http://www.droit-technologie.org

présente :

LA BELGIQUE SORT ENFIN SES ARMES CONTRE LA CYBERCRIMINALITÉ : A PROPOS DE LA LOI DU 28 NOVEMBRE 2000 SUR LA CRIMINALITE INFORMATIQUE

Florence de Villenfagne

Chercheur au Centre de Recherches Informatique et Droit, Facultés Universitaires Notre-Dame de la Paix de Namur

Florence.devillenfagne@fundp.ac.be

Séverine Dusollier

Maître de Conférences et chercheuse au Centre de Recherches Informatique et Droit, Facultés Universitaires Notre-Dame de la Paix de Namur

Severine.dusollier@fundp.ac.be

16 mars 2001

TABLE DES MATIERES

1. Introduction

On n'a pas manqué de reprocher au législateur belge sa lenteur à inscrire dans l'arsenal répressif la criminalisation de certaines activités liées à l'informatique. Et l'apparente impunité dont s'enorgueillissaient les quelques *hackers* belges ayant fait la une des médias ne pouvait qu'apporter de l'eau au moulin de ces critiques.

Il est vrai que la Belgique fait figure de mauvais élève à cet égard, la plupart de ses confrères européens et extra-européens ayant légiféré en matière de criminalité informatique depuis de nombreuses années déjà[1]. Ce n'est qu'au tournant de ce millénaire que le législateur aura remis sa copie. Copie tardive certes, mais copie tant attendue qu'on lui pardonnera facilement. La loi du 28 novembre 2000[2] relative à la criminalité informatique n'aurait pu mieux tomber pour inaugurer un nouveau siècle de technologies de l'information. Plus que jamais, les réseaux électroniques semblent constituer la cible des pirates, corsaires et autres flibustiers du cyberespace. Leurs agissements, bien que considérés unanimement comme criminels, ne correspondent bien souvent plus à des catégories connues d'infractions. En outre, dans des espaces par nature internationaux, souvent garants d'un certain anonymat, les autorités judiciaires doivent réinventer des modes appropriés d'actions et de recherche des infractions. C'est à ces deux grandes problématiques que la loi belge relative à la criminalité informatique entend répondre.

En conséquence, la loi nouvelle introduit dans le Code Pénal des infractions spécifiques à l'informatique, telles que le faux en informatique, la fraude informatique, et des infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes et données informatiques. L'analyse de ces incriminations fera l'objet de la quatrième partie de cette étude.

Ensuite, et cela conclura notre analyse, le législateur adapte la procédure pénale belge aux spécificités et difficultés de la recherche et de la poursuite des infractions commises sur les réseaux informatiques.

Mais dans un premier temps, il n'est pas inutile de revenir aux sources historiques de la réglementation de la criminalité informatique ainsi qu'aux classifications traditionnelles qui définissent la matière.

2. Les sources du droit de la criminalité informatique

Si la majorité des Etats et institutions internationales ont désormais inscrit la lutte contre la criminalité informatique dans leur arsenal législatif[3], il s'agit toutefois d'un mouvement assez lent qui a réellement pris naissance dans les années quatre-vingts.

L'OCDE a été la première organisation internationale à se pencher sur le phénomène de la criminalité informatique en 1982 en mettant sur pied un groupe de travail *ad hoc.* Le rapport qui en est issu recommandait aux législateurs nationaux d'inclure dans leur arsenal pénal une série d'infractions commises intentionnellement dans le domaine de l'informatique[4]. A titre de référence, l'OCDE et ce groupe de travail ont proposé un liste d'agissements répréhensibles qui pourrait former une base minimale et

---

[1] La Suède fut sans doute le premier pays à adopter une loi relative à la criminalité informatique dès 1973.

[2] M.B. 3 février 2001, p. 2909.

[3] Pour un panorama des législations européennes et américaines en matière de criminalité informatique, voir U. SIEBER, *Legal aspects of computer-related crime in the information society – COMCRIME Study*, Rapport établi pour la Commission Européenne, 1998; S. SCHJOLBERG, *The legal framework – Unauthorized access to computer systems.* Disponible à <http://www.mossbyrett.of.no/info/legal.html>

[4] O.C.D.E., *La fraude liée à l'informatique : analyse des politiques juridiques*, Paris 1986.

commune aux différentes approches susceptibles d'être adoptées par les pays membres. Cette liste reprend les agissements suivants :

(1) l'introduction, l'altération, l'effacement et/ou la suppression de données et/ou de programmes informatiques effectués volontairement avec l'intention de commettre un transfert illégal de fonds ou d'autres valeurs;

(2) l'introduction, l'altération, l'effacement et/ou la suppression de données et/ou de programmes informatiques effectués volontairement avec l'intention de commettre un faux en écriture;

(3) l'introduction, l'altération, l'effacement et/ou la suppression de données et/ou de programmes informatiques ou autres ingérences dans des systèmes informatiques accomplis volontairement avec l'intention d'entraver le fonctionnement du système, informatique et/ou de la télécommunication;

(4) la violation du droit exclusif du propriétaire d'un programme informatique protégé avec l'intention d'exploiter commercialement ce programme et de le commercialiser sur le marché;

(5) l'accès à ou l'interception de fonctions d'un système informatique et/ou de télécommunications, accomplis volontairement et sans l'autorisation de la personne responsable du système, en violation des mesures de sécurité ou avec l'intention de nuire ou d'autres intentions frauduleuses.

En outre, le rapport visait un renforcement de la protection des secrets commerciaux et industriels ainsi que des topographies.

Ce premier travail a été poursuivi en 1989, avec un emphase particulière sur les questions de sécurité, et a abouti à l'adoption d'une Recommandation comportant des lignes directrices sur la sécurité des systèmes informatiques[5]. Ce texte, adressé à la fois aux pouvoirs publics et au secteur privé, encourage la mise en place de standards minimaux de sécurité et l'instauration de sanctions pénales, administratives ou autres en cas d'atteintes aux systèmes informatiques.

Au cours des années 80, la criminalité informatique a également été examinée par un Comité d'Experts du Conseil de l'Europe. Suite à ce travail, le Conseil de l'Europe a adopté en 1989 une Recommandation[6] qui incite les Etats Membres à insérer dans leur dispositif juridique des sanctions adéquates en ce qui concerne certains agissements à l'égard des systèmes informatiques, des données ou des programmes d'ordinateur. En annexe de cette recommandation figure une liste reprenant les types d'agissements pour lesquels les Etats devraient intervenir (liste dite minimale comprenant les infractions de fraude informatique, faux en informatique, dommages affectant les données et les programmes, sabotage informatique, accès et interception non autorisés à des systèmes informatiques), ainsi que ceux pour lesquels l'intervention législative est laissée au libre choix des Etats. En 1995, une deuxième recommandation, dont s'est largement inspiré le législateur belge, aborde plus spécifiquement les questions de procédure[7].

---

[5] O.C.D.E., *Guidelines for the security of information systems*, 1992, OECD/GD (92) 190, disponible sur <http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm>

[6] Recommandation R (89) 9 sur la criminalité en relation avec l'ordinateur, adoptée le 13 septembre 1989, Editions du Conseil de l'Europe, Strasbourg, 1990, disponible sur <http://www.coe.fr/cm/ta/rec/1989/f89r9.htm>

[7] Recommandation R(95) 13 du Conseil de l'Europe relative aux problèmes de procédure pénale liés à la technologie de l'information, adoptée le 11 septembe 1995, éditions du Conseil de l'Europe, 1996, disponible sur <http://www.coe.fr/cm/ta/rec/1995/f95r13.htm>. Voir P. CSONKA, "Criminal procedural law and information technology – The main features of the Council of Europe Recommandation nr R (95) 13", *C.L.S.R.*, 1995, p. 37 et s.

En 2000, le Conseil de l'Europe a publié un projet de convention internationale sur la cyber-criminalité[8]. Ce projet distingue le droit pénal positif dans lequel les Etats sont invités à inscrire l'incrimination d'une série d'agissements informatiques des questions de procédure. Au titre des infractions pour lesquelles une intervention législative est souhaitée, on retrouve l'accès illégal, l'interception illégale, l'atteinte à l'intégrité des données ou du système, les dispositifs illégaux ou *hackertools*, la falsification informatique et la fraude informatique. Le projet de Convention presse également les Etats d'ériger en infraction pénale les actes relevant de la pornographie enfantine et des atteintes au droit d'auteur[9] et droits connexes. Au chapitre de la procédure, le texte insiste notamment sur les questions de perquisition et de saisie des données informatiques, d'injonction de produire des données, de conservation de données relatives au trafic et à l'abonné. Le Conseil de l'Europe souhaite également renforcer la coopération internationale entre autorités judiciaires et policières, notamment en matière d'extradition, d'investigation, de mesures provisoires et d'accès aux données stockées. L'accès aux données stockées dans un autre Etat est ainsi favorisé sans qu'aucune précaution en matière de protection des données à caractère personnel et de flux transfrontalier soit prévue. Le projet de convention est d'ailleurs singulièrement muet sur les implications des questions procédurales sur le respect de la vie privée, ce qui, pour une institution internationale principalement chargée de la protection des droits fondamentaux de l'être humain, ne manque pas de surprendre. Nous verrons ce point plus loin.

De nombreuses voix se sont également élevées pour critiquer la possibilité d'assistance mutuelle entre Etats même en dehors d'un principe de double incrimination.

