces appareils. C'est cet algorithme de décryptage implémenté dans l'appareil qui permettra l'accès à l'œuvre, et c'est un autre logiciel qui permettra l'usage de l'œuvre.

De même, une clef physique à connecter sur un port de l'ordinateur constitue une mesure technique de protection. Une telle clef peut être vendue en même temps qu'un logiciel. Il s'agit d'un élément à brancher sur un port parallèle, série ou USB de l'ordinateur. Cet élément se connecte entre la prise du port de l'ordinateur et le câble qui y est normalement branché. Il contient un circuit logique particulier ou un code informatique. Lors du démarrage du logiciel, celui-ci vérifie si la clef physique est bien connectée à l'ordinateur, afin de s'assurer des droits de l'utilisateur. A défaut de clef, le logiciel refusera de fonctionner.

Ces différents systèmes constituent des mesures techniques de protection. Elles reposent en général sur un principe de lecture et de codification d'informations. Elles permettent de protéger des œuvres contre l'accès non-autorisé ou contre la copie, mais également, donc, l'accès à un « *STAD* ».

Une atteinte à un « *STAD* » suppose dès lors le plus souvent une atteinte préalable à la mesure technique elle-même, qui le protège. Un tel contournement pourrait être réprimé par le biais de la répression de l'accès frauduleux à un « *STAD* ».

- Dans un arrêt de la Cour d'appel de Douai du 7 octobre 1992[53], le délit d'accès frauduleux à un « *STAD* » a été reconnu, en présence d'une copie d'un logiciel de compatibilité réalisée sans autorisation et permettant d'accéder à des informations sur des tiers.

  Cet arrêt fait à la fois application de la législation sur les programmes d'ordinateur pour contrefaçon de logiciel, et application de la législation sur la fraude informatique pour accès frauduleux à un « *STAD* ». Nous sommes en présence d'un concours d'infractions. Ceci conforte l'idée selon laquelle la législation actuelle, composée comme en l'espèce de la législation relative aux logiciels et de celle relative à la fraude informatique, est parfaitement appropriée pour réprimer le contournement d'une mesure technique protégeant une œuvre, effectué par exemple pour copier illicitement de cette dernière.

2. **Ont été qualifiés de « *systèmes* » par la jurisprudence** le réseau France Télécom, le système Carte bancaire[54], Internet, le courrier électronique, les services techniques d'accès

[53] CA Douai, 4e ch., 7 oct. 1992, Gaz. Pal. 1993, 2, p. 326 ; JCP (E) 1994, I, n° 359, n° 15, obs. Vivant et Le Stanc.
[54] TGI Paris, 13e ch., 25 fév. 2000, Dalloz 2000, IR p. 99 ; Expertises, mars 2000, p. 49.

ou d'hébergement qui permettent d'utiliser le réseau[55], un site Internet, une simple carte à microprocesseur[56], un disque contenant un logiciel et des données[57], un CDRom contenant une base de données et son logiciel d'accès[58], des « *STAD* » d'entreprises, des services accessibles par télématique ou Internet.

La notion est donc particulièrement large, et permet sans conteste d'appréhender une œuvre mise à disposition en ligne, ou encore sur un CD ou DVD ou tout support.

3. Il est par ailleurs possible d'assimiler les mesures techniques de protection à des « *STAD* ». Il faut pour cela étudier les différentes définitions données aux « *STAD* » et aux mesures techniques de protection.

Lors des travaux parlementaires sur la future loi « *Godfrain* », le rapporteur au Sénat, M. Thyraud, a déclaré qu'on devait entendre par **système de traitement automatisé de données** « *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties, et de liaisons, qui* ***concourent à un résultat déterminé*** »[59]. Cependant, le législateur n'a pas souhaité introduire cette définition dans la loi, préférant ne pas restreindre cette incrimination à l'existence de « *liaisons* », ce qui aurait pour effet d'exclure « *du champ de la protection pénale les systèmes informatiques autonomes* »[60]. M. Thyraud souhaitait toutefois qu'il soit procédé à une « *acception extensive de la notion de système* »[61].

