

ALAI 2001 Rapports Nationaux  
Séance IC  
Belgique

Congrès 2001 de l'ALAI

Questionnaire I.C. : Les protections techniques vues dans un contexte juridique plus large

1. [Aucune réponse fournie].

**2. Droit commun de la responsabilité civile**

Le droit belge de la responsabilité civile repose principalement sur les dispositions des articles 1382 et 1383 du Code civil. L'article 1382 dispose que « tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer ». L'article 1383 ajoute que « chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou son imprudence ».

Trois éléments doivent être établis afin que la responsabilité d'une personne puisse être engagée. Il convient en effet de démontrer l'existence d'une faute, d'un dommage et, enfin, d'un lien de causalité entre la faute et le dommage subi.

La notion de faute n'est pas définie par la loi. La cour de cassation joue donc un rôle particulièrement important dans ce domaine, par son contrôle de la légalité des décisions des juges du fond. Afin de déceler une éventuelle faute, le juge doit comparer le comportement du défendeur à celui qu'aurait adopté une autre personne normalement prudente et avisée placée dans les mêmes circonstances<sup>1</sup>.

Pour être réparable, le dommage doit être certain<sup>2</sup>. La lésion d'un intérêt suffit, pour autant que cet intérêt soit légitime<sup>3</sup>.

Le lien de causalité requis pour la mise en œuvre de la responsabilité civile existe dès le moment où le dommage ne se serait pas réalisé tel qu'il s'est produit si la faute n'avait pas été commise<sup>4</sup>.

La simple neutralisation de mesures techniques en vue d'accéder à un contenu déterminé pourrait-elle être sanctionnée sur base du droit de la responsabilité civile ? Pour ce faire, il conviendrait tout d'abord de prouver une faute de la personne contournant le dispositif technique, ce qui ne sera pas toujours aisé<sup>5</sup>. En outre, le dommage réparable sera bien souvent très minime, voire inexistant en l'absence de diffusion.

Le droit de la responsabilité civile pourrait par contre plus efficacement sanctionner la mise à disposition du public de dispositifs de contournement des mesures techniques. En effet, dans ce cas, la faute et le préjudice seront plus

---

<sup>1</sup> J.-L. FAGNART, « La responsabilité civile. Chronique de jurisprudence 1985-1995 », *Dossiers du Journal des Tribunaux*, Bruxelles, Larcier, 1997, pp. 44-45, n°36. Pour un aperçu de la jurisprudence sur cette question, lire R.O. DALCQ, « Examen de jurisprudence (1980-1986). La responsabilité délictuelle et quasi délictuelle (1<sup>ère</sup> partie) », *Revue critique de jurisprudence belge (R.C.J.B.)*, 1987, pp. 607 et s.

<sup>2</sup> Cass., 28 mars 1990, *Journal des Tribunaux (J.T.)*, 1990, p. 452. Cf. également R.O. DALCQ et F. GLANSDORFF, « Examen de jurisprudence (1980-1986). La responsabilité délictuelle et quasi délictuelle (2<sup>ème</sup> partie) », *R.C.J.B.*, 1988, p. 436, n°110.

<sup>3</sup> J.-L. FAGNART, op. cit., p. 21.

<sup>4</sup> J.-L. FAGNART, op. cit., p. 25, n°13.

<sup>5</sup> Par exemple, dans le cas où un chercheur aurait besoin d'accéder à une œuvre disponible uniquement en ligne en vue de l'étudier et de la citer dans ses travaux, le contournement du dispositif technique pourrait difficilement être qualifié de fautif.

facilement démontrés, car l'efficacité du mécanisme de protection technique pourrait être réduite à néant par ces agissements.

Toutefois, pour des raisons pratiques de procédure, le recours au droit de la responsabilité civile n'est probablement pas la solution la plus adéquate. En effet, elle nécessite une action au fond, ce qui prend un certain temps. La possibilité d'initier une procédure en référé n'est pas pleinement satisfaisante car, d'une part, les mesures ordonnées en référé le sont à titre provisoire et, d'autre part, l'urgence doit être démontrée. Le recours au droit de la concurrence déloyale offre des réponses procédurales plus appropriées, grâce à la possibilité d'introduire une action en cessation<sup>6</sup>.

A notre connaissance, il n'existe d'ailleurs pas de jurisprudence basée sur le droit commun de la responsabilité civile en matière de contournement de mesures techniques.

Il n'est enfin pas exclu que la théorie de l'abus de droit permette, dans certaines circonstances, de limiter l'emploi de mesures techniques. En effet, on considère traditionnellement qu'il y a exercice abusif d'un droit lorsque les inconvénients causés à l'autre partie sont « sans commune mesure » avec les avantages que retire le titulaire du droit de l'exercice de celui-ci<sup>7</sup>. C'est donc par le biais d'un test de proportionnalité que l'on peut identifier les usages abusifs de droits<sup>8</sup>. Or, bloquer complètement<sup>9</sup> l'accès à des contenus qui ne seraient pas accessibles ailleurs, alors que les éléments protégés par la mesure technique sont nécessaires à l'exercice d'une activité licite par des tiers ou alors que ces contenus devraient être partiellement accessibles en vertu d'exceptions aux droits exclusifs de leurs auteurs<sup>10</sup>, pourrait conférer à l'utilisateur de la mesure technique un avantage sans commune mesure avec l'inconvénient résultant pour les tiers de la privation d'accès aux contenus ainsi protégés.

On pourrait également considérer que l'utilisation de mesures techniques au-delà des limites du droit d'auteur constituerait une utilisation des droits afférents aux mesures techniques qui ne serait pas justifiée par un intérêt légitime<sup>11</sup>. En effet, il ne semble pas légitime pour l'auteur de « neutraliser » les exceptions à ses droits en utilisant des mesures techniques de protection de son œuvre dans la mesure où les articles 23*bis* et 47*bis* de la loi belge du 30 juin 1994 sur le droit d'auteur et les droits voisins<sup>12</sup> ont conféré un caractère impératif aux exceptions aux droits de l'auteur et aux droits voisins.

### **3. Droit des télécommunications.**

La loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques<sup>13</sup> contient un chapitre consacré au secret des communications et à la protection de la vie privée (chapitre X*bis*).

L'article 109*ter* D de cette loi prévoit la protection des signes, signaux, écrits, images, sons, données de toute nature transmis par voie de télécommunication, en provenance d'autres personnes et destinées à celles-ci<sup>14</sup>. Ces données protégées ne doivent pas être cryptées pour bénéficier d'une protection. Aucune autre précision n'est faite

---

<sup>6</sup> Cf. infra sur ce point.

<sup>7</sup> Cass., 19 décembre 1983, *R.C.J.B.*, 1986, p. 304 ; J.-L. FAGNART, op. cit., pp. 54-56, n°45.

<sup>8</sup> P.-A. FORIERS, « Observations sur le thème de l'abus de droit en matière contractuelle », note sous Cass., 30 janvier 1992, *R.C.J.B.*, 1994, pp. 217-218, n°21.

<sup>9</sup> Sans considération du type d'usage envisagé.

