

## LA FRAUDE INFORMATIQUE EN DROIT LUXEMBOURGEOIS<sup>1</sup>

Stephan LE GOUEFF<sup>2</sup>

La généralisation de l'outil informatique a entraîné ces dernières années l'émergence d'une criminalité bien spécifique de nature à inquiéter les pouvoirs publics, les entreprises et les institutions financières du Grand-Duché.

Il s'agit de l'intrusion frauduleuse dans les systèmes informatiques.

En effet, les hackers de la première génération (ceux qui déjouent les systèmes et déambulent dans les programmes en laissant leur signature comme un tag à la gloire de la cyberculture), cohabitent désormais avec les crackers (ou pirates), à but lucratif ou destructeur. Ces derniers forment une délinquance informatique dont les conséquences financières sont autrement plus inquiétantes.

La fraude informatique n'est pas seulement le fait de quelque passionné pas toujours conscient de la gravité de ses actes, elle est aussi le fait de groupements criminels organisés, s'attaquant aux systèmes informatiques d'institutions bancaires, allant jusqu'à leur extorquer d'importantes sommes d'argent contre une "assistance technique" plus ou moins durable.

L'intrusion frauduleuse est ainsi devenue au fil des années un véritable fléau économique, dans la mesure où de plus en plus de fraudeurs s'introduisent dans les réseaux d'entreprises ou de banques, pour y voler des informations, détruire des données sensibles, ou encore pour y procéder à des détournements de fonds.

Au Luxembourg, il faut le souligner, le montant des sinistres dû à ce type de malveillance est inconnu car il n'existe aucune statistique officielle à ce sujet.

Il est donc difficile de se faire une idée précise de l'ampleur de ce phénomène, et ce d'autant plus que l'on peut concevoir que la plupart des acteurs économiques luxembourgeois, dans un souci d'éviter toute publicité négative, hésiteraient de communiquer sur ce thème.

Cela est particulièrement vrai pour les établissements financiers de la place qui traitent des sommes importantes via leurs réseaux informatiques et qui par conséquent, pour ne pas prendre le risque de perdre de clients, ne voudront pas apparaître comme sous-sécurisés.

Une étude annuelle datant de 2006, aux Etats-Unis, du *Computer Security Institute*<sup>3</sup>, en partenariat avec le FBI, affirme que la cybercriminalité serait devenue la première cause des pertes financières des entreprises américaines : en effet, 75% des pertes serait dues à la criminalité informatique, chiffre à cependant prendre avec prudence, car seulement 25% des entreprises révéleraient avoir été victimes de fraude informatique.

---

<sup>1</sup> A jour au 1<sup>er</sup> avril 2007

<sup>2</sup> Avec la collaboration de Hervé Wolff. Stéphane Le Goueff est avocat à la Cour au cabinet LG@vocats. Il est également le rédacteur en chef de "the l.i.n.k.", une lettre d'information électronique traitant des sujets juridiques liés à la société de l'information disponible sur le site [link@the-link.lu](http://link@the-link.lu).

<sup>3</sup> <http://www.gocsi.com> et <http://www.silicon.fr/>

Aussi, ayant pris la mesure du problème, le législateur luxembourgeois a été amené ces dernières années à intervenir à plusieurs reprises<sup>4</sup>, afin de mettre en place un dispositif répressif destiné à lutter efficacement contre cette nouvelle forme de criminalité.

D'autres pays tels que la France et la Belgique se sont dotés d'outils répressifs spécifiques. Le besoin d'harmonisation des législations pousse aujourd'hui les institutions européennes à intervenir. La convention sur la cybercriminalité du Conseil de l'Europe adoptée le 23 novembre 2001 tend à encourager cette harmonisation des législations et à faciliter la coopération internationale. Le conseil de l'Union européenne quant à lui a adopté le 24 février 2005 une décision cadre relative aux attaques visant les systèmes d'information, dans le but de rapprocher les législations européennes et le cas échéant, de permettre à certains Etats de compléter leurs dispositions internes.

Il paraît ainsi opportun de passer en revue l'actuelle législation luxembourgeoise ayant vocation à réprimer les actes d'intrusion dans les systèmes informatiques afin d'en apprécier la qualité.

Au Luxembourg, la répression des délits d'intrusion s'organise essentiellement autour de trois thèmes :

- l'accès ou le maintien dans un système informatique ;
- l'entrave au fonctionnement d'un tel système ; et
- l'introduction, la suppression ou la modification de données.

Auxquels s'ajoutent des qualifications pénales traditionnelles, telles que par exemple la fabrication de fausses clefs ou encore le recel.

L'objet de cet article est de présenter le dispositif pénal existant.

A cet égard, la question de la responsabilité pénale sera abordée sous deux éclairages :

- les infractions aux systèmes informatiques (1) ; et
- les autres infractions (2).

Il conviendra dans un troisième temps, d'apprécier ce cadre législatif interne au regard des lignes directrices fixées par les normes internationales (3).

## **1. Les infractions aux systèmes informatiques**

Les articles 509-1 et suivants du Code Pénal luxembourgeois (« CP »), qui traitent de la fraude informatique, ont été introduits par la loi du 15 juillet 1993 et ont été modifiés par la loi du 14 août 2000. La loi du 10 novembre 2006 quant à elle, introduit un nouvel article 509-4 dans le code pénal, qui instaure des circonstances aggravantes aux infractions relatives à la fraude informatique. Ils sont directement inspirés de la loi française « Godfrain »<sup>5</sup> et ont pour but de réprimer un certain nombre d'infractions en matière informatique.

Bien que l'arsenal répressif soit complet, la répression reste rare que ce soit au Luxembourg, ou même en France où les cas de jurisprudence sont peu nombreux. La parenté des législations luxembourgeoise et française nous permettra cependant de tirer quelques enseignements de la jurisprudence française dans ce domaine.

En relation avec ces infractions, nous aborderons successivement :

---

<sup>4</sup> Loi du 15 juillet 1993, Mém. A. 1993, p. 1152, et Loi du 14 août 2000, Mém. A. 2000, p. 2176.

<sup>5</sup> Loi n°88-19 du 5 janvier 1988 insérant les articles 462-2 et suivants dans le Code pénal français. Ces textes se retrouvent aujourd'hui aux articles 323-1 et suivants du nouveau Code pénal français entrée en vigueur le 1<sup>er</sup> mars 1994.

- l'élément matériel de chacune de ces infractions (1.1) ;
- l'élément intentionnel (1.2) ; et
- les personnes responsables (1.3).

### **1.1 L'élément matériel**

L'élément matériel sera traité en relation avec les infractions des articles 509-1 et suivants CP :

- art. 509-1 CP : l'accès ou le maintien dans un système informatique (1.1.1) ;
- art. 509-2 CP : l'entrave au fonctionnement d'un tel système (1.1.2) ;
- art. 509-3 CP : l'introduction, la suppression ou la modification de données (1.1.3) ;
- art. 509-6 CP : la tentative et la complicité (1.1.4) ;
- art. 509-7 CP : l'association de malfaiteurs économiques
- art. 509-4 CP : le détournement d'argent

#### **1.1.1 L'accès à un système informatique**

L'article 509-1 CP, tel que modifié par la loi du 14 août 2000 relative au commerce électronique, dispose que :

*« Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines.*

*Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1250 euros à 25.000 euros ».*

Cet article établit deux infractions :

- l'accès ou le maintien frauduleux dans un système (1.1.1.1) ; et
- l'atteinte aux données ou au système qui peut en résulter (1.1.1.2).