L'Union européenne s'est aussi lancée dans la réglementation de la criminalité informatique en publiant, à la fin du mois de janvier 2001, une Communication abordant toutes les questions essentielles du débat tant procédurales que relatives au droit pénal matériel[10]. Aux dires de la Commission, il s'agit d'un simple document de réflexion qui devra servir de base aux auditions et discussions habituelles. Mais la communication est bien plus que cela et constitue une synthèse précise des questions essentielles qui se posent en matière de cybercriminalité.

Après avoir répété le contexte particulier de la criminalité informatique sur les réseaux et à l'ère du commerce électronique, la Commission s'inscrit dans la lignée des initiatives internationales telles que celles du Conseil de l'Europe ou de l'OCDE. En effet, elle considère d'une part la nécessité d'agir en droit matériel sur la définition et l'incrimination de comportements illicites sur Internet, qu'il s'agisse de délits spécifiquement liés à l'informatique tels le *hacking*, le faux ou la fraude, ou de délits classiques facilités ou amplifiés par les réseaux électroniques tels la pornographie infantile, la contrefaçon ou les atteintes à la vie privée. La communication rappelle les directives et autres mesures communautaires adoptées et annonce une proposition de directive harmonisant les incriminations nationales des délits informatiques et les inscrivant dans le droit communautaire. Et d'autre part, sur le plan de la procédure, la communication relève une série de questions, classiques ou moins classiques, qui se posent dans la recherche et la poursuite des infractions informatiques: l'interception des télécommunications, la conservation des données relatives au trafic, l'anonymat de l'accès et de l'utilisation des réseaux, la coopération et la compétence internationales, la force probatoire des données informatiques, ainsi que la question de la formation et de l'expertise des autorités policières et judiciaires en charge de cette catégorie particulière de criminalité. Enfin, la communication propose de créer un Forum Européen rassemblant les autorités et personnes responsables de la poursuite des infractions, des représentants des organismes nationaux de protection des données ainsi que des opérateurs de télécommunications et prestataires de services Internet.

---

[8] Projet de convention du Conseil de l'Europe sur la criminalité informatique (Projet N° 22 REV. 2), version du 2 octobre 2000, disponible sur <http://conventions.coe.int/treaty/FR/projetsubercrime22.htm>

[9] Remarquons qu'à ce titre, il n'est pas demandé aux Etats de considérer la violation du droit moral comme une infraction. Le droit moral n'est décidément que rarement invité à la table des textes internationaux.

[10] Communication de la Commission au Conseil, au Parlement Européen, au Comité Economique et Social et au Comité des Régions, *Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité*, COM(2000) 890 final, disponible sur <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html>

La spécificité de l'approche communautaire, par rapport aux initiatives du Conseil de l'Europe, tient surtout à l'insistance sur la nécessité d'une approche préventive en matière de sécurité, notamment en soutenant des recherches dans ce domaine, et d'une attention constante aux problèmes de vie privée que la recherche et la poursuite des cybercrimes sont susceptibles de poser.

3. Les domaines de la criminalité informatique

L'étude du phénomène et de la législation propre à la criminalité informatique peut difficilement se faire sans s'attarder sur ce que l'on entend par *criminalité informatique*. Une analyse de la doctrine en la matière met en lumière que la criminalité informatique peut être comprise de diverses manières, certains auteurs se bornant à étudier la criminalité informatique *sensu stricto* tandis que d'autres considèrent qu'il faut l'analyser au sens large. Dans tous les cas néanmoins, les auteurs définissent des catégories de délits informatiques qu'ils affinent et complètent de façon très personnelle.

Ulrich Sieber[11], par exemple, se base sur la définition donnée en 1983 par l'OCDE pour diviser la criminalité informatique en six domaines. L'OCDE définissant la criminalité informatique de façon très large comme *tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou une transmission de données*[12], les catégories de Sieber recouvrent la criminalité informatique au sens large, mais avec la particularité de les voir à travers un prisme « législatif ». Concrètement Sieber définit les domaines suivants :

- *field I : Protection of privacy*
- *field II : Economic criminal Law*
- *field III : Protection of Intellectual Property*
- *field IV : Illegal and Harmful Contents*
- *field V : Criminal Procedural Law*
- *field VI : Security Law*

Sa démarche qui se rapproche plus d'une tentative de classification des initiatives législatives dans le domaine que d'un essai de classer les délits informatiques eux-mêmes en différentes catégories, nous permet pourtant – en mettant à part les deux derniers domaines – de dégager des catégories très claires de délits :

- les actes qui portent atteinte aux données à caractère personnel (*field* I),
- les délits informatiques économiques (*field* II),
- les actes portant atteinte aux droits de propriété intellectuelle (*field* III) et
- les contenus illégaux et préjudiciables (*field* IV).

D'autres auteurs[13] divisent la criminalité informatique en deux grandes catégories :

- les actes où l'informatique est la cible de l'infraction ; et
- les actes où l'informatique est l'outil de l'infraction.

Le professeur David L. Carter de l'Université de l'Etat du Michigan[14] estime même qu'il faut y ajouter deux catégories supplémentaires :

- les actes où l'informatique a un caractère incident au délit (il s'agit d'un délit classique, l'informatique n'y est pas indispensable, mais permet d'agir plus vite, plus facilement, autrement. Par exemple la publication de pornographie enfantine sur Internet, ou le meurtre d'un patient en modifiant le dosage de ses médicaments dans l'ordinateur de l'hôpital) ; et

---

[11] U. SIEBER, *op.cit.*

[12] OCDE, *La fraude liée à l'informatique: analyse des politiques juridiques,* op.cit., p.7.

[13] division classique retrouvée communément dans les textes parlant de criminalité informatique.

[14] D. L. CARTER, « Computer Crime Categories : How techno-criminals Operate », *FBI Law enforcement Bulletin,* 1992, <http://nsi.org/Library/Compsec/crimecom.html>

- les actes constituant de nouvelles versions de délits traditionnels (il s'agit de délits classiques adaptés à l'ordinateur, comme la copie pirate de logiciels, par exemple).

Carter souligne néanmoins que certains agissements se classeront difficilement dans une seule de ces quatre catégories.

4. Les infractions informatiques dans la loi belge

4.1. Le faux en informatique

Le faux en informatique, premier délit traité dans la loi belge, peut, à notre avis, être rangé dans la catégorie des « délits informatiques économiques » de Sieber, dans la catégorie classique des « actes où l'informatique est l'outil de l'infraction », mais aussi dans celle des « actes constituant de nouvelles versions de délits traditionnels » de Carter[15]. Nous verrons que la classification dans cette dernière catégorie aura des conséquences importantes.

4.1.1. La difficulté d'appliquer le délit de faux en écriture au faux informatique

Considérant que le faux en informatique constitue une nouvelle version d'un délit « traditionnel », à savoir le faux en écriture, l'on aurait dû pouvoir se tourner vers les articles 193 et suivants du Code pénal pour incriminer ce genre de comportement s'il n'était interdit en matière pénale d'avoir recours à une interprétation analogique de la loi. L'*informatique* semble en effet ne pas pouvoir entrer dans la définition donnée au mot *écriture* tel qu'il est utilisé dans ces articles[16]. Les dispositions relatives au faux en écriture ne suffisent donc pas pour appréhender des infractions comme la fabrication de fausses cartes de crédit, de fausses signatures digitales ou la modification d'éléments d'un contrat numérique. L'introduction du faux en informatique était réellement nécessaire.

4.1.2. L'article 210bis du Code Pénal introduit par la loi

La loi sanctionne d'une peine de six mois à cinq ans d'emprisonnement et d'une amende "*celui qui commet un faux, en introduisant dans un système informatique, en modifiant ou effaçant des données, qui 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, et par là modifie la portée juridique de telles données"*. L'usage des données ainsi obtenues est également considéré comme un délit.

L'article 210*bis* en projet érige en infraction le faux en informatique, ce qui vise la *dissimulation intentionnelle de la vérité par le biais de manipulations informatiques de données pertinentes sur le plan juridique*[17].

Malheureusement, n'ayant pas considéré qu'une révision complète du chapitre sur le faux se justifiait, le législateur n'a pas harmonisé les dispositions relatives au faux en écriture et celles concernant le faux en informatique. Contrairement au faux traditionnel[18], l'infraction informatique est unique et n'établit pas de distinction quant à la nature des actes falsifiés (acte public, acte authentique, commercial ou privé), ni quant à l'auteur de l'infraction (fonctionnaires dans l'exercice de leurs fonctions ou particuliers). L'abandon

---

[15] Certains estimeront peut-être que le faux en informatique devra plutôt être rangé parmi les actes où l'informatique a un caractère incident au délit. Cela démontre la complexité de la classification des délits.

[16] Voir notamment le fameux arrêt Bistel, Bruxelles, 24 juin 1991, *Rev. dr. pén.*, 1992, p. 340.