<sup>10</sup> En ce qui concerne les œuvres protégées par le droit d'auteur, il convient d'être prudent car les tiers n'ont pas à proprement parler de droit sur l'œuvre (il ne s'agit que d'une limitation aux droits de l'auteur).

<sup>11</sup> Sur les différents critères révélateurs de l'abus de droit, lire S. STIJNS, D. VAN GERVEN et P. WERY, « Chronique de jurisprudence. Les obligations : les sources (1985-1995) », *J.T.*, 1996, p. 707, n°45.

<sup>12</sup> Cf. infra sur le droit d'auteur.

<sup>13</sup> *Moniteur belge* du 27 mars 1991, *err.* 20 juillet 1991.

<sup>14</sup> Dans la suite du texte, nous utiliserons la notion de « données protégées » pour parler de l'ensemble de ces éléments.

quant aux techniques de protection qui seraient nécessaires pour bénéficier de la couverture de l'article 109ter D. On peut en conclure que les données sus nommées sont protégées quel que soit leur état<sup>15</sup>.

Les actes sanctionnés sont décrits comme étant le fait de : prendre frauduleusement connaissance de l'existence des données protégées, transformer frauduleusement par n'importe quel procédé les données protégées, supprimer par n'importe quel procédé les données protégées, identifier les correspondants dans le cadre d'une télécommunication, relever ou faire usage des informations ou identifications obtenues (intentionnellement ou non), modifier ou annuler des données obtenues intentionnellement.

L'interdiction de transformation ou de suppression des données protégées existe quelque soit le procédé technique utilisé. Cette précision peut être étendue à la « prise de connaissance de l'existence » des données protégées, bien que cette précision ne soit pas apportée dans les textes.

Ces actes sont sanctionnés sauf consentement des personnes directement ou indirectement concernées par l'information, l'identification ou les données (art 109ter D, alinéa 1<sup>er</sup>).

Le législateur a toutefois prévu des exceptions à ce système (art. 109ter E): la protection n'est pas d'application si la loi prévoit expressément un de ces actes, si les actes sont accomplis dans le but de vérifier le fonctionnement du réseau (problème des maintenances techniques) ou si les actes sont nécessaires à l'intervention des services de secours en réponse à une demande d'aide (raison évidente de sécurité publique).

Ainsi, le Code d'instruction criminelle prévoit les procédures à suivre pour permettre les écoutes téléphoniques dans le cadre d'une instruction pénale. Ces procédures font l'objet du paragraphe 6 du titre VI du Code d'instruction criminelle (articles 90ter à 90decies). Les actes qui pourront être requis par un juge d'instruction sont l'écoute, la prise de connaissance et l'enregistrement pendant leur transmission des communications ou des télécommunications privées. On vise ici l'autorisation de mesures de surveillance. Le juge ne pourra prévoir ces procédures que si « les nécessités de l'instruction l'exigent », « à titre exceptionnel » et « si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité ». De plus ce n'est que pour les faits punissables prévus au paragraphe 2 de l'article 90ter que ces mesures peuvent éventuellement être requises. On voit donc que c'est dans un champ très étroit que ces méthodes de surveillance sont permises.

A noter aussi l'article 88bis du Code d'instruction criminelle qui permet au juge d'instruction de requérir un repérage des données d'appel de moyens de télécommunications ou la localisation de l'origine ou de la destination des télécommunications lorsque les circonstances rendent ces repérages nécessaire à la manifestation de la vérité<sup>16</sup>.

Les sanctions en cas d'infraction à l'article 109ter D sont prévues à l'article 114 § 2. Il s'agit de sanctions pénales : une amende de 50 à 50.000 francs belges<sup>17</sup> à multiplier par les décimes additionnels<sup>18</sup> est prévue pour la personne qui enfreint les articles 109ter D et E.

L'article 109quater ajoute à ces dispositions pénales la possibilité d'une intervention de l'IBPT<sup>19</sup>. En cas de manquement notamment à l'article 109ter D, l'IBPT peut adresser une mise en demeure motivée aux

---

<sup>15</sup> Il faut noter qu'en Belgique, selon l'article 109terF de la Loi de 1991 sur les entreprises publiques autonomes, l'emploi de la cryptographie est libre. La fourniture des services de cryptographie peut être soumise à la déclaration préalable auprès de l'autorité réglementaire nationale (IBPT – Institut Belge des Postes et des Télécommunications) pour les services déterminés par le Ministre. La détermination des services visés se fera donc par Arrêté royal. Aucun Arrêté n'a encore été pris à ce jour (31 décembre 2000) en la matière.

<sup>16</sup> L'article 109terE §2 prévoit que c'est par un Arrêté délibéré en Conseil des ministres que le Gouvernement déterminera les moyens par lesquels les opérateurs doivent permettre le repérage et les écoutes telles que prévues aux articles 88bis et 90ter à decies du Code d'instruction criminelle. Le Gouvernement s'instaure ainsi une possibilité de venir à bout de toute mesure de protection des données par cryptage ou autres technologies.

<sup>17</sup> 1 euros = 40.3399 francs belges.

<sup>18</sup> C'est-à-dire, à multiplier par 200 (au 31-12-2000).

contrevenants. Si les intéressés négligent la mise en demeure, une amende administrative peut être adressée : 10.000 à 100.000 francs belges<sup>20</sup> pour les personnes physiques, 0.5 à 5 % du chiffre d'affaires pour les personnes morales.

A côté des dispositions spécifiques du droit des télécommunications, le Code pénal belge contient deux articles sur la violation du secret des télécommunications. L'un concernant les infractions commises par des personnes qui exercent une fonction publique, l'autre plus général.

L'article 314*bis* du Code pénal expose le principe général du secret des communications et télécommunications privées. Les actes considérés comme constituant une violation du secret des communications et télécommunications sont l'écoute, la prise de connaissance et l'enregistrement des communications et des télécommunications privées auxquelles une personne ne prend pas part (et sans le consentement des participants à ces communications). Ces actes doivent avoir été accomplis intentionnellement pour être sanctionnés. L'article 314*bis* prévoit que ces actes peuvent avoir été commis « à l'aide d'un appareil quelconque » : aucun instrument quelles que soient ses spécifications techniques ne justifie la violation du secret des communications. Le seul fait d'installer ou de faire installer un appareil quelconque avec l'intention de commettre une des infractions mentionnées constitue également une infraction. Est également sanctionné, celui qui détient, révèle ou divulgue sciemment à une autre personne le contenu des communications illégalement enregistrées ou écoutées, ou dont il a pris connaissance illégalement. Enfin, l'article 314*bis* sanctionne quiconque utilise avec une intention frauduleuse ou à dessein de nuire, un enregistrement légalement effectué de communications ou de télécommunications privées.

L'article 259*bis* du Code pénal envisage le cas du fonctionnaire public ou de l'agent de la force publique qui se rendrait coupable intentionnellement dans l'exercice de ses fonctions (hors cas prévus par la loi ou en violant les conditions prévues par la loi lorsque celle-ci l'autorise) d'une violation du secret des télécommunications. Les faits visés sont les mêmes que ceux envisagés par l'article 314*bis*. La différence réside dans la sanction qui peut être infligée. Dans le premier cas, le coupable sera puni d'une amende de 100 à 10.000 francs belges et/ou d'un emprisonnement de six mois à un an, le fonctionnaire public quant à lui risque une amende de 500 à 20.000 francs belges et/ou d'un emprisonnement de six mois à deux ans.