Il convient au préalable de définir la notion de système de traitement automatisé de données. La loi n'a pas souhaité dicter une définition. La décision-cadre du 24 février 2005 relative aux attaques visant les systèmes d'information définit le « système d'information » comme étant « tout dispositif isolé ou groupe de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, conformément à un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ces derniers en vue de leur fonctionnement, utilisation, protection et maintenance », autrement dit, il s'agit d'un système de traitement automatisé de données... Il faut donc au moins un ordinateur capable de recevoir, stocker et transmettre des données<sup>6</sup>. En ce sens, peuvent constituer des systèmes de traitement automatisé de données, tout ordinateur, qu'il soit connecté ou non à un réseau.

##### **1.1.1.1. L'accès ou le maintien**

---

<sup>6</sup> La Convention du Conseil de l'Europe sur la cybercriminalité parle de « système informatique » au lieu de système d'information.

Le législateur a voulu par cet article 509-1 CP sanctionner l'accès et le maintien frauduleux dans un système, ou dans une partie de système, indépendamment du fait que cet accès ou ce maintien n'est que la première phase d'une fraude plus grave ou qu'il ne cause aucun préjudice. C'est donc une infraction dite formelle, car elle n'exige aucun résultat dommageable subi par la victime de l'intrusion<sup>7</sup>.

De plus, la formulation employée est générale et n'est pas liée à l'emploi d'une technique d'intrusion particulière. En recourant à une telle formulation, le législateur a voulu couvrir toutes les techniques d'accès.

Ainsi, les techniques suivantes sont toutes mentionnées dans l'Avis du Conseil d'Etat relatif à la loi du 15 juillet 1993<sup>8</sup>:

- « cheval de Troie » encore appelé « sniffing » (insertion d'un programme espion enregistrant les codes d'accès des abonnés) ;
- « raccourci » (utilisation des faiblesses du contrôle interne) ;
- acte « asynchrone » (utilisation des faiblesses du système d'exploitation) ;
- « déplombage » (élimination des instructions de contrôle) ;
- « déguisement » (le fait de se faire passer pour une personne autorisée), autrement appelé « spoofing » et consistant à usurper l'identité d'une personne en utilisant son code d'accès ;
- « poubelle » (découverte de codes d'accès dans des documents mis au rebut).

L'article ne distingue pas selon que l'accès se fait à partir d'une machine appartenant au système ou plutôt à distance à partir d'un branchement par un réseau externe. Toutefois, le passage qui précède montre que tant l'accès interne qu'externe sont couverts. Ainsi, l'intrusion peut être le fait d'un employé de la société victime<sup>9</sup>, comme d'une personne extérieure à celle-ci<sup>10</sup>.

En sanctionnant séparément le « maintien » dans un système informatique, le texte punit celui qui se maintient dans un système qu'il a pénétré, soit par inadvertance, soit légalement, par exemple en restant dans le système pour une durée supérieure à celle autorisée. Cependant, le délit suppose que soit rapporté le forçage d'un dispositif de sécurité<sup>11</sup>.

En définitive, la loi réprime de façon extrêmement large tous types d'intrusions, dans tous types de systèmes informatiques, quel que soit le résultat.

### 1.1.1.2 Atteinte aux données ou au système

---

<sup>7</sup> Voir TGI de Vannes, 13 juillet 2005, JurisData n°2005-294765. Le juge relève que l'infraction d'accès frauduleux à un système de traitement automatisé de données est constituée dès lors qu'une personne non habilitée pénètre dans ce système tout en sachant être dépourvue d'autorisation, peu importe le mobile.

<sup>8</sup> Avis du Conseil d'Etat, 16.10.90, n° 3493, Chambre des Députés, Projet de loi tendant à renforcer la criminalité économique et la fraude informatique, p. 9, p. 16.

<sup>9</sup> L'agent France Télécom qui utilise à des fins personnelles et à l'insu de sa hiérarchie un terminal minitel raccordé clandestinement à une ligne téléphonique et occasionnant de ce fait un préjudice à sa société, se rend coupable du délit d'intrusion. CA Aix-en-Provence 23 octobre 1996, Gaz. Pal. 20-22 juillet 1997 p. 34. Précisons que ces faits ne sont pas constitutifs d'un vol, faute de matérialité de la « chose » soustraite.

<sup>10</sup> L'informaticien licencié qui conserve le code d'accès au système informatique de son ancien employeur et l'utilise pour s'introduire dans ledit système se rend coupable du délit. CA Toulouse 21 janvier 1999, Juris-Data n°040054.

<sup>11</sup> Voir CA Paris, 30 octobre 2002. Il a été jugé qu'il n'y avait pas accès frauduleux dès lors que celui-ci est réalisé par la simple utilisation d'un logiciel grand public avec ajout d'un plug-in

Le 2<sup>ème</sup> alinéa de l'article 509-1 modifié du CP sanctionne le résultat de l'intrusion dans un système informatique. Il s'agit d'une circonstance aggravante de l'infraction précédemment étudiée à l'alinéa 1<sup>er</sup>.

Une peine aggravée est encourue lorsqu'il résulte de l'accès ou du maintien frauduleux dans un système informatique :

- soit la suppression ou la modification de données contenues dans le système ;
- soit une altération du fonctionnement du système.

On vise donc deux types d'atteintes. D'une part, une atteinte aux données (la suppression ou la modification de données<sup>12</sup>), et d'autre part, une atteinte au fonctionnement du système, par l'envoi, par exemple, d'une grande quantité de messages électroniques sans contenu, ou de lourds fichiers, à destination d'un site Internet ayant pour effet d'encombrer la bande passante<sup>13</sup>.

### 1.1.2 L'entrave

L'article 509-2 modifié du CP dispose que :

*« Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines ».*

Ces dispositions visent à incriminer le fait de fausser ou d'entraver le fonctionnement du système informatique qu'il y ait ou non accès au système informatique de la victime. Selon le Conseil d'Etat, l'insertion de « cheval de Troie », de « bombes logiques » ou de « vices informatiques » sont notamment couverts.

Compte tenu de la formulation générale employée, il nous semble que tout type d'entrave au fonctionnement d'un système informatique est visé (y compris les virus informatiques).

Si ces dispositions complètent celles de l'article 509-1 al. 2, elles sont toutefois plus restrictives. L'article 509-1 al. 2 sanctionne en effet une altération du fonctionnement du système (qu'elle soit majeure/mineure, positive/négative/neutre), sous réserve qu'elle résulte d'un accès ou du maintien frauduleux dans un système informatique. Par contre, pour que l'infraction de l'article 509-2 CP soit constituée, il faut que le fonctionnement du système soit faussé ou entravé, c'est-à-dire qu'il soit affecté de manière préjudiciable. Ce dommage peut consister en un ralentissement du système<sup>14</sup>, en l'accessibilité réduite du système<sup>15</sup>, ou encore en la perte de données<sup>16</sup>.

Il convient à cet égard d'attirer l'attention sur l'hypothèse suivante : la victime télécharge sur son système informatique un virus « mis à disposition » sur un réseau. La personne qui a mis à

---

<sup>12</sup> CA Toulouse 21 janvier 1999, Juris-Data n°040054. Condamnation d'un employé licencié qui utilise son code d'accès pour s'introduire dans le système informatique de son ancienne entreprise et y détruire des fichiers.

<sup>13</sup> Tribunal correctionnel de Paris, 24 mai 2002 : le spammeur qui par logiciel avait bloqué les serveurs de Noos en envoyant des centaines de milliers de messages a été condamné à un mois de prison avec sursis.