[17] *Exposé des motifs*, Doc. Parl. Chambre, 0213/001, p.14

[18] A. MASSET, "Faux en écritures et usages de faux", in F. GORLE, A. DE NAUW, P.L. BODSON (ed.), *Qualifications et jurisprudences pénales*, 1986.

de cette distinction dans la version informatique du faux a été critiqué par le Conseil d'Etat[19] qui rappelle ce qui est dit dans l'exposé des motifs lui-même, à savoir que toute situation en ligne doit être traitée de la même manière qu'une situation similaire hors ligne. Or le faux en informatique n'est qu'une nouvelle forme de faux, une « nouvelle version » d'un délit traditionnel, il ne devrait donc pas être traité différemment que le faux en écriture. On observe pourtant une rupture du principe d'égalité entre faux traditionnel et faux informatique qu'il n'est ni légitime ni opportun de pénaliser de manière différente selon qu'ils soient commis au moyen de l'informatique ou non. Il y a ici une discrimination que les plaideurs se feront une joie de porter à la connaissance de la Cour d'Arbitrage.

4.1.3. Eléments constitutifs de l'infraction

Quant à savoir dans quels cas ce nouvel article pourrait s'appliquer, il conviendra de vérifier que tous les éléments du faux en informatique soient réunis :

- Il faut tout d'abord qu'il y ait introduction, modification ou effacement de *données* dans un système informatique ou une modification de l'utilisation possible de ces données. L'exposé des motifs[20] donne une définition très large de la notion de données puisqu'il spécifie qu'il faut entendre par là « les représentations de l'information pouvant être stockées, traitées et transmises par le biais d'un système informatique ». La volonté de faire face à toute évolution technologique est manifeste dans cette définition.

- Il faut ensuite que le faux modifie la portée juridique de ces données. A ce propos, l'exposé des motifs souligne qu'il appartiendra au juge d'apprécier si cette modification a effectivement eu lieu.

- Il faut enfin vérifier qu'il y ait eu intention frauduleuse ou dessein de nuire. A la lecture de l'article 210*bis* en projet on pourrait croire que les manipulations informatiques seront punissables du seul fait de leur commission volontaire et consciente, contrairement au faux traditionnel qui requiert un dol spécial, soit l'intention frauduleuse ou le dessein de nuire. Mais depuis un amendement apporté par le Sénat[21], il faut bien un dol spécial dans les deux cas. L'article 193 du Code pénal ayant été modifié, désormais, comme pour le faux en écriture, l'intention frauduleuse ou le dessein de nuire constituent un élément essentiel du faux ou de l'usage de faux en informatique. En conséquence, nous pensons que, par exemple, la fabrication de fausses cartes de crédit ou de fausses signatures digitales dans un but scientifique (par exemple pour démontrer la vulnérabilité d'un système ou dans le cadre d'un enseignement) ne devrait pas pouvoir mener à une condamnation sur base de cet article.

4.2. La fraude informatique

L'article *504quater* quant à lui définit la nouvelle infraction de fraude informatique. Celle-ci peut également être rangée dans la catégorie des « délits informatiques économiques » de Sieber. Quant à savoir dans quelle catégorie classique il faut la classer, la question est plus délicate. Si la plupart des cas qui seront qualifiés de fraude informatique seront des « actes où l'informatique est l'outil de l'infraction » puisqu'il s'agit bien sûr principalement de *se procurer, pour soi-même ou pour autrui, un avantage patrimonial frauduleux*, nous pensons que certaines infractions pourront difficilement échapper à la classe des « actes où l'informatique est la cible de l'infraction » ou aux deux nouvelles catégories introduites par David L. Carter. Vu la nécessité d'analyser les infractions au cas par cas pour les faire entrer dans une ou plusieurs catégories, la classification perd –à notre sens– tout intérêt dans le cadre de la fraude

[1919] Avis du Conseil d'Etat, Doc. Parl. Chambre, 1999-2000, 0213/001 et 0214/001, p. 51

[20] Doc. Parl., Chambre 0213/001, o*p. cit.,* p.12

[21] daté du 19 juillet 2000

informatique. Nous ne nous y attarderons donc pas, préférant insister sur la compréhension de l'infraction et l'interprétation extrêmement large qui peut en être faite.

4.2.1. La difficulté d'appliquer le droit pénal traditionnel aux fraudes informatiques

Comme pour le faux en informatique, le droit pénal traditionnel ne suffisait plus pour appréhender des comportements qui justifiaient pourtant qu'un juge pénal s'y intéresse. Sans avoir recours à une interprétation analogique des textes de loi existants, des exemples[22] tels que l'utilisation d'une carte de crédit volée pour retirer de l'argent à un guichet automatique, le dépassement illicite du crédit sur sa propre carte de crédit, le détournement motivé par l'appât du gain de fichiers ou programmes confiés dans un but précis, l'introduction d'instructions informatiques pour modifier le résultat de certaines opérations, ne pouvaient être incriminés.

4.2.2. L'article 504quater du Code pénal introduit par la loi

Cette nouvelle disposition 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".

Les exemples de fraude informatique sont nombreux. En plus des exemples cités plus haut, on songe à des manipulations effectuées par un employé de banque sur les comptes des clients ou à des altérations informatiques de comptes de répartition des droits d'auteurs perçues par des sociétés de gestion pour en faire bénéficier des personnes qui ne devraient pas y avoir droit. Selon nous, l'introduction dans un programme informatique piraté d'une liste de numéros de licence trouvés sur Internet constituera également un délit de fraude informatique, l'avantage patrimonial frauduleux consistant en l'utilisation et la copie d'un logiciel sans autorisation de l'auteur.

L'infraction est relativement distincte de l'escroquerie dont l'objectif est principalement de tromper la confiance d'un tiers. Dans le cas présent il faut, mais il suffit, que l'avantage patrimonial obtenu grâce à la commission de l'infraction présente un caractère frauduleux. Ce qui voudrait dire, si l'on reprend la définition de « fraude » de CORNU[23], que l'avantage patrimonial a été obtenu par « un acte accompli dans le dessein de préjudicier à des droits que l'on doit respecter, », par « un agissement illicite par l'emploi de moyens illégaux » ou même par « un agissement illicite par l'emploi de moyens réguliers ».

La définition de la fraude informatique est donc large, trop large nous semble-t-il. Pourtant cette largesse qui nous semble dangereuse peut difficilement être palliée. C'est ici que l'on trouve toute la complexité d'un domaine lié aux Technologies de la Communication et de l'Information : les textes doivent être suffisamment larges pour englober les technologies à venir tout en étant suffisamment précis pour respecter le principe de prévisibilité valable en droit pénal. Le citoyen doit clairement savoir ce qu'il n'a pas le droit de faire sous peine d'être pénalement poursuivi, mais le législateur peut difficilement énumérer tous les exemples de fraude informatique qui se diversifient tous les jours grâce au développement des technologies. Si cette difficulté existe, il n'en reste pas moins que la largesse de la définition comporte des dangers réels. On peut imaginer que certains actes parfaitement courants sur les réseaux informatiques puissent désormais être qualifiés de fraude.

Il est courant, par exemple, que des cookies soient installés sur le disque dur[24] de l'ordinateur d'un utilisateur lorsqu'il visite un site. Ce petit fichier texte contient des informations concernant la navigation

[22] cités dans l'exposé des motifs.

[23] G. CORNU, *Vocabulaire juridique*, PUF, 1998

[24] J.M. DINANT, "Les traitements invisibles sur Internet", in E. MONTERO (ed.), *Droits des technologies de l'information – regards prospectifs*, Cahier du CRID n°16, Bruylant, Bruxelles, 1999, p. 271-294.

de l'internaute, il contient la langue dans laquelle l'internaute a souhaité s'exprimer, le pseudonyme qu'il s'est donné ou éventuellement les pages qu'il a consultées. Sans vouloir entrer dans des considérations techniques trop poussées sur le cookie, il convient de souligner qu'il en existe différentes sortes. Les cookies de session s'effacent de l'ordinateur de l'internaute dès que celui-ci quitte le site en question. Il est indispensable à la bonne navigation de l'internaute : comme il garde en mémoire tous les actes posés lors d'une même session c'est grâce à lui, par exemple, que l'internaute peut faire différents achats sur un site et remplir son « panier ». D'autres cookies sont plus insidieux, car ils ne peuvent être effacés du disque dur de l'ordinateur que par un acte volontaire de l'internaute ou à l'expiration de leur durée de validité[25] : ces cookies sont dits permanents[26]. Ils peuvent être envoyés à l'internaute par le site consulté, mais aussi par un autre site dont l'internaute ignore jusqu'à l'existence. Les bannières publicitaires, par exemple, cachent souvent des 'ordres informatiques' cachés du type 'set cookie' qui viennent de la société qui gère ces bannières et non du site sur lequel ces bannières apparaissent. Lors d'une navigation ultérieure les cookies permanents seront renvoyés[27] au site qui les a installés (le site sur lequel on a surfé ou celui qui est caché derrière une bannière). Mais l'objectif d'une telle technologie, très simple au demeurant, est particulièrement ambivalent. Souvent utiles, les cookies permettent une authentification de l'utilisateur lors de visites répétées d'un même site[28], par exemple, en conservant une liste d'achats antérieurs, un compte de courrier électronique, des notes et préférences personnelles. L'internaute est tout de suite accueilli dans sa langue par exemple. Mais dans certains cas les cookies servent des buts bien moins indispensables. Des profils assez précis des utilisateurs peuvent notamment être déduits d'une collecte et d'un traitement des cookies stockés sur le disque dur de ceux-ci. Cette pratique permet au marchand, à l'insu de l'internaute, de se constituer une base de données dont la valeur en termes de marketing augmente à chaque nouvelle connexion.