Concernant les équipements hertziens et les équipements terminaux de télécommunication<sup>21</sup>, le régime instauré par la Directive européenne 1999/5<sup>22</sup> est d'application en Belgique depuis le 8 avril 2000. Ce régime a donné lieu à de nouvelles dispositions légales pour le commerce des équipements hertziens et terminaux de télécommunications<sup>23</sup>. Ce cadre réglementaire impose aux fabricants d'équipements que ceux-ci satisfassent à des exigences essentielles.

En Belgique, ces exigences essentielles sont définies à l'article 93 de la loi de 1991 sur les entreprises publiques autonomes. A côté de certaines spécifications obligatoires concernant la sécurité et la gestion des ressources rares, on trouve la possibilité qui est donnée au Ministre d'imposer pour certaines catégories d'équipements qu'il définira, des exigences de base concernant (notamment) la lutte contre la fraude, la protection des données à caractère personnel et la vie privée des utilisateurs et des abonnés, la prévention des dommages possibles au réseau, de l'abus des moyens du réseau et d'actions entraînant une détérioration inacceptable du service. Bien qu'aucun Arrêté ne soit encore pris à ce sujet, le Ministre pourrait trouver ici une voie pour interdire les systèmes de télécommunication permettant la réception non-autorisée de communications.

---

<sup>19</sup> Institut belge des postes et télécommunications : l'autorité réglementaire belge compétente en matière de télécommunications.

<sup>21</sup> *J.O.C.E.*, L 91/10 du 07.07.1999

<sup>22</sup> Directive 1999/5/CE du Parlement européen et du conseil du 9 mars 1999 concernant les équipements hertziens et les équipements terminaux des télécommunications et la reconnaissance mutuelle de leur conformité, *J.O.C.E.*, L 91/10 du 7 avril 1999.

<sup>23</sup> voy. Arrêté royal du 26 septembre 2000, *Moniteur belge*, 31 octobre 2000, p. 36388, ainsi que les modifications apportées à la loi du 21 mars 1991.

#### **4. Droit de l'audiovisuel.**

##### **Compétence des Communautés en matière audiovisuelle.**

Les problèmes liés à l'audiovisuel doivent en Belgique être analysés à trois niveaux. En effet, matière culturelle par excellence, l'audiovisuel relève de la compétence des Communautés (un type d'entité fédérée). Chaque Communauté (la Belgique en compte trois<sup>24</sup>) aura donc son régime propre.

##### ***Communauté française***

Le Décret sur l'audiovisuel de la Communauté française<sup>25</sup> comprend deux articles sur les programmes cryptés.

Tout d'abord l'article 19 du Décret précise que la télévision de service publique (RTBF) peut assurer seule une activité dont l'objet est la fourniture de services de télévision payants. La RTBF peut aussi s'associer à des partenaires publics ou privés pour créer des entreprises ou prendre des participations au capital d'entreprises existantes dont l'objet est la fourniture de services de TV payants.

En ce qui concerne la réception de programmes cryptés sans autorisation ou le décryptage de programmes cryptés, c'est l'article 43 du Décret qui traite de la problématique.

Les actes sanctionnés sont les suivants: le fait de décoder sciemment, sans en régler le prix, les signaux de tout ou partie des services de télévision payants ; transmettre sciemment en direct à un tiers qui n'a pas payé le prix du service, tout ou partie des programmes décodés d'un service de télévision payant ou fournir à un tel tiers l'enregistrement complet ou partiel de ces programmes ; recevoir sciemment d'un tiers sans régler le prix, soit en direct soit par voie d'enregistrement tout ou partie des programmes décodés d'un service de télévision payant.

La protection est assez élevée car même fournir une copie d'une émission provenant d'un service payant serait sanctionné.

En cas de découverte d'une de ces infractions, une amende de 26 à 10.000 francs belges<sup>26</sup> (multipliée par les décimes additionnels) pourra être infligée.

La sanction est accompagnée de la confiscation des appareils ayant permis de commettre l'infraction (art. 43 du Décret renvoi à l'art. 42 du Code pénal). L'article 43 du Décret précise encore que toutes les dispositions du Livre 1<sup>er</sup> du Code pénal sont applicables aux infractions du présent Décret. Ainsi pourra s'appliquer la notion de participation : celui qui, par un fait quelconque, aura prêté pour l'exécution une aide telle que, sans leur assistance, le crime ou délit n'eût pu être commis (article 66 du Code pénal).

##### ***Communauté flamande.***

Le Décret flamand relatif à la radiodiffusion et à la télévision<sup>27</sup> traite également de la question des services de télévision payants.

---

<sup>24</sup> La Communauté française qui couvre la partie francophone du territoire, la Communauté flamande qui couvre la partie néerlandophone du territoire, et la Communauté germanophone qui couvre la partie germanophone du territoire.

<sup>25</sup> Décret sur l'audiovisuel du 17 juillet 1987, *Moniteur belge* du 22 août 1987.

<sup>26</sup> 1 euro = 40.3399 francs belges

<sup>27</sup> Décrets relatifs à la radiodiffusion et à la télévision, coordonnés le 25 janvier 1995, *Moniteur belge* 30 mai 1995.

L'article 119 du Décret vise les appareils ou éléments de ceux-ci permettant de capter et/ou utiliser de manière frauduleuse des programmes et/ou des services uniquement accessibles au public moyennant paiement d'un montant en sus du prix de l'abonnement du câble et/ou de la redevance radio et télévision.

Les actes sanctionnés sont la fabrication, la mise en vente, la mise en location, la vente, la location, l'importation, la distribution, la promotion, l'installation, la conservation ou le remplacement, le fait de procéder à l'achat ou à la location, la détention en vue de l'utilisation.

Est également sanctionné l'acte de décodage sans autorisation du propriétaire de la technologie de codage (ou du tiers désignés par celui-ci pour délivrer l'obligation).

Les sanctions pénales prévues sont une peine de prison pouvant aller de 8 jours à 5 ans, et/ou un amende de 1.000 à 100.000 francs belges (multipliée par les décimes additionnels).

On vise donc ici des services payants, sans préciser si ceux-ci doivent ou non être cryptés.

### ***Communauté germanophone.***

Le Décret sur les médias de la Communauté Germanophone<sup>28</sup> ne comporte aucune disposition concernant la sanction du décryptage illégal de programmes codés ou la vente d'appareils permettant le décryptage frauduleux. Ce sera donc le droit de la concurrence déloyale qui s'appliquera et plus particulièrement la loi sur les pratiques du commerce<sup>29</sup>.

### **Loi sur les pratiques du commerce.**

Le législateur fédéral, s'il n'a pas de compétence directe en ce qui concerne le domaine de l'audiovisuel, traite indirectement la problématique du décryptage par le biais du droit de la concurrence déloyale.