<sup>14</sup> CA Paris 5 avril 1994, Juris-Data n°21053. Egalement CA Paris 14 janvier 1997, Juris-Data n°020128. Dans ces deux affaires, il y a entrave du système informatique dans le fait de programmer l'envoi d'un grand nombre de messages et de simuler de multiples connexions sur le serveur victime, avec pour effet le ralentissement de sa capacité de traitement.

<sup>15</sup> CA Paris 5 octobre 1994, Juris-Data n°023667. L'entrave résultait de la modification des codes d'accès au système par un informaticien et son refus de les divulguer.

<sup>16</sup> CA Paris, 17 janvier 2000, Juris-Data n°109747. L'entrave résultait de l'introduction d'un virus dans le système qui avait provoqué la modification et la suppression de certaines données.

disposition ce virus est-elle coupable du délit de l'article 509-2 CP ? On pourrait estimer que celui qui met à disposition ce virus n'est pas l'auteur d'une intrusion. En ce sens, il n'est punissable ni sur le fondement de l'article 509-1 CP, ni sur celui de l'article 509-2 CP. Toutefois, il nous semble que cette mise à disposition n'est qu'un moyen de commettre l'infraction, à savoir fausser ou entraver un système informatique. Ce mode opératoire est un acte positif (le fait de mettre le virus sur le réseau) et l'identité de la victime importe peu (la loi n'exige pas que le pirate vise un système identifié de manière précise). Dès lors qu'il est constaté que ce virus est à l'origine du dommage subi par la victime (et même si celle-ci a fait preuve d'imprudence en ne vérifiant pas l'origine du programme qu'elle télécharge), l'auteur de cette mise à disposition est coupable sur le fondement de l'article 509-2 CP. Il est intéressant de noter sur ce point que la France s'est dotée, dans la loi pour la confiance dans l'économie numérique du 21 juin 2004, d'une incrimination spécifique qui sanctionne « le fait, sans motif légitime, d'importer, 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 une ou plusieurs des infractions prévues » ; sont ainsi directement visés les créateurs de virus.

Toutefois, l'intérêt de l'article 509-2 est remis en cause, car concurrencé par l'article 509-3 CP, qui réprime des mêmes peines celui qui, indirectement, modifie ou supprime les données d'un système.

### **1.1.3 L'introduction ou la suppression de données**

L'art. 509-3 modifié du CP dispose que :

*« Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé de données ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines ».*

Cet article, recoupe l'article 509-1 al. 2 CP et complète le précédent.

En effet, l'article 509-1 al. 2 sanctionne toute « *modification de données contenues dans le système* » qui résulte d'un accès ou maintien frauduleux dans un système informatique. L'article 509-3 CP sanctionne, outre la modification des données, l'introduction ou la suppression des données, qu'il y ait ou non accès ou maintien dans le système.

De plus, cet article 509-2 CP tel qu'il est interprété par les juridictions françaises, fait double emploi avec l'article 509-3 CP en ce que tous deux répriment (des mêmes peines) le fait de modifier ou de supprimer les données d'un système.

Les dispositions de l'article 509-3 CP ont cependant pour avantage d'élargir les filets de la répression en punissant sans équivoque celui qui modifie ou supprime des données à la suite de la propagation d'un virus sur le réseau. Ainsi, quel que soit le mode d'inoculation du virus (envoi par le pirate ou téléchargement par la victime), la répression est encourue.

### **1.1.4 La tentative**

L'article 509-6 CP dispose que:

*« La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui même ».*

Précisons tout de suite que l'article 509-5 a été abrogé par la loi du 14 août 2000.

Cet article 509-6 CP permet de sanctionner les actes perpétrés pendant la phase d'approche et de contact avant même que l'intrusion ne soit réalisée. Il serait en effet absurde d'assurer l'impunité à celui qui a échoué face à la sécurité informatique mise en place par ces établissements.

Ainsi, que les actes des fraudeurs soient constitutifs de simples actes préparatoires (détention de programmes utiles à l'intrusion par exemple) ou d'un commencement d'exécution (utilisation du programme utile à l'intrusion), le droit pénal luxembourgeois connaît une solution répressive.

Ajoutons enfin que la complicité est punissable sur le fondement des articles 67 et s. CP. Ainsi, celui qui fournit le matériel permettant d'accéder frauduleusement à un système de traitement automatisé de données est punissable dès lors qu'il agit en connaissance de cause. Ainsi, le fait de prêter un téléphone ou un modem peut suffire<sup>17</sup>.

### **1.1.5 L'association de malfaiteurs informatiques**

Il convient d'évoquer l'article 509-7 CP réprimant « *quiconque aura participé à une association ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues aux articles 509-1 à 509-5* ».

Cet article permet ainsi de réprimer les associations de malfaiteurs, dès leurs premiers efforts accomplis en vue de l'intrusion. Elle permet également d'élargir la répression à tous les participants au groupement, quels que soient leurs actes, et même si l'infraction est déjà consommée. Ainsi, il a été jugé que constituait une association de malfaiteurs informatiques, le fait pour des commis de change d'avoir détourné des fonds, tandis que d'autres fournissaient des informations sur les comptes à détourner et en permettaient l'utilisation<sup>18</sup>. Ces personnes ont également été punies pour abus de confiance et falsification.

### **1.1.6 Le détournement d'argent**

Le nouvel article 509-4 al1 CP, introduit par la loi du 10 novembre 2006, prévoit que :

*« Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1.250 euros à 30.000 euros. »*

Le législateur, avec cet article, souhaite réprimer plus durement les infractions informatiques s'accompagnant ou ayant pour but un détournement d'argent.

L'article 509-4 al 2 ajoute que : « *encourront les mêmes peines, ceux qui auront fabriqué, reçu, obtenu, détenu, vendu ou cédé à un tiers des logiciels ayant pour objet de rendre possible une infraction visée à l'alinéa qui précède* ». Le champ répressif est donc élargi et permet d'appréhender les créateurs de logiciels, mais seulement en rapport avec l'alinéa 1<sup>er</sup>. Il aurait

---

<sup>17</sup> TGI Paris 16 décembre 1997, Lamyline. Complicité d'accès frauduleux à un système de traitement automatisé de données par la mise à disposition d'un téléphone à l'auteur principal en toute connaissance de cause.

<sup>18</sup> CA Paris, 22 mai 1989, RTDCom 1990, p. 73, obs. M. Cabrillac et B. Teyssié.

été plus judicieux de viser l'ensemble des infractions informatiques, afin de tenir compte de tous les types de logiciels malveillants<sup>19</sup>.

\*\*\*

L'arsenal répressif luxembourgeois en matière de lutte contre la fraude informatique semble complet. Infraction obstacle ou matérielle, tentée ou consommée, tous les stades du cheminement criminel sont couverts par la répression. Il appartient alors au juge de vérifier que l'intrus a agi intentionnellement. De plus, il n'est pas toujours aisé de déterminer la personne pénalement responsable.

## **1.2 L'élément moral**

### **1.2.1 La règle générale**

En droit pénal, l'élément moral consiste dans l'intention d'enfreindre la loi pénale. Plus précisément, l'auteur doit agir volontairement et avec conscience, c'est-à-dire en toute connaissance de cause.

La loi peut requérir expressément cet élément moral en employant des termes comme : « sciemment », « à dessein », « intentionnellement », etc. Ces expressions sont toutefois surabondantes, car elles n'ajoutent rien à la notion de dol général.

Si le législateur exige en outre un mobile spécial qui consiste dans une intention de nuire ou frauduleuse, il emploie les termes « méchamment, frauduleusement, à dessein de nuire » etc<sup>20</sup>.