Selon nous, l'inscription de cookies sur les disques durs des ordinateurs ainsi que toute requête ultérieure qui en interroge le contenu constituent des "introductions dans un système informatiques de données stockées, traitées ou transmises par un système informatique". Mais pour qu'il y ait fraude, il faut encore que l'on se soit procuré un avantage patrimonial frauduleux. Dans le cas de cookies permanents, l'avantage patrimonial consiste en une masse de données relatives au trafic de l'utilisateur sur Internet, des informations de marketing extrêmement précieuses dont le bénéfice sur le patrimoine d'une société n'est plus à démontrer. Encore faudrait-il démontrer que l'avantage patrimonial a été obtenu par « un acte accompli dans le dessein de préjudicier à des droits que l'on doit respecter», par « un agissement illicite par l'emploi de moyens illégaux » ou même par « un agissement illicite par l'emploi de moyens réguliers »[29].

Reprenons pour cela les deux cas d'installation de cookie que nous trouvons les plus problématiques et analysons-les au regard de la loi du 8 décembre 1992 relative à la protection des données à caractère personnel :

(1) le cas où un site X installe un *cookie* permanent qui lui sera renvoyé lors d'une nouvelle connexion de l'internaute et

---

[25] Qui excède parfois 40 ans !

[26] Lire à ce propos l'article de J.M. DINANT, *op. cit.*

[27] Il doit être spécifié que les *cookies* ne peuvent en principe être lus que par celui qui les a envoyés. Cela signifie que le site X ne peut que lire les *cookies* X et cela uniquement lorsque l'internaute se re-connecte au site X. Par contre, les sociétés gérant des bannières publicitaires –installant des *cookies* Z à l'insu de l'internaute lorsqu'il se connecte au site X sur lequel apparaît une bannière de la société publicitaire Z– se voient renvoyer et peuvent lire ce *cookie* Z même lorsque l'internaute visite un site Y. Il suffit qu'une bannière Z soit installée sur ce site Y.

[28] ou lors de visites de sites différents contenant des bannières publicitaires d'une même société.

[29] G. CORNU, *op.cit.*

(2) le cas où Z installe un *cookie* permanent via une bannière publicitaire qui apparaît sur le site Y et qui lui sera renvoyé lors d'une connexion de l'internaute sur n'importe quel site affichant une bannière Z.

Que les informations contenues dans les *cookies* soient qualifiées de données personnelles n'est pas toujours certain. Les avis divergent quant à déterminer qu'un profilage extrêmement précis, mais non associé ou associable au nom de l'internaute, constitue une donnée à caractère personnel. Nous pensons néanmoins que ce sera souvent le cas car un profilage précis reprendra presque toujours « toute information concernant une personne physique identifiée ou identifiable » au sens de la loi du 8 décembre 1992 relative à la protection des données à caractère personnel[30]. La loi définit en effet qu'il faut entendre par personne « identifiable une personne qui 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, psychique, économique, culturelle ou sociale** ».

Dans la mesure où la collecte de ces données à caractère personnel se fait alors sans respecter les préceptes de la loi du 8 décembre 1992, nous nous trouvons devant un agissement illicite qui doit, selon nous, être qualifié de fraude informatique. Aucune différence ne peut être faite à ce point de vue entre les deux cas problématiques que nous avons présentés plus haut. Et c'est là que, pour nous, se situe le problème[31]. Faut-il nécessairement permettre une qualification pénale dans les deux cas ? Nous ne pensons pas qu'il faille permettre d'aller jusque là dans le premier cas[32]. Que le responsable du traitement puisse être poursuivi pour non respect de la loi sur la protection des données à caractère personnel est une bonne chose, mais qu'il puisse s'agir en plus de fraude informatique nous paraît beaucoup plus contestable. Dans le deuxième cas, par contre, où le profilage se fait de façon massive, totalement cachée et extrêmement efficace, nous espérons que la nouvelle infraction de fraude informatique permettra –en plus de la loi sur la protection des données à caractère personnel– d'éradiquer le fléau du cybermarketing sauvage particulièrement lucratif.

4.3. Les infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes

Le titre IX*bis* qui est inséré dans le livre II du Code pénal par la nouvelle loi propose un dernier type d'infractions. Il s'agit des infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes. Ce titre recouvre en réalité plusieurs types d'infractions :

- l'accès et le maintien non autorisé dans un système informatique qui visent (art. 550*bis*) :

[30] art. 1er §1.

[31] C'est là que se profile le danger de la largesse de la définition donnée à la fraude informatique.

[32] Il s'agit du cas où les *cookies* sont placés par le site que l'internaute visite. Bien sûr, dans la plupart des cas l'internaute n'est pas au courant du placement de ce *cookie* puisque par défaut le navigateur ne prévient pas l'internaute de l'inscription de ce petit fichier texte. Mais il s'agit là d'un problème qui concerne surtout les fabricants des navigateurs dont l'innocence dans le maintien dans l'ignorance de l'internaute des pratiques « privacides » (Voyez J.M. DINANT, *op.cit)* sur le Net doit sérieusement être mise en doute.

- les atteintes portées à partir de l'extérieur du système, *hacking* externe (§ 1er)
- les atteintes portées par des utilisateurs qui possèdent certains pouvoirs d'accès, *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)

- le sabotage des données et le sabotage informatique qui visent (art. 550*ter*) :
  - toute manipulation de données effectuée dans le but de nuire (§ 1er)
  - le fait de causer des dommages aux données (§ 2).
  - le fait d'empêcher le bon fonctionnement d'un système informatique (§ 3)
  - les actes préparatoires tels la conception ou mise à disposition de virus ou de programmes visant à développer pareils virus (§ 4).

4.3.1. L'accès et le maintien non autorisé dans un système informatique

Une large part de la criminalité informatique, et sans doute la plus médiatisée, consiste en l'intrusion non autorisée dans les systèmes informatiques ou *hacking*. Cette pratique des milieux *underground* d'Internet est un jeu pour les uns, de la provocation pour d'autres, une manière de faire connaître ses revendications pour les troisièmes. Mais les jeunes fous de l'informatique ne sont pas les seuls à s'adonner au *hacking*. Il ne faut pas sous-estimer l'ampleur des actes de *hacking* accomplis par des sociétés ou des mafias au titre d'espionnage et de sabotage industriel ou politique. Ces cas-là sont toutefois beaucoup moins connus, les entreprises ou administrations publiques qui en sont victimes préférant ne pas se faire de la mauvaise publicité.

Ces accès non autorisés sont évidemment facilités par l'apparition des réseaux et par l'entrée des sociétés sur Internet, notamment par le biais de services et informations rendus à la clientèle ou d'offres de commerce électronique qui donnent souvent aux *hackers* des portes d'entrée idéales vers les systèmes informatiques de l'entreprise.

L'accès illicite est un délit informatique pour lequel la solution doit être particulièrement adaptée. Le législateur peut établir diverses conditions d'incrimination. L'accès peut être illicite uniquement dans le cas où il s'effectue en violation des mesures de sécurité, lorsqu'il poursuit un but d'obtention de données ou de sabotage ou toute autre intention délictueuse. L'accès peut également être sanctionné en tant que tel sans qu'aucune de ces conditions ne soit requise. C'est le choix du législateur belge qui, en vertu du nouvel article 550*bis* du Code Pénal, pénalise le simple accès non autorisé à un système informatique ou le maintien indu dans le système. Soulignons néanmoins, comme le rappelle l'exposé des motifs[33], que cela n'empêche en aucun cas « l'application des dispositions pénales d'autres régimes de protection concernant des catégories particulières de données ». Ce qui signifie que si l'accès non autorisé est poursuivi sur base

Voyez M. ANTOINE, F. de VILLENFAGNE, D. GOBERT, A. SALAÜN, L. ROLIN, V. TILMAN, E. WERY, sous la direction du professeur Yves POULLET, *Guide à destination des utilisateurs d'Internet*, Ministère des Affaires économiques, avril 2000.

[33] Doc. Parl. , Chambre 0213/001, o*p. cit.,* p.17.

d'une loi particulière, les conditions de cette loi[34] seront d'application, en ce compris l'exigence éventuelle d'un dol spécial.

a. L'article 550bis

L'article 550*bis* 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.

« *- § 1 er. 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 1er, 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, outrepasse 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 seule-ment. (...) »

b. le hacking externe

La première hypothèse vise les cas classiques de *hacking* dans lesquels la défense d'un réseau fermé est contournée via l'infrastructure de télécommunications. Les noms de Kevin Mitnick[35], ReDaTtacK, viennent immédiatement à l'esprit. Le texte vise clairement "*celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient"* et le punit de manière différente selon qu'il ait eu ou non une intention frauduleuse.
Le maintien est bien entendu 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. Un jugement français donne un exemple de ce genre de pratiques[36]. Des agents de France Télécom se connectaient à des jeux télématiques non pour y jouer, mais dans le seul but de bénéficier de jetons de présence qui leur ouvraient le droit à certains cadeaux. Toutefois, pour éviter le système de déconnexion automatique après un certain laps de temps pendant lequel aucune donnée ne transite, ils utilisaient un mécanisme dit de rafraîchissement d'écran. En dépit du fait que la connexion initiale était parfaitement régulière, les joueurs-fraudeurs ont été condamnés par le tribunal sur base de l'infraction de maintien illicite dans un système de traitement de données.

Pour être poursuivi tant pour accès que pour maintien non autorisés dans un système informatique, un dol général est suffisant. Les peines sont seulement aggravées lorsque l'accès s'accomplit dans une intention frauduleuse.