Avant que soient prises dans chaque Communauté des dispositions spécifiques concernant les émissions cryptées, c'est le droit de la concurrence déloyale qui était en effet utilisé pour fonder une action contre la commercialisation de décodeurs pirates. En effet, une décision de la Cour d'appel de Liège du 20 avril 1990 souligne le caractère spécifique des programmes codés, en précisant que si les ondes hertziennes ne sont pas susceptibles d'appropriation, cela « ne modifie en rien les droits de celui de qui émane le message hertzien qui a d'ailleurs manifesté par le cryptage de ce message, qu'il entendait en garder la maîtrise »<sup>30</sup>.

## **5. Criminalité informatique**

Avec beaucoup de retard, bien souvent critiqué, la Belgique s'est finalement dotée d'une loi relative à la criminalité informatique le 28 novembre 2000<sup>31</sup>. Cette loi instaure de nouvelles infractions touchant aux systèmes informatiques, dont certaines pourraient servir de base à la poursuite d'actes de neutralisation d'un dispositif technique de protection ou d'actes de fabrication et de commercialisation d'outils permettant cette neutralisation.

L'infraction la plus pertinente en la matière est celle de l'accès non autorisé à un système informatique, introduit dans notre droit pénal par le nouvel article 550bis du Code Pénal.

---

<sup>28</sup> Décret sur les médias du 26 avril 1999, *Moniteur belge*, 17 juillet 1999.

<sup>29</sup> Loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection des consommateurs, *Moniteur belge*, 21 août 1991.

<sup>30</sup> Liège, 20 avril 1990, *J.T.*, 1990, pp. 642 et s. Pour plus de détails, cf. *infra* sur le droit de la concurrence déloyale.

<sup>31</sup> *Moniteur belge*, 3 février 2001, p. 2909.

L'article 550bis vise :

- les atteintes portées à partir de l'extérieur du système, soit le *hacking* externe (§ 1)
- les atteintes portées par des utilisateurs qui possèdent certains pouvoirs d'accès, soit le *hacking* interne (§2)
- les actes préparatoires : les *hackertools* (§ 5)
- le fait de commanditer un *hacking* (§ 6)
- le « recel » de données obtenues à la suite des infractions précédentes (§7)

a) L'infraction de *hacking*

Le *hacking* ou accès non autorisé aux systèmes informatiques constitue une des infractions classiques en matière de criminalité informatique, et, à tout le moins, celle dont les agissements sont le plus souvent médiatisés.

L'article 550bis distingue plusieurs hypothèses pourvues de peines largement différentes. Une première distinction est établie entre les actes d'accès illicite commis par une personne externe au système informatique enfreint (« *hacking* externe ») et les intrusions en provenance de l'intérieur même du système (« *hacking* interne »). Mais la loi fait également une distinction entre le *hacking* externe commis avec ou sans intention frauduleuse.

*« - § 1er . Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement.*

*Si l'infraction visée à l'alinéa 1<sup>er</sup>, est commise avec une intention frauduleuse, la peine d'emprisonnement est de six mois à deux ans.*

*§ 2. Celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepassé son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement. (...) »*

Le nouvel article 550bis du Code Pénal, pénalise le simple accès non autorisé à un système informatique ou le maintien indu dans le système, sans qu'aucune condition, parfois exigée pour la criminalisation de l'accès, telle que déverrouillage des mesures de sécurité ou but d'obtention de données ou de sabotage, ne soit requise. L'accès à un système ou à des données informatiques est donc constitutif d'une infraction pénale dès que cet accès n'est pas autorisé. Que cet accès s'effectue en violation des mesures de sécurité et des dispositifs techniques de protection importe peu, bien que cette violation apportera la preuve de l'absence d'autorisation d'accès au système. Exiger que l'infraction se réalise moyennant un 'cassage' des dispositifs de sécurité aurait eu pour désavantage de contraindre les plaignants à exposer publiquement les mesures de sécurité et la manière dont elles auraient été contournées, ce qui serait préjudiciable pour leur sécurité future.

L'acte de maintien dans un système informatique, également sanctionné par l'article 550bis, est la conséquence logique de l'accès. Il suffit qu'au delà de l'intrusion dans le système, on s'y "promène" un certain temps, pour que l'élément de maintien soit satisfait. Ainsi, même si l'accès au système n'a pas été commis de manière illicite, un séjour prolongé de manière non autorisée pourra être poursuivi. Ce serait par exemple le cas si, suite à un accès licite à une base de données payante, on déjoue les systèmes permettant de calculer le prix lié à la durée de connexion ou au nombre de consultations.

L'infraction d'accès et de maintien non autorisé dans un système informatique est punissable même si elle est accomplie sans intention frauduleuse, ce qui a suscité de nombreuses critiques<sup>32</sup>. Le Conseil d'Etat s'est d'ailleurs inquiété du fait que "*dans un contexte informatique, la simple curiosité peut susciter un délit pénal*"<sup>33</sup>. Selon le législateur belge, il s'agissait de protéger l'intégrité du système<sup>34</sup> et la sécurité des systèmes informatiques<sup>35</sup>. En conséquence, le simple fait de déverrouiller un dispositif d'accès à un système informatique et à des données, par exemple à une œuvre protégée par le droit d'auteur, suffira à constituer le délit, que l'intention ait été frauduleuse ou non. Cette absence de dol spécial criminalise le contournement des mécanismes techniques de contrôle d'accès quelle que soit l'intention de ce dernier et empêche que les exceptions et limites au droit d'auteur, ou quelque autre moyen de justification, puissent servir de défense à l'incrimination.

Une intention frauduleuse ne sera toutefois pas sans incidence puisqu'elle justifiera l'aggravation des peines jusqu'à deux ans d'emprisonnement et vingt-cinq mille francs d'amende. En outre, la présence d'une intention frauduleuse est requise lorsque le hacking se réalise en interne, par des employés notamment.

La loi mentionne également une série de circonstances considérées comme aggravantes, lorsque le pirate informatique

*1° soit reprend de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique*

*2° soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers;*

*3° soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées, traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système;*

Ces circonstances aggravantes sont susceptibles d'être fréquemment rencontrées en matière de contournement des mesures techniques de protection. Reproduire ou communiquer au public les données et œuvres auxquelles le pirate aura accédé 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*.

#### b) Les *hacker tools*

Le 5<sup>ème</sup> paragraphe de l'article 550bis du Code Pénal dispose désormais :

*§ 5. Celui qui, avec une intention frauduleuse ou dans le but de nuire, recherche, rassemble, met à disposition, diffuse ou commercialise des données qui sont stockées, traitées ou transmises par un système informatique et par lesquelles les infractions prévues par les §§ 1<sup>er</sup> à 4 peuvent être commises, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement.*

L'objectif de cette disposition est de sanctionner les personnes qui conçoivent et diffusent des outils de *hacking* et de déverrouillage des dispositifs de sécurité. La commercialisation de mots de passe, de clés de décryptage, de logiciels permettant de craquer des codes d'accès devient donc un délit. La simple recherche de tels moyens est criminalisée si cette recherche poursuit un but de nuire, ce qui inquiète particulièrement les milieux de la recherche en cryptographie et de la sécurité informatique.