### **1.2.2 L'application aux articles 509-1 et s.**

Pour l'article 509-1 le législateur a inséré l'expression « frauduleusement ». Ainsi, pour que cette infraction soit constituée, il faut, outre l'intention générale d'enfreindre la loi pénale en accédant ou en se maintenant dans un système informatique sans autorisation, un mobile spécifique, en l'occurrence une intrusion dans un but frauduleux. Ainsi, celui qui accède à un système de manière non intentionnelle (c'est-à-dire accidentelle) n'est pas punissable. Il le devient s'il s'y maintient en toute connaissance de cause, le but frauduleux se confondant avec le fait de se maintenir volontairement dans le système<sup>21</sup>. Ainsi, il en résulte que l'intention découle largement des faits. Celui qui se promène dans un système informatique sans autorisation est en quelque sorte présumé être animé d'un but frauduleux<sup>22</sup>. Il est en effet difficilement concevable qu'une personne puisse de façon involontaire déjouer la sécurité d'un système informatique, le préalable étant que la personne doit avoir conscience de s'être introduit dans le système informatique.

L'expression « intentionnellement et au mépris des droits d'autrui » que l'on retrouve aux articles 509-2 et 509-3 CP ne fait en revanche pas ressortir de mobile spécial, mais la nécessité d'avoir un élément intentionnel général (volonté et conscience) d'enfreindre la loi pénale pour que l'infraction soit constituée. En revanche, il résulte de la rédaction de ces deux textes, que l'intention porte sur l'intégralité de l'élément matériel, non seulement le comportement, mais aussi le résultat de ce comportement. Or, nous avons vu précédemment

---

<sup>19</sup> C'est ce qu'a fait au demeurant la France comme vu précédemment (point 1.1.2)

<sup>20</sup> Trib. arr. Lux. 10-04-84, n° 724/84 VII.

<sup>21</sup> Voir en ce sens, CA Paris 5 avril 1994, Juris-Data n°21093 ; CA Paris 14 janvier 1997, Juris-Data n°020128.

<sup>22</sup> Toutefois, le doute doit toujours profiter au prévenu. Si une imprudence peut expliquer le comportement de l'agent, en l'absence de preuve non équivoque de son intention, il doit être relaxé (CA Paris 15 mars 1995, Juris-Data n°020627).

que les articles 509-2 et 509-3 CP exigeaient un certain résultat (la modification ou la suppression de données entre autres). L'intention doit donc porter également sur ce résultat.

Ainsi, les articles 509-1 alinéa 2 et 509-2 sont fondamentalement distincts, en ce que le dommage résultant de l'intrusion visée par le premier article est en principe non intentionnelle, tandis que si le pirate a pour but de créer ce dommage, c'est alors la qualification visée à l'article 509-2 CP qu'il convient de retenir.

### 1.3 Les personnes responsables

Les intrusions peuvent être soit le fait d'individus dont les mobiles peuvent passer du défi à une réelle intention de nuire, soit le fait d'entreprises qui cherchent par ce biais à s'approprier des informations appartenant à des concurrents ou qui cherchent encore à saboter leurs systèmes informatiques.

La recherche de la personne responsable, lorsqu'il s'agit d'un individu, ne pose guère de difficultés. En effet, les articles 509-1 s. CP répriment « quiconque » aura accompli l'un ou l'autre des actes incriminés. En ce sens, il est permis d'affirmer que le Code pénal est un code individualiste. Le fait de participer à une association de malfaiteurs informatiques (art. 509-7 CP) est d'ailleurs réprimé de la même manière, alors qu'il s'agit d'une infraction collective.

En revanche, lorsque l'intrusion est le fait d'une entreprise, personne morale, la question qui se pose alors est celle de savoir quelles sont les personnes dont la responsabilité doit être recherchée.

A cet égard, il faut souligner que le droit pénal luxembourgeois n'accepte pas, pour l'heure, la responsabilité pénale des personnes morales. Cependant, cette situation devrait changer d'ici peu ; en effet un projet de loi introduisant la responsabilité pénale des personnes morales a été adopté par le conseil de gouvernement le 30 mars 2007<sup>23</sup>

Jusqu'à présent, lorsqu'une personne morale est impliquée dans une infraction, on recherche la ou les personne(s) physique(s), organe(s) ou préposé(s), à l'intérieur de la personne morale, qui, par commission ou omission, est la cause de l'infraction<sup>24</sup>. L'entreprise n'est jamais qu'une somme de personnes physiques.

Le chef d'entreprise répond pénalement des infractions qui se commettent dans l'entreprise en raison de l'autorité qu'il exerce sur les hommes et sur les choses ainsi rassemblées qui constituent son industrie<sup>25</sup>. C'est ce pouvoir qui est à la source des responsabilités encourues, le salarié étant prisonnier d'une structure sur laquelle il n'a guère de prise<sup>26</sup>.

Le chef d'entreprise peut s'exonérer de la responsabilité résultant des actes commis par ses préposés sous condition de démontrer qu'il avait délégué à un subordonné la direction et la surveillance des services dans lesquels l'acte délictueux a été commis. Il reste néanmoins responsable de sa propre faute. Un certain laisser aller dans l'organisation de l'exploitation qui

---

<sup>23</sup> Source : [www.gouvernement.lu](http://www.gouvernement.lu). Le projet de loi abandonne le principe traditionnel de l'irresponsabilité des personnes morales et vise à introduire en droit luxembourgeois un régime de responsabilité pénale des personnes morales. Par l'introduction de ce régime, une personne morale engage sa responsabilité pénale lorsqu'un crime ou un délit est commis en son nom et dans son intérêt par un de ses organes légaux ou par un ou plusieurs des membres de ses organes légaux. L'introduction de ce régime de responsabilité pénale dans le code pénal luxembourgeois s'explique par les obligations internationales auxquelles le Grand-Duché de Luxembourg a souscrit, que ce soit au niveau de l'Union européenne ou encore dans le cadre d'autres organisations internationales (OCDE, Conseil de l'Europe, ONU).

<sup>24</sup> Trib. arr. Lux 16.6.86, n° 974/86 ; Trib. arr. Lux 12.5.87, n° 896/87 ; Trib. Arr. Lux. 16.5.95, n°1027/95 confirmé par CA 6.5.96, n°198/96.

<sup>25</sup> CA 9.7.87, n°247/87. Le gérant d'une SARL est responsable pénalement des dysfonctionnements de son entreprise.

<sup>26</sup> Trib. arr. Lux 13.7.81, n° 1265/84 ; Trib. arr. Lux 23.2.87, n° 371/87.

a favorisé l'oubli de la sécurité, et par là même un accident, a été retenu comme une faute du chef d'entreprise<sup>27</sup>.

Pour qu'il y ait exonération de responsabilité, le chef d'entreprise doit apporter la preuve que les conditions suivantes sont remplies<sup>28</sup> :

- le transfert de l'autorité exprès et public par le chef d'entreprise ;
- la qualification et la compétence de la personne déléguée ; et
- la transmission effective des pouvoirs avec la prérogative de décision.

En conséquence, en principe, ce sont les dirigeants qui seraient pénalement responsables des actes commis par les employés dans l'exercice de leurs fonctions. La responsabilité pénale des dirigeants pourrait être engagée même par une violation des dispositions précitées du CP attribuable à un préposé auquel une délégation de pouvoir serait confiée, dans la mesure où cela résulterait d'une organisation défailante de l'exploitation d'un service sensible.

Il ne pourrait y avoir exonération que s'il y avait une délégation d'autorité à un préposé remplissant les conditions ci-dessus visées ou un acte illégal commis par un préposé à l'extérieur de ses fonctions. Ainsi, le chef d'entreprise ne serait pas responsable dans l'hypothèse où un employé violerait les dispositions du CP relatives à la fraude informatique en utilisant le système informatique de l'entreprise à l'insu de la direction de l'entreprise mais seulement à la condition que l'employé agisse dans un but étranger à sa fonction.