D'autre part, l'informatique se définit comme la science du traitement automatisé de l'information. **« *Ce sont* [donc] *les systèmes informatiques au sens le plus large du terme qui sont visés* » par cette notion de « *STAD* »[62].**

Enfin, en ce qui concerne les **mesures techniques de protection**, elles sont définies par la Directive en son article 6.3 comme « *toute technologie, dispositif ou composant qui,* ***dans le cadre normal de son fonctionnement****, est* ***destiné à*** *empêcher ou à limiter, en ce qui concerne les œuvres ou autres objets protégés, les actes non autorisés par le titulaire d'un droit d'auteur ou d'un droit voisin du droit d'auteur prévu par la loi, ou du droit sui generis prévu au chapitre III de la directive 96/9/CE* ».

Par conséquent, au vu de ces définitions ainsi que des jurisprudences évoquées précédemment précisant la notion de « *systèmes* » [63], il apparaît qu'il est possible d'assimiler les mesures techniques de protection à des systèmes de traitement automatisé de données.

4. Or la législation actuelle est, certes, déjà apte à répondre aux objectifs de l'article 6.1 de la Directive, mais les dispositions en cours d'adoption se révèlent être un complément nécessaire afin de satisfaire aux objectifs de l'article 6.2.

---

[55] MM. A. Lucas, J. Devèze et J. Frayssinet, « *Droit de l'informatique et de l'Internet* », PUF, éd. 2001, n° 981.
[56] MM. A. Lucas, J. Devèze et J. Frayssinet, *op. cit.*
[57] CA Douai, 4e ch., 7 oct. 1992, Gaz. Pal. 1993, 2, p. 326 ; JCP (E) 1994, I, n° 359, n° 15, obs. Vivant et Le Stanc.
[58] CA Paris, 11 mars 1999, Gaz. Pal., 27-28 oct. 2000, note I. Matthyssens ; Trib. Corr. Paris, 22 mai 1998, Expertises, juillet 1998, p. 211.
[59] Rapport de M. Jacques Thyraud devant le Sénat, n° 3 1ère SO 1987-1988, p. 52.
[60] Rapport de M. René André devant l'Assemblée Nationale, n° 1087 1re SO 1987-1988, p. 5.
[61] Rapport de M. Jacques Thyraud devant le Sénat, n° 214 1re SE 1987-1988, p. 6.
[62] M. Vivant *et alii*, Lamy « *Droit de l'Informatique et des Réseaux* », éd. 2003, n° 3495.
[63] V. *supra*, notes 54 à 58.

3.2. La loi pour la confiance dans l'économie numérique vient étendre les incriminations relatives à la fraude informatique et les rendre conformes aux objectifs fixés par la Directive

1. Les « *STAD* » sont non seulement protégés contre tout accès – ce qui vise d'ores et déjà les actes de contournement directs – mais la loi pour la confiance dans l'économie numérique (ci-après « *LCEN* ») vient étendre les incriminations aux actes intermédiaires de promotion et de mise à disposition de moyens de contournement.

2. Les « *STAD* » sont donc protégés contre tout accès ou maintien frauduleux, contre toute modification ou suppression frauduleuse de données[64]. Mais tous les actes visés par l'article 6 de la Directive ne sont pas prévus par la législation actuelle sur la fraude informatique[65].

Or le projet « *LCEN* », présenté au Conseil des ministres le 15 janvier 2003, contient notamment un article 34 modifiant le Code pénal, et complétant les dispositions introduites par la loi « *Godfrain* » sur la fraude informatique par un nouvel article 323-3-1.

L'article 34 du projet de loi pour la confiance dans l'économie numérique insère donc au sein du Code pénal un article ainsi rédigé :

« Art. 323-3-1. - Le fait de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre les faits prévus par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

« Les dispositions du présent article ne sont pas applicables lorsque la détention, l'offre, la cession et la mise à disposition de l'instrument, du programme informatique ou de toute donnée, sont justifiées par les besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de communications électroniques et des systèmes d'information, et lorsqu'elles sont mises en œuvre par des organismes publics ou privés ayant procédé à une déclaration préalable auprès du Premier ministre selon les modalités prévues par les dispositions du III de l'article 18 de la loi n° * du * pour la confiance dans l'économie numérique. »

3. Cet article 34 du projet « *LCEN* » est rédigé en des termes permettant de compléter les dispositions pénales sur la fraude informatique déjà existantes, et de les rendre conformes aux dispositions homologues de la Directive[66].

En effet, les articles 323-1 à 323-7 du Code pénal ne pénalisaient que le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données, d'altérer, d'entraver ou de fausser son fonctionnement, d'y introduire, supprimer ou modifier frauduleusement des données, la tentative de ces délits, la participation

---

[64] V. *supra*, §. 1.2.
[65] V. *supra*, conclusion du §. 1.2.
[66] V. *supra*, conclusion du §. 1.2.