<sup>32</sup> F. DE VILLENFAGNE & S. DUSOLLIER, "La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique", *Auteurs & Média (A.&M.)*, 2001/01; C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique", *Formation Permanente CUP*, février 2001, vol. 45, p. 78.

<sup>33</sup> Avis du Conseil d'Etat, *Doc. Parl.*, Chambre, 1999-2000, 0213/001 et 0214/001, p. 50.

<sup>34</sup> *Doc. Parl.*, Chambre 0213/001, *op. cit.*, p. 17

<sup>35</sup> Justification de l'amendement n°11, *Doc. Parl.*, Chambre 0213/010, 22 septembre 2000.



c) L'infraction de fraude informatique

L'article 504quater du Code pénal introduit par la loi incrimine le fait de "*se procurer, pour soi-même ou pour autrui, un avantage patrimonial frauduleux en introduisant dans un système informatique, en modifiant ou en effaçant des données qui y sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique*".

Selon nous, cette infraction de fraude informatique pourrait trouver à s'appliquer à certains actes relatifs aux dispositifs techniques de protection.

Par exemple, 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, pourraient constituer une fraude informatique, l'avantage patrimonial frauduleux consistant en l'utilisation et la copie d'un logiciel sans autorisation de l'auteur.

## **6. Droit de la concurrence déloyale**

Le droit belge de la concurrence déloyale repose sur les dispositions de la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur (ci-après « LPC »)<sup>36</sup>, et plus particulièrement sur l'article 93 de cette loi, qui énonce que « est interdit tout acte contraire aux usages honnêtes en matière commerciale par lequel un vendeur porte atteinte ou peut porter atteinte aux intérêts professionnels d'un ou de plusieurs autres vendeurs »<sup>37</sup>.

La violation de cette norme générale<sup>38</sup>, destinée à assurer la loyauté des opérations commerciales, ouvre la voie à deux actions : une action au fond en dommages et intérêts et, surtout, une action en cessation<sup>39</sup>. Cette dernière action est instruite selon une procédure accélérée, comme en référé, et tranche (partiellement) le litige au fond. Comme son nom l'indique, elle permet d'obtenir du tribunal qu'il ordonne la cessation des actes enfreignant la norme de l'article 93 LPC. Les juges compétents pour connaître des actions en cessation<sup>40</sup> ne peuvent cependant statuer sur les demandes tendant à la condamnation au paiement de dommages et intérêts (ce qui relève des juridictions du fond). Outre la rapidité, cette procédure présente principalement deux avantages. D'une part, elle

---

<sup>36</sup> *Moniteur belge* 29 août 1991.

<sup>37</sup> Le « vendeur » est défini à l'article 1.6. LPC comme « a) tout commerçant ou artisan ainsi que toute personne physique ou morale qui offrent en vente ou vendent des produits ou des services, dans le cadre d'une activité professionnelle ou en vue de la réalisation de leur objet statutaire ; b) les organismes publics ou les personnes morales dans lesquels les pouvoirs publics détiennent un intérêt prépondérant qui exercent une activité à caractère commercial, financier ou industriel et qui offrent en vente ou vendent des produits ou des services ; c) les personnes qui exercent avec ou sans but de lucre une activité à caractère commercial, financier ou industriel, soit en leur nom propre, soit au nom et pour le compte d'un tiers doté ou non de la personnalité juridique et qui offrent en vente ou vendent des produits ou des services ». Sur la portée de la notion, lire J. STUYCK et C. GOEMANS, « 'consommateurs' et 'vendeurs' dans la loi sur les pratiques du commerce », in *Les pratiques du commerce, autour et alentour*, Bruxelles, FUSL, 1997, pp. 17-37.

<sup>38</sup> Pour une étude du contenu de cette norme et de ses origines, cf. J. STUYCK, « L'acte contraire aux usages honnêtes en matière commerciale », in *Les pratiques du commerce et la protection et l'information du consommateur depuis la loi du 14 juillet 1991*, Editions du Jeune Barreau de Bruxelles, 1991, pp. 125-174.

<sup>39</sup> Article 95 LPC : « Le président du tribunal de commerce constate l'existence et ordonne la cessation d'un acte, même pénalement réprimé, constituant une infraction aux dispositions de la présente loi ».

<sup>40</sup> Les présidents des tribunaux de commerce siégeant comme en référé.

ne requiert pas la démonstration de l'urgence (contrairement à la procédure de référé)<sup>41</sup> et, d'autre part, elle peut être intentée à titre préventif<sup>42</sup>.

Jusqu'à l'entrée en vigueur de la nouvelle loi sur le droit d'auteur et les droits voisins (ci-après « LDA »)<sup>43</sup>, cette action accélérée spécifique constituait, pour les plaideurs, un des principaux attraits du recours au droit de la concurrence déloyale car l'ancienne loi sur le droit d'auteur<sup>44</sup> n'offrait pas pareille possibilité au titulaire du droit d'auteur violé, qui ne pouvait alors introduire, outre l'action au fond, qu'une action en référé (et dès lors n'obtenir que des mesures provisoires). La LDA a comblé cette lacune en offrant aux titulaires de droits d'auteur la possibilité d'introduire une action en cessation spécifique<sup>45</sup>. L'intérêt procédural du recours au droit de la concurrence déloyale a dès lors pour partie disparu lorsqu'il s'agit de protéger indirectement le droit d'auteur.

La jurisprudence et la doctrine se sont interrogées sur l'étendue des possibilités de recourir à l'action en cessation en vue de faire cesser des pratiques comportant des infractions au droit d'auteur. En effet, l'article 96 LPC précise que le juge de la cessation n'est pas compétent pour faire cesser les actes de contrefaçon du droit d'auteur<sup>46</sup>. Cette disposition a été reprise de l'ancienne législation sur les pratiques du commerce<sup>47</sup> (article 56). La jurisprudence se prononce généralement en faveur d'une interprétation restrictive de l'exclusion de l'action en cessation commerciale en matière d'atteintes au droit d'auteur. Si l'action en cessation commerciale doit être exclue lorsque l'action vise à faire cesser une atteinte au droit d'auteur<sup>48</sup>, elle est ouverte dans les cas où l'objet de la demande porte sur une pratique commerciale qui, en négligeant le droit d'auteur, fausse le jeu de la concurrence en défavorisant les commerçants qui respectent les droits des auteurs<sup>49</sup>. Peu importe que les produits considérés soient protégés par le droit d'auteur, l'action ne vise pas l'atteinte au droit d'auteur en tant que telle mais plutôt les pratiques commerciales dans lesquelles s'inscrit cette atteinte au droit d'auteur. Il ne s'agit plus de protéger le droit d'auteur mais de sauvegarder les éléments du patrimoine d'une entreprise contre certaines pratiques commerciales de tiers, qui, en négligeant le droit d'auteur, confèrent à ce tiers un avantage concurrentiel déloyal ou constituent un acte de parasitisme économique<sup>50</sup>.