## **2 Les autres infractions**

Outre la fraude informatique, les intrusions peuvent notamment entraîner des infractions :

- économiques (2.1) ;
- relatives aux données et informations (2.2) ; et
- autres (2.3).

### **2.1 Les infractions économiques**

Les infractions économiques potentielles sont :

- la divulgation de secret de fabrique (2.1.1) ; et
- l'espionnage industriel (2.1.2) ;

Ces deux infractions sont indépendantes des infractions aux systèmes informatiques ; leur commission peut simplement être facilitée par l'emploi des technologies liées à l'informatique.

#### **2.1.1 La divulgation de secret de fabrique**

L'article 309 CP dispose que :

*« Celui qui, étant ou ayant été employé, ouvrier ou apprenti d'une entreprise commerciale, ou industrielle, soit dans un but de concurrence, soit dans l'intention de nuire à son patron, soit pour se procurer un avantage illicite, utilise ou divulgue, pendant la durée de son engagement ou endéans les deux ans qui en suivent l'expiration, les secrets d'affaires ou de fabrication dont il a eu connaissance par suite de sa situation, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 251 euros à 12.500 euros (...) ».*

---

<sup>27</sup> Cour d'appel 25.11.86, n° 290/86 V ; Trib. arr. Lux 18.3.87, n° 489/87.

<sup>28</sup> Trib. arr. Lux. 1.6.87, n° 1073/87.

*« Il en est de même de celui qui, ayant eu connaissance de secrets d'affaires ou de fabrication appartenant à une personne, soit par l'intermédiaire d'un employé, ouvrier ou apprenti agissant en violation des prescriptions de l'alinéa qui précède, soit par un acte contraire à la loi ou aux bonnes moeurs, utilise ces secrets ou les divulgue, soit dans un but de concurrence, soit dans l'intention de nuire à celui à qui ils appartiennent, soit pour se procurer un avantage illicite. (...) »*

Les dispositions du premier paragraphe pourraient s'appliquer au cas où, dans le cadre d'une d'intrusion, un employé accéderait à un secret d'affaires ou de fabrication de sa propre entreprise ou d'une entreprise tierce dans laquelle il effectue une mission quelconque. Mais l'intrusion ne suffit pas à constituer l'infraction visée à l'article 309. Encore faut-il que l'intrus utilise ou divulgue le secret.

Il faudra que l'employé ait eu connaissance du secret d'affaires ou de fabrication divulgué « par suite de sa situation ». Néanmoins, un élément intentionnel spécial est requis. En outre, il doit y avoir soit une intention de nuire à l'employeur, soit l'intention de se procurer un avantage illicite<sup>29</sup> (comme par exemple le paiement d'une somme d'argent).

Le second paragraphe pourrait s'appliquer à une divulgation ou à une utilisation d'informations confidentielles portant sur un secret d'affaires ou de fabrication obtenues par l'agent dans le cadre d'une opération d'intrusion. Le même élément intentionnel est requis.

### **2.1.2 L'espionnage industriel**

Si toutefois l'activité d'intrusion est perpétrée pour le compte d'un Etat étranger, les dispositions de l'art. 118 CP sur l'espionnage industriel peuvent trouver à s'appliquer.

L'article 118, al. 1 CP dispose que :

*« Quiconque aura sciemment livré ou communiqué, en tout ou en partie, en original ou en reproduction, à une puissance étrangère ou à toute autre personne agissant dans l'intérêt d'une puissance étrangère, des objets, plans, écrits, documents ou renseignements dont le secret intéresse la défense du territoire ou la sûreté extérieure de l'Etat, sera puni de réclusion de cinq à dix ans. »*

Les renseignements obtenus par une personne qui se serait introduite dans un système informatique pourraient être couverts par ces dispositions, à condition qu'elle livre ou communique par la suite ces renseignements.

Leur mise en œuvre requiert toutefois :

- un élément intentionnel ;
- que le destinataire des informations soit une puissance étrangère (il n'est pas nécessaire que celle-ci soit une ennemie déclarée du Luxembourg) ;
- que les renseignements communiqués intéressent la défense du territoire ou la sûreté extérieure de l'Etat.

Il est à noter que ces deux dernières incriminations prévues aux articles 309 et 118 du Code pénal constituent des infractions matérielles, en ce sens qu'elles exigent un certain résultat, tel que l'utilisation, la divulgation, la livraison ou la communication d'une information. En revanche, aucune incrimination préventive n'est envisagée. En effet, la lecture des textes ne permet pas

---

<sup>29</sup> Tr. Arr. Lux. 27.4.2000, n°997/2000.

de punir par exemple celui qui stocke sur un support quelconque (un disque dur, un DVD, ...) une information sans pour autant la livrer à autrui. A l'instar du droit français, le droit pénal luxembourgeois ne réprime pas le fait de rendre accessible l'information contenue dans un ordinateur placé en réseau par exemple (quand bien même aucun téléchargement ne serait effectué).

\*\*\*

L'arsenal répressif luxembourgeois compte également divers textes ayant vocation à protéger les données et informations détenues par une entreprise et représentant le plus souvent une valeur considérable. Ces textes sont, pour les uns, d'un intérêt certain, parce que résultant d'une intervention législative récente, pour d'autres, d'une utilité limitée à l'heure actuelle, appelant une adaptation en raison des progrès technologiques.

## **2.2 Les infractions relatives aux données et informations**

Les infractions potentielles concernant les données et informations portent sur :

- les atteintes au secret des correspondances (2.2.1) ;
- le vol d'informations (2.2.2) ;
- le recel d'informations obtenues illégalement (2.2.3) ; et
- le faux en écriture privées électroniques (2.2.4).

### **2.2.1 Les atteintes au secret des correspondances**

Une atteinte à la vie privée pourrait être commise si l'intrusion permettait au fraudeur de prendre connaissance ou de supprimer des messages électroniques à caractère privé, même si ceux-ci devaient se trouver sur le système informatique de l'entreprise.

En effet, l'article 2 de la loi du 11 août 1982 concernant la protection de la vie privée dispose que :

*« Est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 euros à 5.000 euros, ou d'une de ces peines seulement, quiconque a volontairement porté atteinte à l'intimité de la vie privée d'autrui : (...)*

*3° en ouvrant sans l'accord de la personne à laquelle il est adressé ou de celle dont il émane, un message expédié ou transmis sous pli fermé, ou en prenant connaissance, par un appareil quelconque, du contenu d'un tel message ou en supprimant un tel message (...)* ».

L'article 3 ajoute que :

*« Est puni des peines prévues à l'article 2, celui qui a sciemment placé ou fait placer un appareil quelconque dans le but de commettre l'une des infractions prévues par l'article 2 ou d'en rendre possible la perpétration ».*

Le secret des correspondances est également sanctionné par l'article 460 CP :

*« Quiconque sera convaincu d'avoir supprimé une lettre confiée à la poste, ou de l'avoir ouverte pour en violer le secret, sera puni d'un emprisonnement de huit jours à*

*un mois et d'une amende de 251 euros à 2.000 euros, ou d'une de ces peines seulement ».*

En outre, l'article 28 de la Constitution qui dispose que « *Le secret des lettres est inviolable (...)* », témoigne de l'importance accordée au secret des correspondances.