---

[34] comme, par exemple, celles de la loi du 15 janvier 1990 sur la Banque-carrefour de la sécurité sociale

[35] Hacker US célèbre sorti de prison récemment après y avoir passé près de 5 ans pour divers actes de *hacking* ayant coûté plusieurs millions de dollars à des entreprises américaines. Il n'a aujourd'hui plus le droit, et ce pendant trois ans, d'utiliser tout outil de (télé)communication raccordable à Internet (ordinateur, téléphone cellulaire, modem, télévision, ou autres)

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

Ceci nous paraît favoriser l'émergence d'une criminalisation très large et sans doute excessive. Seront ainsi considérés comme criminels tout jeune qui s'amusera à déjouer les mécanismes de sécurité des réseaux et systèmes informatiques, ainsi que tout chercheur ou expert en sécurité informatique qui tente de déverrouiller les dispositifs de protection afin d'en vérifier la fiabilité et l'efficacité. Le Conseil d'Etat s'inquiète d'ailleurs du fait que "*dans un contexte informatique, la simple curiosité peut susciter un délit pénal*"[37]. Pourtant le législateur estime que « l'intérêt juridique protégé par les nouvelles dispositions est en premier lieu l'intégrité du système »[38] et que ne pas punir ceux qui agiraient contre ces systèmes même sans intention frauduleuse ou méchante "ouvrirait la voie à toutes sortes d'abus qui mettraient en danger la sécurité des systèmes informatiques"[39]. L'impasse est donc totale sauf à imaginer un système où il est requis que l'infraction se fasse en dépit de mesures de sécurité. La neutralisation de ces mesures pouvant constituer alors un élément de preuve de l'absence d'autorisation d'accès au système. Mais exiger que l'infraction se réalise moyennant un 'cassage' des dispositifs de sécurité entraîne également certains inconvénients. L'explication des mesures de sécurité et de leur contournement sera nécessaire à l'établissement de l'infraction. On comprend que les plaignants, sociétés commerciales ou non, seront peu enclins à produire de tels éléments, ce qui serait préjudiciable pour leur sécurité future. Les travaux préparatoires rappellent par ailleurs combien ces mesures deviennent extrêmement standardisées ce qui rend de plus en plus inutile une telle condition. Le problème reste donc entier et nous persistons à croire que requérir un dol spécial eût été la meilleure solution.
Un autre exemple souligne le danger de l'absence d'une intention frauduleuse ou d'un but de nuire. Récemment, un site américain d'enchères sur Internet a réussi à faire condamner un concurrent, la firme e-Bay, qui fournit aux utilisateurs des informations comparées sur les offres proposées par différents sites d'enchères. La base de la condamnation était le *trespass*, institution juridique américaine qui sanctionne l'intrusion non autorisée dans une propriété. L'extension de cette protection de la propriété matérielle au monde de l'immatériel a suscité de nombreuses critiques outre-Atlantique. Or, l'infraction d'accès et de maintien indu, sans qu'aucun dol spécial ne soit requis, est susceptible de mener aux mêmes conséquences non désirées. Reprenons l'hypothèse de l'affaire e-Bay. Cet opérateur effectuait des recherches sur les sites d'enchères en ligne au moyen d'agents électroniques ou de moteurs de recherche qui rapportaient ensuite à l'internaute le résultat de leurs investigations dans les bases de données visitées. Bidder's Edge Inc., demandeur à l'action, a soutenu que la recherche électronique d'e-Bay, accaparait un espace non négligeable de son serveur ce qui ralentissait la capacité de traitement des demandes des utilisateurs légitimes de son site. Le juge a admis cette "occupation" de l'espace informatique et les dommages qu'elle occasionnait. Le délit de maintien indû permet une solution bien plus directe. L'accès aux sites Internet ouverts au public est bien sûr autorisé, mais l'opérateur d'un site pourrait facilement plaider que sa consultation prolongée par un moteur de recherche ou tout autre type d'agent électronique constitue un maintien non autorisé dans le site.

Ne pourrait-on pas imaginer à l'extrême que l'infraction d'accès, ou plus spécifiquement celle de maintien non autorisé, puisse servir de base à une entreprise pour poursuivre un ancien employé qui enverrait de façon répétée à son personnel des emails critiquant leur employeur ou à une société contestée pour essayer de faire condamner des militants politiques ou associatifs qui l'assiégeraient de fax ou d'emails ? Il nous semble qu'en l'absence d'un dol spécial, ces cas d'école pourraient devenir réalité.

c. le hacking interne

L'article 550*bis* vise ensuite les cas d'accès illicite à partir de l'intérieur du réseau: le cas typique de l'employé qui jette un œil sur des fichiers confidentiels auxquels il n'est pas censé avoir accès. Contrairement au cas précédent, un dol spécial est requis lors du dépassement du niveau d'autorisation accordé. Le simple fait d'entrer illicitement dans des parties du système n'est pas incriminé, il faut qu'il y

[37] Avis du Conseil d'Etat, *op.cit.*, p. 50.

[38] Doc. Parl. , Chambre 0213/001, o*p. cit.,*p. 17

[39] Justification de l'amendement n°11, Doc. Parl. , Chambre 0213/010, 22 septembre 2000.

ait une intention particulière comme l'appât du gain illicite ou la malveillance. Le législateur estime en effet que d'autres « mécanismes moins radicaux (sanctions internes, législation du travail, droit civil, ...) »[40] doivent aborder les cas où le dol spécial fait défaut. Ce point de vue nous semble particulièrement sensé, nous regrettons seulement qu'il n'ait pas été appliqué également au *hacking* externe.

d. les circonstances aggravantes

L'article 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;*

Selon l'exposé des motifs, ces circonstances visent respectivement l'espionnage industriel ou le vol de secrets d'entreprise; l'usage abusif, le vol de capacité ou de temps-ordinateur et le dommage causé, même non intentionnellement. Mais à notre avis, ces circonstances sont libellées de telle façon qu'elles seront systématiquement applicables dans tous les cas de *hacking* interne ou externe. Vu qu'en informatique il n'est pas possible d'accéder à un système sans l'utiliser, sans en *faire un usage quelconque*, nous pensons que le 2° sera systématiquement applicable et les peines inévitablement alourdies. Le juge ne se bornera probablement pas à interpréter ce deuxième point au seul « usage abusif » ou « vol de capacité » tel que semble le vouloir l'exposé des motifs.

La conséquence de cette remarque est importante. Il en résulte que les deux premiers paragraphes qui décrivent l'infraction ne seront jamais appliqués tels quels et que, finalement, le *hacker* externe (qu'il ait agi avec des intentions frauduleuses ou non) et le *hacker* interne (ayant agi avec des intentions frauduleuses) risquent exactement les mêmes peines (celles qui s'appliquent aux actes commis avec des circonstances aggravantes), ce que le législateur aurait voulu éviter.

e. les hackertools

Le 5ème paragraphe du même article traite la problématique des *hackertools*.
§ 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 §§ 1er 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'intention est clairement de punir ceux qui s'adonnent au trafic de mots de passe, qui publient des numéros de licences de logiciels sur Internet ou commercialisent des logiciels permettant de craquer des codes d'accès, etc. En bref il s'agit de ceux qui diffusent, mettent à disposition ou commercialisent ce que l'on appelle les *hackertools*. Cela étant, les scientifiques, spécialistes en sécurité informatique ou constructeurs, redoutent particulièrement cette disposition. Ils craignent en effet qu'elle ne soit utilisée, soit pour les poursuivre pour complicité dans la création des *hackertools*, car ce sont leurs machines et logiciels qui rendent cette pratique possible et ce sont les professeurs qui expliquent les attaques à leurs

[40] Doc. Parl. , Chambre 0213/001, o*p. cit.,* p.16.

élèves, soit pour les poursuivre pour utilisation et recherche de *hackertools*, car ils reconnaissent avoir besoin de ces outils pour constamment augmenter la sécurité de leurs systèmes.

La loi prévoit heureusement qu'il faut un dessein de nuire ou une intention frauduleuse pour être susceptible d'être poursuivi, mais, pour les spécialistes, professeurs ou fabricants de logiciels, le danger existe que cette disposition serve de base juridique et soit une porte ouverte à des procès sans fin.

Cette disposition pourra également servir à incriminer la commercialisation d'équipements permettant la neutralisation de dispositifs de protection d'œuvres protégées par le droit d'auteur, dans l'attente d'une transposition en droit belge de la directive européenne sur l'harmonisation du droit d'auteur dans la société de l'information. Protéger son œuvre ou en verrouiller l'accès par le biais d'une mesure technique qualifie tout accès en violation de ce dispositif, d'accès non autorisé qui pourra être poursuivi sur base de l'article 550*bis* nouveau du Code Pénal. La distribution d'appareils permettant le contournement d'un tel dispositif se verra pareillement pénalement sanctionnée si elle est accomplie avec une intention frauduleuse.

*4.4. le sabotage des données et le sabotage informatique (art. 550***ter***)*

a. La manipulation de données effectuée dans le but de nuire

Finalement, dans l'article 550*ter*, le projet de loi s'attaque au sabotage proprement dit. Le droit pénal actuel ne prenant en compte "les destructions et dommages que lorsqu'ils se rapportent à des objets tangibles"[41] (mis à part le dommage moral bien sûr), il fallait prévoir le cas où le dommage se rapportait à des données. La nouvelle disposition veut donc punir "toute manipulation de données effectuée dans le but de nuire"[42].
"Celui qui, dans le but de nuire, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation possible de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement."