La jurisprudence belge a déjà sanctionné la commercialisation d'appareils permettant de neutraliser des dispositifs techniques de contrôle d'accès. Plusieurs décisions ont été prononcées dans le cadre de litiges relatifs à la commercialisation de décodeurs pirates offrant la possibilité de décrypter de manière non autorisée les émissions de chaînes de télévision à péage. La cour d'appel de Bruxelles a ainsi souligné « *qu'il n'est pas conforme à la moralité des affaires de greffer son activité sur celle d'une autre entreprise déterminée en commercialisant un produit qui a pour seule fonction de déjouer la protection licite dont cette autre entreprise a entouré son activité* ;

---

<sup>41</sup> Cf. notamment V. d'HUART et A.-F. HONHON, « La procédure », in *Pratiques du commerce*, CUP, vol.XVI, 1997, p. 73.

<sup>42</sup> Cf. le libellé de l'article 93 LPC, qui vise les actes par lesquels un vendeur porte atteinte ou peut porter atteinte aux intérêts professionnels d'un autre vendeur.

<sup>43</sup> Loi du 30 juin 1994, *Moniteur Belge*, 27 juillet 1994.

<sup>44</sup> Loi du 22 mars 1886.

<sup>45</sup> Article 87 LDA.

<sup>46</sup> Article 96 LPC : « L'article 95 ne s'applique pas aux actes de contrefaçon qui sont sanctionnés par les lois sur les brevets d'invention, les marques de produits ou de services, les dessins ou modèles et le droit d'auteur et les droits voisins ».

<sup>47</sup> Loi du 14 juillet 1971, *Moniteur Belge*, 30 juillet 1971.

<sup>48</sup> En ce sens, lire notamment Liège, 24 mars 1989, *Revue de Jurisprudence de Liège, Mons, Bruxelles (J.L.M.B.)*, 1989, pp. 888-889.

<sup>49</sup> En ce sens, lire : Com. Bruxelles, 2 avril 1990, *J.L.M.B.*, 1991, p. 260-263 ; Président Com. Ypres, 21 décembre 1990, *Revue de droit commercial belge (R.D.C.)*, 1991, 351-356. Egalement J.-J. EVRARD, *Chronique de jurisprudence (1978-1984) : les pratiques du commerce*, *J.T.*, 1985, p. 196, n°99.

<sup>50</sup> Lire l'étude de I. VEROUGSTRAETE, « Droit d'auteur et pratiques du commerce », in *Les journées du droit d'auteur*, Actes du colloque organisé à l'Université Libre de Bruxelles les 11 et 12 décembre 1987, Bruylant, 1989, p. 226.

qu'un tel agissement est un abus de la liberté d'entreprendre »<sup>51</sup>. La cour d'appel de Liège abonde dans le même sens, estimant « qu'aucune entreprise ne peut licitement rattacher son activité à celle d'une autre entreprise en vue de détruire, dans un but lucratif, le système de protection dont cette dernière s'est entourée »<sup>52</sup>.

Si le caractère général de la norme permet une grande souplesse, le principal inconvénient du recours au droit de la concurrence déloyale réside précisément dans l'incertitude relative que présente le recours à une norme très générale d'évaluation des comportements<sup>53</sup>.

## **7. Protection du dispositif technique**

### **7.1. Droit d'auteur**

Dans la mesure où les dispositifs techniques de protection des œuvres pourraient s'apparenter à un programme d'ordinateur, ils sont susceptibles de bénéficier de la protection du droit d'auteur telle qu'organisée par la loi du 30 juin 1994 transposant en droit belge la directive européenne du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur (ci-après « LPO »)<sup>54</sup>. La proposition originelle de directive sur la protection juridique des programmes d'ordinateur définissait ceux-ci comme « l'expression, dans toute forme, tout langage, toute notation ou tout code, d'un ensemble d'instructions ayant pour objet de permettre à un ordinateur d'accomplir une tâche ou une fonction particulière »<sup>55</sup>. La version finalement adoptée n'a retenu aucune définition, afin d'éviter que celle-ci ne devienne trop vite obsolète et ne restreigne dès lors le champ d'application des dispositions de la directive. Pour bénéficier de la protection, le dispositif technique doit être original, « en ce sens qu'il est une création intellectuelle propre à son auteur » (article 2 LPO). Compte tenu de la relative largesse des tribunaux quant à l'appréciation de la condition d'originalité<sup>56</sup>, de nombreux dispositifs techniques de protection des œuvres devraient pouvoir entrer dans le champ d'application de la législation protectrice des programmes d'ordinateur (ECMS, système de gestion d'accès conditionnel, par exemple)<sup>57</sup>.

Le contournement du dispositif technique de protection nécessitera plus que vraisemblablement de poser des actes couverts par les prérogatives exclusives du titulaire des droits d'auteur sur le dispositif technique (reproduction, adaptation). La fabrication de mécanismes de contournement requiert pareillement des actes de reproduction et d'adaptation. Le droit d'auteur pourrait donc constituer un moyen de protection efficace. Cependant, seul le titulaire des droits d'auteur sur le programme d'ordinateur que constitue le dispositif technique de protection pourra invoquer le droit d'auteur, ce qui semble, à première vue, réduire fortement l'intérêt pratique de la solution. Toutefois, l'action en cessation de l'atteinte au droit d'auteur est ouverte à « tout intéressé »<sup>58</sup>, c'est-à-dire à « quiconque peut justifier d'un intérêt né et actuel au sens des articles 17 et 18 du code judiciaire »<sup>59</sup>. Le titulaire d'une simple licence d'utilisation d'un programme de protection technique des œuvres pourrait dès lors introduire une action en cessation afin de faire interdire les pratiques de contournement des dispositifs techniques de

<sup>51</sup> Bruxelles, 13 juin 1986, *J.T.*, 1986, pp. 529-531 (observations L. VAN BUNNEN).

<sup>52</sup> Liège, 20 avril 1990, *Revue régionale de droit*, 1990, pp. 503-506. Cf. également Comm. Liège (prés.), 9 janvier 1998, *A. & M.*, 1999, pp. 106

<sup>53</sup> Cf. A. STROWEL et J.-P. TRIAILLE, *Le droit d'auteur, du logiciel au multimédia*, Cahier du Crid n°11, Bruxelles, Bruylant, 1997, n° 192 et 193.

<sup>54</sup> *Moniteur belge*, 27 juillet 1994.

<sup>55</sup> A ce propos, lire A. STROWEL et J.-P. TRIAILLE, op. cit., pp. 144-147.

<sup>56</sup> Sur la portée de la condition d'originalité, lire A. STROWEL, « L'originalité en droit d'auteur, un critère à géométrie variable », *J.T.*, 1991, pp. 513-518.

<sup>57</sup> En ce sens, S. DUSOLLIER, « Electrifying the fence : the legal protection of technological measures for protecting copyright », *E.I.P.R.*, 1999, n°6, pp. 285-297.

<sup>58</sup> Article 87 LDA.