Il est à noter néanmoins le faible intérêt que présente l'article 460 CP en la matière. En effet, d'une part, les peines encourues étant relativement faibles, on lui préférera celles de l'article 2 de la loi de 1982. Ensuite, les juges rejettent l'application de l'article 460 CP dès lors que le message n'est plus confié aux services de la Poste<sup>30</sup>. Il en résulte que la captation matérielle du message est quasiment inopérante pour la répression, car le vol est mieux à même d'assurer la répression. Or, un courrier électronique n'étant pas une chose corporelle, il n'est pas susceptible de vol. C'est donc surtout la violation de la vie privée, et par conséquent, la violation du secret entourant une information, qui sera réprimée. Dès lors, celui qui prend connaissance volontairement d'un message quelconque qui ne lui est pas destiné et par quelque moyen que ce soit, tombe sous le coup de la loi de 1982. Le support du message importe peu.

Par ailleurs l'article 3 de la loi du 11 août 1982 réprime sous forme d'infraction formelle la mise en place de tout dispositif destiné à capter un message. Sorte de tentative d'atteinte à la correspondance érigée en infraction autonome, elle permet une répression anticipée, avant que la violation ne soit effective.

### **2.2.2 Le vol d'informations**

L'article 461 CP qui a trait au vol, réprime « *quiconque a soustrait frauduleusement une chose qui ne lui appartient pas* ».

Au Luxembourg, la jurisprudence admet traditionnellement que seuls les meubles corporels sont susceptibles de vol<sup>31</sup> et que la soustraction doit être entendue comme le fait matériel d'appréhender une chose<sup>32</sup>.

Des évolutions sont toutefois intervenues dans d'autres pays, et en France, certaines juridictions ont reconnu que le vol pouvait porter sur des biens incorporels, dans un premier temps à condition que ces biens incorporels soient liés à un support matériel, et ensuite en reconnaissant que l'information seule pouvait faire l'objet d'un vol<sup>33</sup>.

La jurisprudence luxembourgeoise semble attachée à la définition traditionnelle du vol et estime encore que « *l'objet de la soustraction doit être une chose corporelle ou mobilière* »<sup>34</sup>.

En tout état de cause, la répression exige toujours une dépossession du légitime propriétaire, dans le système luxembourgeois tout du moins<sup>35</sup>.

---

<sup>30</sup> Tr. Arr. Lux. 8.6.88, n°1002/88 ; Tr. Arr. Lux. 13.7.89, n°1057/89 ; Tr. Arr. Lux. 11.11.92, n°1398/92 ; Tr. Arr. Lux. 17.5.93, n°763/93 ;

<sup>31</sup> Cour de cass. 12.7.28, p. 11, 330.

<sup>32</sup> Cour d'appel 26.9.66, p. 20, 239.

<sup>33</sup> Voir sur ce point l'étude de Mohamed Chawki « le vol d'informations: quel cadre juridique aujourd'hui ? », juillet 2006, [www.droit-ntic.com](http://www.droit-ntic.com)

<sup>34</sup> Voir par exemple Tr. Arr. Lux. 4.6.03 n°1438/2003

### 2.2.3 Le recel d'informations obtenues illégalement

Il est envisageable que les informations obtenues lors d'une intrusion soient mises à la disposition de tiers, soit contre rémunération, soit gratuitement. Par exemple, certaines informations obtenues lors de l'intrusion sur un site connu.

Dans l'un ou l'autre de ces cas, les dispositions de l'article 505 modifié du CP sont applicables:

*« Ceux qui auront recelé, en tout ou en partie, les choses ou les biens incorporels enlevés, détournés ou obtenus à l'aide d'un crime ou d'un délit, seront punis d'un emprisonnement de quinze jours à cinq ans et d'une amende de 251 euros à 5.000 euros.*

*Ils pourront, de plus, être condamnés à l'interdiction, conformément à l'article 24.*

*Constitue également un recel le fait de sciemment bénéficier du produit d'un crime ou d'un délit ».*

Le dernier paragraphe devrait pouvoir être utilisé contre une personne qui se serait procurée sur un site de « hackers » les informations obtenues illégalement et permettant de pénétrer le système informatique d'une entreprise.

Il est intéressant de relever ici que, contrairement aux dispositions concernant le vol, le législateur a décidé de modifier le texte sur le recel afin que ce dernier puisse porter sur des biens incorporels, lors de l'adoption de la loi du 14 août 2000 relative au commerce électronique. A ce titre, le concept de « biens incorporels » doit pouvoir englober les informations au sens strict du terme.

Tout bien, qu'il soit corporel ou incorporel, peut donc faire l'objet d'un recel, dès lors qu'il est détenu ou qu'il profite au receleur.

### 2.2.4 Le faux en écritures privées électroniques

Une intrusion peut avoir pour objet ou comme conséquence, la manipulation ou l'altération de documents qui se trouvent dans le système informatique de la victime. Le faux en écriture est sanctionné par l'article 196 CP qui a été modifié, par la loi du 14 août 2000, pour couvrir les écritures électroniques. En conséquence, la falsification d'un document électronique résultant d'une intrusion ou visant à permettre une intrusion entrerait dans le cadre de l'article 196 CP.

Ainsi, les dispositions actuelles de l'article 196 CP prévoient :

*« Seront punies de réclusion de cinq à dix ans les autres personnes qui auront commis (...) un faux en écriture de commerce, de banque ou en écritures privées, en ce compris les actes sous seing privé électronique, soit par fausses signatures, soit par contrefaçon ou altération d'écritures ou de signatures, soit par fabrication de conventions, dispositions, obligations ou décharges, ou par leur insertion après coup dans les actes, soit par addition ou altération de clauses, de déclarations ou de faits que ces actes avaient pour objet de recevoir et de constater ».*

---

<sup>35</sup> Ainsi en a-t-il été jugé en matière d'abus de confiance (qui soulève le même problème que le vol). Tr. Arr. Lux. 27.4.2000, n°997/2000. Le tribunal écarte la qualification d'abus de confiance dans le fait d'avoir détourné des informations contenues dans la mémoire centrale d'un ordinateur, faute de dépossession du propriétaire.

En outre, l'usage d'un faux est réprimé par l'article 197 CP.

Ces dispositions s'inscrivent dans le cadre de l'introduction de la signature électronique au Luxembourg, qui constituait l'un des axes de la loi du 14 août 2000 relative au commerce électronique. Comme cette loi donne à la signature électronique la même valeur probante que la signature manuscrite, sa contrefaçon doit être sanctionnée de manière identique. C'est la raison pour laquelle, le texte apporte la précision que les écrits en cause peuvent également être de nature électronique<sup>36</sup>.

Les éléments constitutifs de cette infraction sont :

- Une intention générale de violer la loi pénale ;
- Un préjudice ou une possibilité d'un préjudice ; et
- La réalisation d'un faux en écriture électronique de commerce ou de banque par un certain nombre de moyens.

Bien que le texte ne le précise pas, il doit y avoir une intention criminelle pour que l'infraction soit constituée. Il n'y a pas de faux lorsque l'altération de la vérité est le résultat d'une erreur ou d'une négligence<sup>37</sup>. L'article 196 CP punit le faux commis, avec une intention frauduleuse ou à dessein de nuire, par addition ou altération de clauses ou de faits que ces actes avaient pour objet de recevoir et de constater<sup>38</sup>.

Toutefois, la jurisprudence a indiqué que pour qu'il puisse y avoir poursuite pour faux en écritures, il faut que l'altération de la vérité cause préjudice ou encore qu'à sa suite il y ait possibilité de préjudice soit matériel, soit moral<sup>39</sup>.

Dans tous les cas, celui qui aura fait usage du faux sera puni comme s'il était l'auteur du faux.