Si des dommages résultent de cette manipulation désormais incriminée, l'exposé des motifs souligne que « les causes des dommages occasionnés au système informatique sont également reprises parce que dans la pratique, les dommages causés aux données et au système informatique même se produiront souvent simultanément et que, d'un point de vue technique, on ne peut pas toujours les différencier de manière stricte. Toutefois, il est souhaitable d'établir une distinction juridique entre les conséquences sur les données et celles qui concernent le système informatique. »[43] Les paragraphes 2 et 3 explicitent ce point de vue en punissant :

§ 2. Celui qui, suite à la commission d'une infraction visée au § 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique et

§ 3. Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique

Le législateur justifie la punition plus sévère prévue au §3 par « l'importance que prennent les systèmes informatiques dans notre société »[44].

---

[41] *Exposé des motifs, op. cit.,* p. 19.

[42] *Ibidem.*

[43] *Ibidem*

[44] *Ibidem*

b. les actes préparatoires tels la conception ou la mise à disposition de virus ou de programmes visant à développer pareils virus (§ 4).

Il suffit d'un tout petit programme exécuté sur votre ordinateur pour que les pires catastrophes arrivent. Des données se modifient toutes seules, de nouveaux fichiers apparaissent, d'autres deviennent introuvables, vous envoyez des dizaines d'emails à votre insu et encombrez le réseau ou même constatez, sans ne rien pouvoir y faire, que votre disque dur s'autodétruit. Le mal est facilement identifiable : vous avez exécuté un virus sur votre ordinateur. Cachés dans un jeu téléchargé sur Internet ou dans un fichier attaché reçu par courrier électronique, les virus –comme le ver Morris, les virus Melissa ou ILoveYou– font trembler la cyberplanète. Ils se propagent à une vitesse incroyable grâce à l'interconnexion des millions d'ordinateurs mis en réseau et, de ce fait, leurs conséquences sont incalculables. Le législateur belge s'est donc donné les armes pour lutter contre cette maladie propre à l'ère de l'informatique en punissant désormais :

> *"§ 4. Celui qui, avec une intention frauduleuse ou dans le but de nuire, conçoit, met à disposition, diffuse ou commercialise des données stockées, traitées ou transmises par un système informatique, alors qu'il sait que ces données peuvent être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique."*

La disposition qui forme le quatrième paragraphe du nouvel article 550*ter* du Code pénal a le mérite d'attaquer le mal à la racine. Le législateur a eu la clairvoyance d'incriminer non seulement le concepteur du virus, mais également toute personne qui le diffuse ou commercialise des logiciels permettant sa création. Bien sûr, et il n'en eût pas pu être autrement, un dol spécial est requis. Celui qui propage le virus à son insu (par envoi d'un e-mail auquel le virus s'est accroché, par exemple) n'est pas visé par la loi. Néanmoins, comme pour les *hackertools*, nous nous demandons si l'exigence d'un dol spécial pourra empêcher des entreprises de nuire à leurs concurrents en leur faisant des procès intempestifs pour « commercialisation de données pouvant être utilisées pour causer un dommage à des données ou empêcher, totalement ou partiellement, le fonctionnement correct d'un système informatique » lorsque les logiciels de ces concurrents se révèlent pouvoir être détournés de leur but premier pour servir d'outil de création de virus. Bien sûr le dol spécial devra encore être prouvé, il n'en reste pas moins que le danger existe. Finalement, l'on se demande aussi ce qui pourrait empêcher l'utilisation de cet article pour attaquer les entreprises qui commercialisent des logiciels contenant des *bugs* informatiques. De quoi faire réfléchir quelques « grands » de l'informatique qui lancent souvent trop tôt leur produit sur le marché…

5. La procédure pénale adaptée aux réseaux et systèmes informatiques

5.1. Problèmes de procédure particuliers à la criminalité informatique

Les problèmes pratiques et procéduraux que posent Internet et autres réseaux numériques sont multiples:

- Les procédures judiciaires sont généralement peu adéquates ou inapplicables à la poursuite des délits informatiques ou de tout délit traditionnel commis dans l'environnement numérique. S'agissant de données immatérielles, les concepts traditionnels de saisie ou de perquisition sont difficilement transposables.

- De nombreux délits informatiques se commettent de manière anonyme et les traces qu'ils laissent sont fugaces. Il est donc nécessaire de pouvoir agir vite avant que les preuves de la commission d'un délit ne disparaissent. Des moyens d'identification des auteurs des infractions sont également indispensables.

- La criminalité informatique a gagné dans le cyberespace une dimension internationale, ce qui nécessite un renforcement de la coopération inter-Etats.

- La technicité des systèmes informatiques exige que les autorités judiciaires et policières chargés de la poursuite des infractions informatiques disposent d'une expertise et de moyens particuliers.

- La nécessité de rechercher les infractions sur les réseaux électroniques, notamment en interceptant les télécommunications ou en conservant les données y relatives, constitue un risque inédit pour les droits humains et la vie privée.

La complexité de ces questions impose au législateur une prudence particulière. Nous verrons que cette prudence lui a parfois manqué dans l'adaptation de la procédure pénale aux réalités informatiques.

5.2. La saisie des données

Il n'est pas rare d'assister, en personne ou par le biais des médias, à des perquisitions qui aboutissent à la saisie des disques durs d'une entreprise ou d'un individu, dans le but de pouvoir prendre connaissance de quelques fichiers stockés en mémoire de l'ordinateur, qu'il s'agisse d'images pédophiles, de contrefaçons au droit d'auteur, de données de navigation et d'accès non autorisés à des sites et systèmes informatiques tiers. Quelle que soit la nature du délit que de telles saisies tentent à démontrer, l'enlèvement de matériel informatique lourd constitue une mesure particulièrement laborieuse pour les autorités policières et judiciaires en charge de la perquisition. En outre, la saisie de l'ensemble du matériel informatique d'une entreprise ou d'un individu peut causer des dommages irréversibles. Songeons à une entreprise de graphisme qui se verrait dépossédée de son principal outil de travail parce qu'elle est soupçonnée de détenir des copies illicites d'un logiciel ou parce que, dans l'une de ses créations, elle a utilisé sans autorisation l'œuvre d'autrui. La disproportion de la mesure de saisie dans de tels cas mène à certaines critiques. La saisie des supports peut également se révéler impraticable lorsque les données utiles à l'établissement et la poursuite de l'infraction sont disséminées dans tout le système informatique d'un entreprise. C'est particulièrement le cas lorsque l'entreprise est une multinationale et héberge des données dans des systèmes informatiques localisés dans différents Etats.

Pourtant, l'état du droit antérieur à l'adoption de la loi du 28 novembre 2000 ne pouvait que mener à de telles situations. Le Code d'Instruction Criminelle n'autorise pas la saisie de données immatérielles[45]. Seules les données stockées sur un support informatique, disquettes, CDs ou disques durs, étaient donc généralement saisies[46].

Pour remédier à ce problème, la loi insère dans le Code d'Instruction Criminelle un nouvel article 39*bis* qui autorise la copie, le fait de rendre inaccessibles et de retirer des données stockées dans un système informatique. C'est toutefois un mode particulier de saisie puisqu'il ne s'agit que de prendre copie des éléments ou d'en bloquer l'accès et non de les soustraire à leur détenteur, ce qui est généralement le cas des biens mobiliers saisis.

Les paragraphes 2 à 6 du nouvel article 39*bis* C.I.C. décrivent les différentes modalités de 'saisie' des données informatiques. En premier lieu, les données seront copiées lorsque la saisie du support n'est pas souhaitable, notamment parce que la saisie des disques durs et disquettes serait inopportune, impraticable ou disproportionnée. La copie s'étendra aux "données nécessaires pour les comprendre", en d'autres

[45] articles 35-37 et 87 du C.I.C. qui n'envisagent que le cas de "choses", "avantages patrimoniaux tirés directement de l'infraction", "papiers ou autres pièces et effets" ou encore de "tout ce qui pourra servir à la manifestation de la vérité".

[46] P. VAN EECKE, *Criminaliteit in Cyberspace*, Mys and Breesch, 1997, p. 105; Cf. cependant la décision de la Cour d'appel d'Anvers du 13 décembre 1984, *R.W.*, 1985-86, 244-246 qui autorise la saisie de données indépendamment de leur support.

termes, des clés de décryptage ou tout autre outil de décodage des données qui seraient copiées dans un format inintelligible, ou encore des logiciels qui ont servi à la création des fichiers ainsi copiés. Les copies seront réalisées sur des supports appartenant à l'autorité, hormis le cas d'urgence ou pour des raisons techniques (par exemple parce que le volume des données utiles excède la capacité de stockage des supports amenés par l'autorité), cas dans lesquels le Procureur du Roi est habilité à utiliser les supports adéquats de l'entreprise ou de l'individu qui subit la saisie.

Dans un deuxième temps, le Procureur du Roi devra rendre indisponible l'accès aux données ainsi copiées. On se retrouve là dans une hypothèse plus classique de saisie pénale qui, en principe, dépossède le saisi des biens soustraits. Il s'agit également de veiller à ce que l'original des données copiées ne soit pas altéré et puisse servir de preuve de conformité des copies effectuées pour les besoins de l'enquête. Ce blocage de l'accès aux données se substituera à la copie des données lorsque celle-ci est impossible, pour des raisons techniques ou à cause du volume des données, en vertu du §4 de l'article 39*bis*. L'inaccessibilité des données peut se réaliser de diverses manières, notamment en recourant aux techniques de cryptage.