<sup>59</sup> A. et B. STROWEL, « La nouvelle législation belge sur le droit d'auteur », *J.T.*, 1995, p. 136, n° 108. Lire également F. DE VISSCHER et B. MICHAUX, *Précis du droit d'auteur et des droits voisins*, Bruxelles, Bruylant, 2000, n°646 (prônant une interprétation large visant toute personne qui est lésée par la violation du droit concerné).

protection de l'accès aux œuvres, dans la mesure où elles impliqueraient une utilisation des prérogatives exclusives relevant du droit d'auteur afférent au programme d'ordinateur que constituerait le système technique. Il semble en effet difficile de nier l'existence d'un intérêt dans la mesure où les pratiques litigieuses réduisent l'utilité de la licence d'utilisation qui lui a été concédée.

La personne contournant un dispositif technique pourrait de son côté difficilement invoquer le bénéfice des exceptions aux droits d'auteur prévues par la législation spécifique aux programmes d'ordinateur. En effet, si, par exemple, elle contourne les dispositifs techniques anti-copie en vue de réaliser une copie de sauvegarde d'un programme d'ordinateur, l'exception de copie de sauvegarde ne pourra être invoquée car elle ne joue dans ce cas que concernant les actes de reproduction du programme d'ordinateur protégé et non concernant les actes de reproduction du programme que constitue le dispositif anti-copie.

Il en va de même en ce qui concerne l'exception de décompilation dont le bénéfice est limité aux personnes ayant le droit d'utiliser le programme décompilé et qui ne peut être invoquée qu'afin de pouvoir obtenir les informations nécessaires à l'interopérabilité d'un programme d'ordinateur créé de façon indépendante avec d'autres programmes.

Les exceptions aux droits d'auteur sur les programmes d'ordinateur n'ont pas été envisagées dans le contexte d'un nécessaire et préalable contournement de dispositifs techniques. Leur non application dans ce contexte pourrait les rendre de nul effet lorsque les programmes auxquels elles sont censées s'appliquer sont protégés par des dispositifs techniques. L'équilibre de la directive programmes d'ordinateur pourrait donc être perturbé par le recours aux dispositifs techniques de protection des œuvres. La législation devrait être adaptée afin de permettre des actes de reproduction et d'adaptation d'un programme de protection technique réalisés pour contourner cette protection technique en vue d'exercer les exceptions permises par la loi sur le programme ou l'œuvre objet de la protection technique. Le caractère impératif des exceptions au droit d'auteur prévues par la LDA et d'une partie des exceptions prévues par la LPO renforce cette nécessité d'adaptation. En l'état actuel du droit belge, on pourrait envisager l'application de la théorie de l'abus de droit dans les hypothèses où l'exercice du droit d'auteur sur la mesure technique « neutraliserait » l'exercice des exceptions au droit d'auteur sur l'œuvre protégée par la mesure technique<sup>60</sup>.

En ce qui concerne les dispositifs techniques dont l'objet est de protéger un programme d'ordinateur, l'article 10 de la LPO prévoit que « Les atteintes au droit d'auteur sur un programme d'ordinateur sont sanctionnées conformément à la loi. Sont par ailleurs punis d'une amende de 100 à 100.000 francs ceux qui mettent en circulation ou qui, à des fins commerciales, détiennent une copie d'un programme d'ordinateur en sachant qu'elle est illicite ou en ayant des raisons de le croire, ainsi que ceux qui mettent en circulation ou détiennent à des fins commerciales tout moyen ayant pour seul but de faciliter la suppression non autorisée ou la neutralisation des dispositifs techniques qui protègent le programme d'ordinateur ». Les seuls cas couverts par cette disposition sont ceux relatif à des moyens dont le seul but est de contourner des dispositifs techniques de protection. Si la sanction pénale de ce type de comportement est acquise, la possibilité de recourir à l'action en cessation civile en pareil cas est moins évidente. En effet, l'article 10 LPO envisage les atteintes au droit d'auteur sur un programme d'ordinateur (renvoi à la LDA) et par ailleurs énonce des sanctions pénales spécifiques concernant la mise en circulation de copies illicites ainsi que de moyens de contournement des dispositifs techniques de protection des programmes d'ordinateur. Si la disposition ne visait que les actes relatifs aux moyens de contournement des dispositifs techniques de protection des programmes d'ordinateur, il semblerait logique d'écarter la possibilité d'action en cessation civile car il n'y a pas d'atteinte au droit d'auteur sur le programme protégé par les actes visés. Mais la disposition vise également la mise en circulation de copies illicites qui, à tout le moins, porte atteinte au droit de distribution de l'auteur, ce qui rend son interprétation pour le moins malaisée<sup>61</sup>.

---

<sup>60</sup> Cf. supra à propos du droit de la responsabilité civile.

<sup>61</sup> En faveur de la possibilité de l'action en cessation, cf. F. DE VISSCHER et B. MICHAUX, op. cit., n°632.

## **7.2. Droit des brevets**

La matière du droit des brevets est régie par la loi du 28 mars 1984 sur les brevets d'invention (ci-après « LBI »)<sup>62</sup>. Pour être susceptible de bénéficier de la protection accordée par cette législation, une création doit répondre à quatre conditions cumulatives (et faire en outre l'objet d'une procédure de dépôt)<sup>63</sup> : il doit s'agir d'une invention (1) nouvelle (2) résultant d'une activité inventive (3) et susceptible d'application industrielle (4).

La LBI ne définit pas l'invention. On considère généralement que ce concept couvre toute invention dans le domaine de la technique<sup>64</sup>. Selon l'article 5 LBI, la nouveauté de l'invention doit s'apprécier par rapport à l'état de la technique, qui comprend l'ensemble des connaissances accessibles au public ou contenues dans des demandes de brevets. Une invention est considérée comme impliquant une activité inventive « si, pour un homme du métier, elle ne découle pas de d'une manière évidente de l'état de la technique »<sup>65</sup>. Enfin, la condition d'application industrielle limite le champ d'application du droit des brevets aux inventions susceptibles d'être fabriquées ou utilisées dans tout genre d'industrie, y compris l'agriculture<sup>66</sup>.

L'application cumulative de ces différentes conditions ne devrait *a priori* pas exclure les dispositifs techniques de protection des œuvres du champ du droit des brevets<sup>67</sup>. Mais il convient de ne pas perdre de vue l'exclusion des programmes d'ordinateur, édictée par l'article 52 de la Convention de Munich du 5 octobre 1973 sur le brevet européen<sup>68</sup>. L'éventuelle demande de brevet devra donc porter sur un procédé de protection des œuvres et non directement sur le logiciel mettant en œuvre ce procédé<sup>69</sup>.

Le titulaire d'un brevet dispose du droit exclusif d'exploiter ou d'autoriser l'exploitation de l'invention faisant l'objet du brevet. Ce droit exclusif porte sur la fabrication, l'offre, la mise dans le commerce, l'importation ou la détention du produit objet du brevet, ainsi que sur l'exploitation du procédé objet du brevet ou du produit obtenu grâce à ce procédé<sup>70</sup>.

La mise au point d'un mécanisme de contournement d'un dispositif technique est-elle constitutive d'une contrefaçon du brevet portant sur le procédé de protection de l'œuvre ?

Différentes hypothèses envisagées par la loi sur le brevet pourraient inclure les actes liés à la fabrication et/ou la mise à disposition du public d'un procédé de contournement.