à un groupement formé ou à une entente établie en vue de la préparation de ces infractions. Ils étaient en cela conformes à l'article 6.1 de la Directive (« *contournement de toute mesure technique efficace, que la personne effectue en sachant, ou en ayant des raisons valables de penser, qu'elle poursuit cet objectif* »).

L'article 34 du projet « *LCEN* », quant à lui, introduit également la pénalisation du « *fait de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre les faits prévus par les articles 323-1 à 323-3* », et est en cela conforme à l'article 6.2 de la Directive (« *la fabrication, l'importation, la distribution, la vente, la location, la publicité en vue de la vente ou de la location, ou la possession à des fins commerciales de dispositifs, produits ou composants ou la prestation de services* […] »).

L'article 6 de la Directive se trouverait ainsi parfaitement intégré dans la législation française. Il suffirait, pour satisfaire pleinement à l'obligation de transposer, d'introduire un article dans la loi de transposition énonçant que « *le contournement des mesures techniques de protection efficaces est réprimé par les articles 323-1 à 323-7 du Code pénal* », ces articles comprenant alors le futur article 323-3-1 tel que prévu par l'article 34 du projet « *LCEN* »[67].

4. À ce titre, Sylvie Rozenfeld[68] remarque d'ailleurs que « *ce texte* [de l'article 34] *se superposerait, en partie, à une disposition de l'avant-projet de loi sur le droit d'auteur dans la société de l'information qui protège les mesures techniques de protection des droits* ». Il s'agit bien entendu des dispositions transposant l'article 6 de la Directive. Parler de superposition, c'est reconnaître que ces articles édictent les mêmes dispositions. Or il est inutile et dangereux d'avoir les mêmes dispositions dans deux codes différents, à la fois le Code pénal et le Code de la propriété intellectuelle. Il convient donc de favoriser une insertion de ces mesures dans le Code pénal et non dans le Code de la propriété intellectuelle.

Ainsi, en admettant que cet article 34 soit adopté tel qu'il figure actuellement dans le projet de loi pour la confiance dans l'économie numérique, le droit pénal français de l'informatique se trouverait efficacement complété. La législation française serait alors en parfaite adéquation avec les dispositions communautaires, permettant d'accueillir en son sein, en vue de la transposition de la Directive, le délit de contournement des mesures techniques de protection.

Il est donc possible de considérer que le dispositif français actuel est satisfaisant s'agissant de la répression de la fraude informatique, en permettant dès à présent de sanctionner un grand nombre d'actes de « *contournement* ».

5. Dès lors, la transposition de l'article 6 de la Directive devrait s'effectuer au sein du droit pénal de l'informatique.

Il apparaît en effet inopportun, d'une part d'inventer de nouveaux dispositifs, alors que ceux existant actuellement et ceux à venir (« *LCEN* ») sont parfaitement adaptés et suffisants pour réprimer les infractions visées par l'article 6 de la Directive ; d'autre part de fractionner ces dispositions en les introduisant dans le Code de la propriété intellectuelle et non dans le Code pénal.

---

[67] V. *supra*, point 2 du §. 3.2.

[68] Sylvie Rozenfeld, « *Projet de loi sur l'économie numérique – Un contenu dicté par les directives européennes* », Expertises, février 2003, p. 43.

Conclusion

La répression du contournement des mesures techniques de protection – telle qu'énoncée par l'article 6 de la Directive du 22 mai 2001 – ne relève pas de la sphère d'influence accordée à l'auteur sur son œuvre.

D'autre part, le droit français répond d'ores et déjà pleinement aux objectifs fixés par cet article 6. La France disposant en effet d'un arsenal répressif important et largement suffisant au titre du contournement des mesures techniques de protection, le législateur pourrait se contenter d'introduire la neutralisation de ce contournement dans la législation relative à la fraude informatique, au sein du Code pénal. La transposition de l'article 6 dans le Code de la propriété intellectuelle serait donc inutile et inopportune, tout comme le serait l'assimilation du contournement des mesures techniques de protection à de la contrefaçon.

L'article 6 de la Directive devrait donc faire l'objet, lors de la transposition du texte communautaire en son entier, d'une attention particulière visant à respecter, en premier lieu, l'objectif d'harmonisation visé par la Directive, et en second lieu, la nécessaire cohérence du droit d'auteur français, en n'y ajoutant pas d'éléments extérieurs à sa logique propre.