Lorsque l'objet de la mesure forme "*l'objet de l'infraction ou a été produit par l'infraction et est contraire à l'ordre public ou aux bonnes mœurs ou constitue un danger pour l'intégrité des systèmes informatiques ou pour des données stockées"*, l'alinéa 2 du paragraphe 3 habilite le Procureur du Roi à rendre ces données inaccessibles. La différence avec l'alinéa qui précède et qui s'applique à tout type de données n'est pas évidente. Elle ressort cependant de l'histoire législative de cette disposition. Dans un premier temps le projet de loi autorisait le Procureur du Roi à retirer ces données du système informatique sans en réaliser de copie préalable[47]. De nombreuses critiques se sont élevées contre cette possibilité réservée au Parquet de détruire des données, ce qui ne peut en principe s'effectuer qu'après la confiscation prononcée par un juge du fond.

Cette possibilité de retrait a donc disparu du texte, mais les documents parlementaires indiquent que cet alinéa se distingue du précédent en ce qu'il permet l'élimination des données, lorsqu'elles sont contraires à l'ordre public et aux bonnes mœurs, tout en en conservant une copie pour la justice[48].

Des sites ou images pédopornographiques, des connections permettant des actes d'espionnage, des virus constituent des exemples de données contraires à l'ordre public ou aux bonnes mœurs ou constituant un danger pour l'intégrité des systèmes informatiques.

Dans certains cas, les données formant l'objet de la saisie particulière désormais décrite à l'article 39*bis* du Code d'Instruction Criminelle peuvent résider dans le système informatique d'un tiers. Le responsable du système informatique dans lequel ont été effectués la recherche, la copie, le retrait ou l'indisponibilité des données doit en conséquence être dûment informé et un résumé des données concernées doit lui être communiqué, ceci afin de lui permettre de demander, le cas échéant, la mainlevée de la saisie. Le Conseil d'Etat a toutefois déploré l'imprécision du terme "responsable du système informatique" et a suggéré de reprendre la définition de responsable préconisée par le Conseil de l'Europe dans la Recommandation n° R (95) 13: « la notion englobe toutes les personnes qui, lors de la perquisition ou de la saisie, paraissent disposer formellement ou réellement du contrôle sur le système informatique, objet de la perquisition »[49]. La même Recommandation invite également à informer de manière identique toute personne concernée par la saisie, même si elle n'est pas le responsable du système informatique dans lequel ces données ont été trouvées[50]. Ces tiers pourraient être les auteurs de pages web hébergées sur un serveur dont ils n'ont pas le contrôle. Dans ce cas, seul le fournisseur de l'hébergement pourrait être informé de la copie et de

---

[47] Doc. Parl. Chambre, 0213/001 & 214/001, p.63

[48] Doc. Parl. Sénat, 2-392/2, p.11

[49] *op.cit.*

[50] Sur cette question, Y. POULLET, "A propos du projet de loi dit n° 214 - La lutte de la criminalité dans le cyberespace à l'épreuve du principe de régularité des preuves ", in *Hommage à Jean Du Jardin*, à paraître, 2001.

l'inaccessibilité des données. Il nous paraît tout aussi important que la personne responsable des pages web dont l'accès aura été rendu indisponible en soit avertie.

5.3. La recherche sur les réseaux

L'article 88*ter* nouveau du Code d'Instruction Criminelle dispose :

> *" Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci, dans le cadre d'une perquisition, cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée:*
>
> *- si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche, et*
>
> *- si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus*".

S'agit-il de la transposition des règles de la perquisition aux nouvelles technologies ? Il est vrai que la disposition s'insère dans la partie du Code d'Instruction Criminelle relative aux perquisitions. Toutefois, cette recherche dans un environnement informatique crée une institution singulière dans notre procédure pénale.

L'article 88*ter* nouveau n'évoque que l'extension de la recherche informatique, comme si cette recherche elle-même était une institution bien connue de notre droit. Or de recherche dans un milieu informatique, le Code d'Instruction Criminelle n'en parle point. Le texte se contente de préciser que la recherche s'effectue lors d'une perquisition. Plusieurs auteurs assimilent cette recherche dans le système informatique à une perquisition[51]. En l'état actuel du droit, et l'adjonction de l'article 88*ter* ne viendra pas nous démentir, la recherche informatique, et par voie de conséquence son extension, ne pourra prendre place que dans le cadre d'une perquisition physique. Pas question donc pour les autorités policières et judiciaires de s'introduire dans des systèmes informatiques pour rechercher des preuves d'infraction sans un mandat dûment délivré par le juge d'instruction. Les recherches seront limitées au temps de la perquisition et ne peuvent s'effectuer qu'au départ du système informatique visé par de cette dernière.

Revenons-en à l'article 88*ter*. Deux conditions cumulatives s'imposent à l'extension de la recherche. La première exige que cette mesure soit nécessaire à la manifestation de la vérité, la seconde se compose de deux hypothèses alternatives: soit, d'autres mesures seraient disproportionnées, soit il existe un risque de déperdition d'éléments de preuve.

Suite à des critiques parlementaires, des limites "géographiques" sont apposées à "l'espace" que peut parcourir cette extension de la recherche. Seuls peuvent être visités les "*systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès*". L'objectif de cette restriction spatiale est d'empêcher une recherche illimitée dans tous les systèmes en connexion ou en relation avec le système informatique "perquisitionné", ce qui, à l'heure du *world wide web*, équivaut à une espace infini. Il n'est pas question non plus que les autorités en charge de la perquisition se transforment en *hackers* de circonstance pour accéder à des systèmes informatiques étrangers au système visité, ce que confirme par ailleurs l'exposé des

[51] D. VANDERMEERSCH, "Le droit pénal et la procédure pénale confrontés à Internet (les apprentis surfeurs) – la procédure pénale", in *Internet sous le regard du droit*, éditions du Jeune Barreau, Bruxelles, 1997, p.260; P. VAN EECKE, op. cit., p. 105; C. MEUNIER, "La loi du 28 novembre 2000 relative à la criminalité informatique", *Formation Permanente CUP*, février 2001, n°103

motifs[52]. Selon Y. Poullet, les espaces informatiques susceptibles d'être l'objet de cette extension de recherche équivalent au domicile "virtuel" c'est-à-dire "*de tout lieu où une personne a le droit de se dire chez elle, quels que soient le titre juridique de son occupation et l'affectation donnée aux locaux*"[53]. L'auteur en donne comme exemples, "*un compte bancaire accessible par un code secret, les messages vocaux ou non déposés dans une boîte électronique au nom de la personne inculpée, la base de données externe où cette dernière collecte ou range une information partagée avec d'autres*"[54].

La loi nouvelle va plus loin encore puisqu'elle autorise l'extension de la recherche dans des systèmes informatiques situés à l'étranger et permet la copie des données dans ce cas. Le juge d'instruction doit toutefois en informer sans délai le ministère de la Justice qui se met alors en contact avec les autorités compétentes de l'Etat concerné. La mesure se comprend. L'extension d'une recherche dans des réseaux informatiques mènera bien souvent à des données hébergées sur des serveurs étrangers. Toutefois, une telle atteinte au principe de souveraineté des Etats, amplement critiquée par le Conseil d'Etat et par la doctrine[55], aurait pu se faire un peu plus prudemment. Les Traités internationaux qui s'ébauchent en la matière envisagent de telles recherches internationales sur base des principes de collaboration et d'information. Le législateur belge, avant de s'arroger de tels pouvoirs, aurait pu attendre que ces conventions ou autres traités de coopérations aboutissent. La nécessité de pallier les difficultés de perquisitions et recherches transnationales en matière de cybercriminalité commande sans doute une solution législative, mais la compétence d'une telle solution relève uniquement d'un acte international.

5.4. L'obligation d'information et de collaboration des personnes connaissant le système informatique

5.4.1. Problématique et principe

Accéder aux données informatiques utiles à la recherche et à la poursuite des infractions, pouvoir en prendre copie, étendre sa recherche à de systèmes tiers ne suffit bien souvent pas. Encore faut-il pouvoir lire et déchiffrer les données saisies et copiées. L'évolution numérique est en effet telle que les données sont de moins en moins transmises en clair. La plupart des communications recourent au cryptage, les sites et systèmes informatiques se barricadent derrière des mots de passe, des identifications biométriques et d'autres outils d'accès conditionnel.

La cryptographie, sésame essentiel de la sécurité des réseaux et du commerce électronique, est aussi un outil très ambivalent. Si elle permet de garantir l'indispensable sécurité des transmissions et systèmes informatiques, ainsi que l'identification et l'authentification des acteurs, elle contribue également à l'opacité des communications et à la garantie de la confidentialité des messages. Les autorités de recherche des infractions sur les réseaux n'ont de cesse de dénoncer un usage trop généralisé de la cryptographie qui à la fois assurerait aux criminels une transmission de contenus en toute impunité et handicaperait la recherche des infractions sur les réseaux.