## **2.3 Autres infractions**

On abordera dans cette section :

- l'usage d'un faux nom (2.3.1) ;
- la fabrication de fausses clefs (2.3.2) ; et
- la captation de données personnelles (2.3.3).

### **2.3.1 L'usage d'un faux nom**

L'utilisation d'un faux nom peut survenir, dans le cadre d'une opération d'intrusion, soit « off-line » (par exemple durant une opération de "social engineering"), afin d'obtenir des informations qui rendront possible l'intrusion, soit « on-line », en s'accaparant l'identité numérique (login, identifiant) d'une personne autorisée à accéder au système d'une entreprise.

L'usage d'un faux nom est sanctionné par l'article 231 du CP qui dispose :

---

<sup>36</sup> De sorte que le faux est aujourd'hui réprimé sans aucune considération de la nature de son support. Voir Tr. Arr. Lux. 10.3.99, n°534/99. Les juges estiment que l'article 509-4 CP s'applique à un document informatisé et non écrit. Si bien que l'abrogation de ce texte par la loi du 14 août 2000 et la modification de l'article 196 CP s'analysent en une volonté du législateur de ne plus distinguer suivant la forme du faux.

<sup>37</sup> Trib. arr. Lux. 15.5.85, n° 937/85.

<sup>38</sup> Cour d'appel Lux. 7.5.84, n° 123/84.

<sup>39</sup> Chambre des mises en accusation, 17.5.83, n° 27/83.

*« Quiconque aura publiquement pris un nom qui ne lui appartient pas sera puni d'un emprisonnement de huit jours à trois mois, et d'une amende de 251 euros à 3.000 euros, ou d'une de ces peines seulement. ».*

Il ressort de la jurisprudence que le mobile qui a déterminé une personne à prendre un faux nom est sans importance pour l'existence du délit de port de faux nom, laquelle n'est subordonnée qu'à la seule condition que le port illicite de faux nom en relation avec une infraction informatique ait eu lieu publiquement<sup>40</sup>. Selon les tribunaux, ce qui est important, c'est d'avoir pour but de s'approprier un faux nom vis-à-vis de la généralité des concitoyens<sup>41</sup>.

Comme l'utilisation d'une fausse identité « on-line » ou « off-line » ne remplira pas cette dernière condition, l'article 231 CP ne trouvera pas à s'appliquer.

En outre, a priori, l'utilisation d'un faux nom réprimée par l'article 231 CP pourrait survenir sur Internet. Non pas dans le cadre d'une utilisation « normale » d'Internet, où l'usage veut que le recours aux pseudonymes et avatars est tout à fait banal, mais dans le cadre d'une appropriation d'une adresse IP ou d'une adresse e-mail, ce qui suppose que l'adresse IP ou e-mail soit assimilée au nom.

Il est toutefois peu probable que les juges acceptent cette assimilation, ce d'autant plus que le droit pénal est d'interprétation stricte.

Force est donc de constater que l'article 231 CP ne s'avère pas adapté aux infractions liées à la fraude informatique.

### **2.3.2 La fabrication de fausses clefs**

L'article 488 du CP tel qu'il résulte de la loi du 14 août 2000 dispose que :

*« Quiconque aura frauduleusement contrefait ou altéré des clefs, y compris électroniques sera condamné à un emprisonnement de trois mois à deux ans et à une amende de 251 euros à 2.000 euros ».*

La loi relative au commerce électronique a ici introduit une innovation importante en reconnaissant la notion de clef électronique et en instaurant des sanctions en cas de contrefaçon.

Toutefois, cette loi n'a pas donné de définition de la clef électronique, ce qui pourrait être source d'incertitude. Aussi, la question, à notre connaissance non tranchée par les tribunaux, est celle de savoir notamment si un code d'accès ou un mot de passe peut être considéré comme une clef électronique.

En supposant que la réponse soit positive, une personne qui s'introduirait à l'aide d'une fausse clef dans un système informatique pourrait donc, en tout état de cause, être sanctionnée non seulement sur la base de l'article 509-1, mais également sur la base de l'article 488 du CP. Ce concours idéal de qualifications donnerait lieu à la poursuite de l'acte sous une seule qualification, la plus sévèrement réprimée, c'est-à-dire l'intrusion. Le fait que l'intrusion puisse être commise par l'usage frauduleux d'une clé électronique falsifiée confirme cette solution, l'infraction moyen étant en quelque sorte absorbée par l'infraction fin.

Cette incrimination sanctionne donc un acte préparatoire à l'intrusion informatique, qui s'il n'est pas accompagné d'intrusion, ne pourrait être réprimé sur la base de cette qualification.

---

<sup>40</sup> Cour 4.6.56, p. 16, 488.

<sup>41</sup> Cour 17.2.1894, p. 4, 73.

### 2.3.3 La captation de données personnelles

Les technologies de l'information facilitent le traitement et l'échange de données. Ce progrès s'accompagne logiquement de risques d'abus, tant dans la création de fichiers, que dans l'accès à ces fichiers. C'est pourquoi le Luxembourg a adopté, le 2 août 2002, la loi relative à la protection des personnes à l'égard du traitement des données à caractère personnel, qui remplace la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, devenue obsolète.

La loi définit la notion de donnée personnelle (article 2) comme étant :

*« Toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable ».*

Une personne physique ou morale est réputée identifiable :

*« Si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ».*

La loi énonce les conditions de licéité d'un traitement :

- Au regard de la qualité des données (article 4), le responsable du traitement doit s'assurer que les données qu'il traite le sont loyalement et licitement, et notamment que ces données sont collectées pour des finalités déterminées, explicites et légitimes, adéquates, pertinentes et non excessives au regard de ces finalités, exactes et, si nécessaire, mises à jour;
- Le traitement doit remplir des conditions de légitimité (article 5) ;
- Certaines catégories particulières de données sont soumises à des règles spécifiques, comme par exemple les données sensibles relatives à l'origine raciale ou ethnique (article 6).

De plus, il est à noter qu'un transfert de données vers un pays tiers ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat.

L'article 12 de la loi soumet la mise en oeuvre des traitements à une formalité préalable : sauf exception, les traitements de données font l'objet d'une notification préalable par le responsable du traitement auprès de la Commission nationale pour la protection des données.

Afin de garantir la sécurité des traitements (article 22):

*« Le responsable du traitement doit mettre en oeuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés ».*

La sanction du non respect des obligations de sécurité ou de confidentialité expose le responsable du traitement à une peine d'emprisonnement de huit jours à six mois et à une amende de 251 à 125.000 euros ou à l'une de ces peines seulement.

Enfin, la loi détaille les droits de la personne concernée par le traitement à savoir un droit à l'information, un droit d'accès et un droit d'opposition.

\*\*\*\*

Nous avons étudié l'arsenal répressif dont disposait le droit luxembourgeois pour faire face à la fraude informatique. Mais les mailles du filet de la répression sont-elles suffisamment resserrées pour retenir ce qui n'est finalement que de l'immatériel?<sup>42</sup>

A cette question, nous répondrons que la répression est aujourd'hui nécessaire à l'égard de comportements immatériels dont les conséquences financières, parfois colossales, sont bien réelles. Mais cette répression doit aussi ménager les libertés individuelles, dont l'Internet constitue aujourd'hui l'un des supports.

Le droit pénal luxembourgeois, nous l'avons vu, n'est pas dépourvu face à ces comportements illicites. Il reste toutefois à apprécier la qualité de cet arsenal répressif au regard des normes internationales adoptées.

### **3. Droit pénal luxembourgeois et normes internationales**

Nous distinguerons le droit pénal de fond (3.1) et le droit pénal de forme (3.2).