Ainsi, il y a utilisation illicite du procédé breveté dès lors qu'il y a reprise des étapes essentielles du procédé breveté. Si le mécanisme de contournement du dispositif technique reprend les étapes essentielles du procédé breveté, il y aura donc utilisation de ce procédé au sens de la loi.

L'offre du produit breveté au sens de la loi vise l'offre en général, en ce compris le don<sup>71</sup>. Pour autant que le dispositif de contournement soit mis à disposition du public accompagné des éléments essentiels du procédé breveté.

---

<sup>62</sup> Moniteur belge, 9 mars 1985. L'exposé n'envisagera pas les brevets européens et internationaux.

<sup>63</sup> Article 2 LBI.

<sup>64</sup> M. BUYDENS, *Droit des brevets d'invention et protection du savoir-faire*, Bruxelles, Larcier, 1999, n°96.

<sup>65</sup> Article 6 LBI. Sur la portée de ce critère, cf. notamment Gand, 19 janvier 1993, *Revue de droit intellectuel – L'Ingénieur-Conseil (Ing.-Cons.)*, 1993, p. 22.

<sup>66</sup> Article 7 LBI.

<sup>67</sup> Pour des exemples d'application de ces différents critères, lire P. VAN DEN BULCK, *Synthèses de jurisprudence : les brevets*, Diegem, Kluwer, 1999, pp. 2-8.

<sup>68</sup> Approuvée par la loi du 8 juillet 1977, *M.B.*, 30 septembre 1977.

<sup>69</sup> En ce sens, lire M. BUYDENS, op. cit., n°150.

<sup>70</sup> A propos des droits conférés par le brevet et leurs limites, lire notamment M. BUYDENS, op. cit., pp. 137 et s.

<sup>71</sup> M. BUYDENS, op. cit., n°375.

La mise dans le commerce vise quant à elle tout acte de mise à disposition du public<sup>72</sup>.

En outre, il convient de préciser que les actes couverts par le brevet doivent avoir été accomplis à des fins commerciales ou à des fins non purement privées pour être constitutifs de contrefaçon<sup>73</sup>. Il ne semble donc pas possible de sanctionner tous les actes de *hacking* sur base de la législation sur le brevet<sup>74</sup>.

Enfin, dans certaines circonstances, il pourrait y avoir offre ou utilisation du produit obtenu par le procédé breveté. En effet, si le procédé a pour objet de donner l'accès à l'œuvre à laquelle le dispositif technique est appliquée, on pourrait considérer que mettre à disposition du public un système de contournement du procédé breveté revient à offrir l'accès à l'œuvre concernée. Mais cet artifice n'est possible que pour autant que l'on puisse considérer l'accès comme le produit du procédé de protection breveté, ce qui n'est pas évident.

Le droit des brevets offre donc peu de possibilités de sanctionner la fabrication ou la mise à disposition du public de mécanismes de contournement.

### **7.3. Protection des secrets de fabrique et du savoir-faire**

L'article 309 du code pénal sanctionne de trois mois à trois ans de prison et d'une amende de 50 à 2.000 BEF (multipliée par les décimes additionnels) « celui qui aura méchamment ou frauduleusement communiqué des secrets de la fabrique dans laquelle il a été ou est encore employé »<sup>75</sup>.

Le droit civil belge ne comporte quant à lui aucune règle spécifique de protection des secrets d'affaires ou du savoir-faire. Il convient donc de se référer au droit commun, soit le droit de la responsabilité civile et le droit de la concurrence déloyale.

Le fait de s'approprier indûment le savoir-faire d'un autre vendeur constitue un acte contraire aux usages honnêtes en matière commerciale susceptible d'être interdit conformément à l'article 93 LPC<sup>76</sup>.

L'appropriation, éventuellement combinée à une diffusion, des secrets afférents à une technologie de protection des œuvres en vue de la mise au point d'un mécanisme de contournement ou de neutralisation pourrait donc, le cas échéant, être sanctionnée sur base du droit de la concurrence déloyale ou du droit de la responsabilité civile.

## **8. Autres protections**

En vertu du principe de l'autonomie de la volonté, il est tout à fait envisageable que la neutralisation d'un dispositif technique soit prohibée par l'insertion de clauses appropriées dans un contrat. La pratique semble fréquente dans le cadre de contrats de licence d'œuvres protégées par le droit d'auteur. La validité des clauses contractuelles concernées dépendra cependant de leur portée. Ainsi, des clauses qui interdiraient le contournement du dispositif technique en dépit de l'existence d'exceptions impératives aux droits d'auteur pourraient être contestées par le titulaire d'une licence d'utilisation qui souhaiterait exercer l'une des exceptions offertes par la loi. Tel pourrait être le cas si un accord de licence d'utilisation d'un logiciel interdisait le contournement des

---

<sup>72</sup> M. BUYDENS, op. cit., n°376.

<sup>73</sup> L'article 28 LBI dispose en effet que les droits conférés par le brevet ne s'étendent pas « aux actes accomplis dans un cadre privé et à des fins non commerciales ».

<sup>74</sup> L'article 28 LBI exclut également du champ des droits exclusifs « les actes accomplis à titre expérimental ». Il n'est pas totalement exclu que certains actes de *hacking* puissent bénéficier de cette exception. Mais il convient de rappeler que cette disposition doit être interprétée de manière restrictive, car il s'agit d'une exception aux droits exclusifs découlant du brevet.

<sup>75</sup> Sur la portée de cette disposition, lire notamment VAN MENSEL, « De bescherming van fabrieksgeheimen of technische know-how naar Belgisch recht », *Rechtskundig Weekblad*, 1981-1982, 2001 et ss.

<sup>76</sup> En ce sens, M. BUYDENS, op. cit., n°560.

dispositifs techniques même dans l'hypothèse d'actes de décompilation du logiciel sous licence<sup>77</sup>. L'article 7 LPO, qui permet d'accomplir certains actes relevant en principe des prérogatives exclusives de l'auteur en vue de décompiler un logiciel, est en effet impératif (art. 8 LPO) et ne peut dès lors être écarté par une clause contractuelle<sup>78</sup>. La clause évoquée ici pourrait dès lors être déclarée nulle dans la mesure où elle a pour effet d'écartier indirectement l'application d'une règle impérative.

Il convient en outre de relativiser la portée de ce mécanisme de protection dans la mesure où bien souvent l'auteur des actes de neutralisation du dispositif technique ne sera pas en relation contractuelle avec l'utilisateur du dispositif technique de protection, ce qui rendra évidemment les éventuelles clauses contractuelles inopérantes.

Alexandre CRUQUENAIRE  
Chercheur au Centre de  
Recherches Informatique  
et Droit, Université de Namur  
[alexandre.cruquenaire@fundp.ac.be](mailto:alexandre.cruquenaire@fundp.ac.be)

Pierre-Yves POTELLE  
Chercheur au Centre de  
Recherches Informatique  
et Droit, Université de Namur  
[pierre-yves.potelle@fundp.ac.be](mailto:pierre-yves.potelle@fundp.ac.be)

---

<sup>77</sup> Y compris dans les limites de l'exception légale.

<sup>78</sup> F. DE VISSCHER et B. MICHAUX, op. cit., n° 265 et 114.