#### **3.1 Le droit pénal de fond**

Deux normes internationales tendent à harmoniser les législations des Etats signataires, afin de faciliter la répression des infractions informatiques.

Parce qu'un Etat ne peut lutter seul contre la criminalité informatique, le Conseil de l'Europe a adopté une convention relative à la cybercriminalité le 23 novembre 2001, dans le but de favoriser la collaboration internationale. Or, une telle collaboration implique en premier lieu un accord sur la définition des comportements illicites.

De son côté, le Conseil de l'Union Européenne a adopté le 24 février 2005 une décision-cadre relative aux attaques visant les systèmes d'information dans le but de *“renforcer la coopération entre les autorités judiciaires et les autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les Etats membres, grâce à un rapprochement de leurs règles pénales réprimant les attaques contre les systèmes d'information”* (considérant 1).

Ces deux textes se caractérisent par leur souplesse. En effet, ils fixent de grandes lignes de répression qui, pour la plupart, coïncident (accès illicite à un système informatique, atteinte à l'intégrité d'un système, atteinte à l'intégrité des données, et tout type d'actes apparentés à la complicité et à la tentative).

Il convient en effet de ne pas courir le risque de voir échouer la répression en raison d'une définition trop stricte des éléments constitutifs de l'infraction.

A cet égard, le droit luxembourgeois est conforme à cet esprit, car il ne donne pas de définition du système de traitement automatisé de données. Le développement des techniques est tel que cette absence de définition constitue d'ailleurs la seule solution admissible pour ne pas risquer de voir un texte à peine entré en vigueur se révéler obsolète. La législation n'en est pas pour autant floue car les comportements incriminés, tels que l'accès illicite ou le maintien illicite dans un système de traitement automatisé de données, sont suffisamment précis pour ne pas laisser place à l'arbitraire judiciaire.

La législation luxembourgeoise présente un panorama quasi complet des incitations législatives contenues dans les deux textes internationaux cités. Un point faible subsiste cependant, qui, nous l'avons vu<sup>43</sup> est sur le point de disparaître : le droit luxembourgeois, ne

---

<sup>42</sup> Nous empruntons cette image à G. Vermelle, L'immatériel et la répression, in *Le droit et l'immatériel*, Archives de philosophie du droit, 1999. 213.

<sup>43</sup> Voir la partie II de l'article

connaît pas, pour l'instant, la responsabilité pénale des personnes morales. L'adoption du projet de loi, le 30 mars 2007, visant à introduire la responsabilité pénale des personnes morales permet ainsi au Luxembourg de se mettre en conformité avec les différentes obligations internationales auxquelles il a souscrit. Cette réforme, mûrie depuis un certain temps déjà, est nécessaire, et constitue une avancée positive qui permettra de faciliter la coopération avec les autorités étrangères connaissant pour la plupart une telle responsabilité dans leur législation.

En effet, l'efficacité de la répression, particulièrement en matière de cybercriminalité, repose en grande partie sur la coopération policière et judiciaire des Etats.

### **3. 2 Le droit pénal de forme**

Si l'efficacité du dispositif actuel en matière de fraude informatique n'est pas à remettre en cause pour des intrusions perpétrées à partir du territoire luxembourgeois, on peut néanmoins se demander s'il n'est pas déjà dépassé par le développement de l'Internet.

En effet, les délits d'intrusion commis au Luxembourg (la victime réside au Luxembourg et/ou le pirate agit au Luxembourg) peuvent, par l'intermédiaire de l'Internet, se perpétrer depuis n'importe quel endroit du globe.

L'article 7-2 du Code d'instruction criminelle luxembourgeois dispose :

*« Est réputée commise sur le territoire du Grand-Duché de Luxembourg toute infraction dont un acte caractérisant un de ses éléments constitutifs a été accompli au Grand-Duché de Luxembourg ».*

Cette disposition permet aux autorités judiciaires luxembourgeoises de connaître de toute infraction informatique, dès lors qu'une partie, même accessoire, de cette infraction est accomplie sur le territoire du Grand-Duché. Il importe peu que l'infraction ne soit pas consommée au Luxembourg, dès lors qu'elle l'est ailleurs. Il en résulte un probable conflit positif de compétence, en ce que deux Etats, voire plusieurs, réclament la compétence à l'égard d'une même infraction sur le fondement de leur compétence souveraine territoriale.

Cette situation est un exemple du besoin d'harmonisation procédurale que les Etats européens ressentent ces dernières années. Même si les choses évoluent, il ne faut pas oublier que le droit pénal est toujours une matière basée sur les principes de souveraineté et de territorialité de la loi pénale, qui se caractérisent par un cloisonnement des politiques criminelles entre les Etats.

Ainsi, la poursuite des infractions se heurte encore trop souvent à un défaut de coopération entre les Etats. Il n'existe pas de police internationale, et de plus, la police d'un Etat ne peut accomplir aucun acte sur le territoire d'un autre Etat, ni d'ailleurs être tenu d'accomplir un acte sur son propre territoire à la demande d'un autre Etat. Dès lors, les policiers luxembourgeois doivent pour pouvoir mener à bien leur enquête, s'en remettre à un juge d'instruction, qui enverra une commission rogatoire internationale.

D'une manière générale, l'exécution de ces dernières prend beaucoup de temps et risque ainsi d'annihiler les efforts d'une lutte qui, pour être efficace, doit être la plus rapide possible. Il est en effet capital que la constatation d'un acte d'intrusion informatique intervienne le plus tôt possible, ne serait-ce que pour éviter les maquillages ultérieurs.

Dans ce contexte, l'adoption par le Luxembourg de la loi du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres de l'Union Européenne constitue à n'en pas douter un progrès.

Ce mandat d'arrêt européen a pour but de se substituer à la procédure d'extradition. Il permet le transfert, d'un Etat membre à l'autre, soit d'une personne ayant fait l'objet d'une condamnation définitive à une peine d'emprisonnement ou une mesure de sûreté ayant, au moins, une durée de 4 mois, soit d'une personne s'étant rendue coupable d'une infraction pour laquelle une peine d'emprisonnement ou une mesure de sûreté d'un maximum supérieur à un an est prévue.

Le mandat d'arrêt ne se heurte plus à l'obstacle que constitue le principe de la double incrimination. L'harmonisation des législations en matière informatique actuellement en cours (la décision-cadre du 24 février 2005 ainsi que la convention du Conseil de l'Europe relative à la cybercriminalité y veillent), permettra bientôt à tous les Etats signataires d'émettre un tel mandat à l'encontre de quiconque se trouvant impliqué dans une telle catégorie d'infractions.

Enfin, l'efficacité du mandat d'arrêt européen ne nuit pas au principe *Non bis in idem*, en ce sens que le transfert forcé de la personne ne sera pas obtenu si celle-ci a déjà été jugée définitivement pour les mêmes faits.

## CONCLUSION

Ainsi, bien que la prévention, par la mise en place d'outils techniques et la formation des entreprises, de leurs employés, ainsi que du public reste encore la meilleure protection, on assiste progressivement à la mise en œuvre d'un cadre juridique qui a pour but de gérer l'internationalité des réseaux et de donner une réponse juridique appropriée à la menace que constitue, pour nos sociétés, les différents types d'atteintes portées aux systèmes et réseaux d'information.

\* \* \*

\*

Avril 2007

*Note: Ce memorandum est non exhaustif et ne doit pas être considéré comme un avis juridique. Pour de plus amples informations, n'hésitez pas à consulter notre site internet [www.vocats.com](http://www.vocats.com), à nous écrire à [slg@vocats.com](mailto:slg@vocats.com) ou nous appeler au +352 44 37 37.*