De tout temps, la cryptographie a été vue par les gouvernements comme une arme à double tranchant qu'il s'agissait de réglementer strictement. De l'interdiction d'exportation de moyens cryptographiques à l'imposition ou à la promotion d'un codage standardisé, les Etats-Unis ont expérimenté diverses solutions qui toutes ont échoué. L'interdiction d'exportation n'était pas viable économiquement et l'industrie n'a pas voulu d'un code imposé, voire contrôlé, par le

[52] Exposé des motifs, p. 23.

[53] Y. POULLET, *op.cit.*, n° 18.

[54] ibidem.

[55] C. MEUNIER, *op. cit.* n°121; Y. POULLET, *op.cit.*, n° 19.

Gouvernement. Le spectre d'un Big Brother était dans tous les esprits. Les propositions récentes visent soit à exiger l'intégration dans les techniques de cryptage d'une "back door" par laquelle, et à la seule condition d'un mandat juridictionnel, les autorités judiciaires pourraient s'introduire en cas de suspicion, soit une remise des moyens de décryptage par les services d'émission ou de conservation des clés de décryptage.

Cette dernière solution fait son chemin en Europe suite à la Recommandation R(95) 13 du Conseil de l'Europe qui considère que les "*autorités chargées de l'enquête devraient avoir le pouvoir d'ordonner aux personnes qui ont des données spécifiques sous leur contrôle de fournir toutes les informations nécessaires pour permettre l'accès au système informatique et aux données qu'il renferme*"[56].

La loi belge se situe en droite ligne de cette Recommandation. L'article 88*quater* qu'elle introduit dans le Code d'Instruction Criminelle dispose :

"*§1. Le juge d'instruction ou un officier de police judiciaire auxiliaire du Procureur du Roi délégué par lui, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système, dans une forme compréhensible*

§2 Le juge d'instruction peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou selon le cas de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite dans la mesure de leurs moyens".

Ces obligations sont sanctionnées pénalement dans la mesure où tout refus de coopération est puni d'un emprisonnement de six mois à un an et d'une amende de vingt-six francs à vingt mille francs.

5.4.2. Personnes tenues du devoir de coopération

La loi n'est pas très claire sur ce point[57]. Elle parle des "*personnes dont [le juge d'instruction] présume qu'elles ont une connaissance particulière du système informatique"*. Il peut donc s'agir du responsable du système informatique, d'un de ses utilisateurs principaux, du gestionnaire du réseau, du concepteur ou du fournisseur des logiciels permettant de déchiffrer les données ou des techniques de cryptage ou d'accès à celles-ci, des *trusted third parties* et autres détenteurs de clés de cryptage. L'éventail est très large. On peut même se demander si des experts en cryptographie, spécialistes de la sécurité et informaticiens qui auraient une connaissance précise de la clé de cryptage sécurisant les données litigieuses ne pourraient pas être requis par le juge de prêter leur concours à la recherche. L'approximation du texte ne s'y oppose en tout cas pas clairement; l'exposé des motifs ne le fait pas davantage[58]. Le paragraphe 2 qui impose un devoir d'intervention, le fait à l'égard de "toute personne appropriée", ce qui n'est pas plus limpide.

Par contre cette mesure ne peut être imposée à l'inculpé et à ces proches. Le législateur évite ainsi un écueil fréquent dans les lois pénales informatiques qui imposent à l'accusé de collaborer au décryptage ou déverrouillage des données saisies ou communiquées. C'est notamment le cas dans la loi néerlandaise que

---

[56] *op.cit.*

[57] L'exposé des motifs admet la largesse des termes employés qui justifie à dessein une décision du juge d'instruction au cas par cas, voir Exposé des motifs, Doc Parl. Chambre, 0213/001, p. 27.

[58] *ibidem*.

l'Ordre National des Avocats a fortement critiquée sur ce point[59]. Forcer l'accusé à fournir les pièces à conviction de son infraction enfreint en effet son droit fondamental au silence, interprété par la Cour Européenne des Droits de l'Homme comme incluant le droit de ne pas s'incriminer soi-même[60]. Les autorités judiciaires ou policières ne peuvent en conséquence contraindre la personne à remettre des documents compromettants.

Le projet de Convention Européenne ne précise pas non plus si l'inculpé est également tenu d'une telle obligation de coopération. Ses articles 14 et 15 habilitent les autorités d'investigation des infractions à enjoindre à toute personne de fournir les informations nécessaires sur le fonctionnement du système informatique dont il connaît le fonctionnement et de communiquer les données qui sont sous son contrôle. L'inculpé paraît également visé par ce pouvoir d'injonction. Le législateur européen contredirait-il sa propre jurisprudence ? Qu'il anéantisse ou réduise un droit fondamental qu'il est chargé de préserver et de défendre nous semble en tout cas extrêmement surprenant.

5.4.3. Obligations de coopération et d'intervention

Les obligations imposées à ces personnes consistent en la fourniture de toute information permettant de faire fonctionner le système ou d'y accéder. Le décryptage des données est particulièrement visé par cette disposition. Le deuxième paragraphe oblige les personnes concernées à intervenir activement pour permettre aux autorités judiciaires d'effectuer les manipulations qui leur sont désormais ouvertes par la loi telles que la recherche dans un système informatique, la copie ou le retrait des données. Il est précisé qu'il s'agit d'une obligation de moyen, précision qui n'apparaît pas pour l'obligation visée au premier paragraphe. L'exposé des motifs étend toutefois en toute logique cette qualification d'obligation de moyen au premier paragraphe.

Les personnes qui prêtent leur concours dans le cadre de cet article sont tenues au secret de l'instruction, dont la violation est sanctionnée conformément à l'article 458 du Code Pénal relatif au secret professionnel.

5.4.4. Vers une remise des clés de cryptage ?

L'exposé des motifs du projet de loi semble inclure dans les interventions qui peuvent être requises de tiers, la remise des clés de cryptage. Le texte même de l'article 88*quater* pourrait permettre au juge d'instruction d'exiger la remise de telles clés. Les concepteurs ou fournisseurs de techniques de cryptographie ainsi que les tiers de confiance ou services de *key escrow* pourraient se voir dans l'obligation de remettre les clés qu'ils détiennent.

Il importe cependant de se montrer particulièrement prudent dans cette matière et d'éviter autant que possible de convertir l'article 88*quater* en une remise systématique des clés de déchiffrement, et ceci pour deux raisons principales. La première est que la clé est susceptible de donner accès à de nombreuses données, dont certaines seulement constituent des éléments de preuves recherchés par l'instruction. Le juge ne jouit pas pour autant d'un accès légitime ou nécessaire à toutes les autres données. Il lui est cependant difficile de distinguer dans le contenu crypté les données auxquelles il lui est indispensable d'avoir accès et les autres. Le munir d'une clé de décryptage l'autorise à accéder à des données de manière disproportionnée. L'autre critique est plus essentielle. Les lois qui, dans certains pays, légitiment la remise des clés aux autorités judiciaires ne prévoient aucune obligation en terme de sécurité et de protection de ces clés. L'industrie informatique et de sécurité désapprouve généralement cette absence de toute obligation dans le chef de la police. Le risque commercial est en effet très grand pour les concepteurs de clés, et plus généralement pour la sécurité du commerce électronique, que ces clés de décryptage soient dérobées et détournées alors qu'elles sont aux mains des autorités de recherche des infractions.

---

[59] TH. A. DE ROOS, "Het concept-wetsvoorstel computercriminaliteit II", *Computerr.* 1998/2, p. 57

[60] C.E.D.H., arrêt *Saunders c. Royaume-Uni* du 17 décembre 1996. Voir F. KUTY, "L'étendue du droit au silence en procédure pénale", *Rev. Dr. Pén. et Crim.*, mars 2000, p. 330-331.

La remise des clés de cryptage doit par conséquent être limitée aux cas dans lesquels une telle mesure se révèle indispensable. Généralement, la personne dont le juge d'instruction requiert la coopération doit pouvoir s'exécuter en remettant une copie des données décryptées, et non la clé de décryptage même. Lorsque la remise des clés paraît incontournable, les autorités judiciaires et policières doivent mettre tout en œuvre pour assurer la sécurité et la confidentialité de celles-ci.

5.4.5. L'obligation de coopération dans le cadre des écoutes et de l'interception des télécommunications

Un quatrième paragraphe est ajouté à l'article 90*quater* du Code d'Instruction Criminelle pour imposer une obligation de coopération similaire aux personnes qui ont une connaissance particulière du service de télécommunications qui fait l'objet d'une surveillance ou d'une mesure d'interception. Il s'agit ici aussi de faciliter l'accès aux données de la communication sous une forme intelligible. La disposition est plus large que les dispositions existantes qui imposaient déjà le concours technique de l'opérateur du réseau ou du fournisseur du service de télécommunication, concours qui n'impliquait que de permettre le branchement des autorités policières au réseau pour la bonne fin de l'écoute. La collaboration imposée par la loi sur la criminalité informatique est d'une toute autre portée, tant en ce qui concerne les personnes visées que les actes de coopération souhaités. Ne sont plus seulement intéressés les opérateurs des réseaux, que le réseau soit téléphonique, cellulaire, satellite ou autre, mais tous les fournisseurs des services de télécommunication offerts sur ces réseaux, tels que la fourniture d'outils cryptographiques, d'accès à Internet, de services de messagerie, de forums de discussions, de chat, etc. Et outre la facilitation du branchement et des moyens d'écoute et d'interception, la loi requiert désormais une aide quant à l'accès aux données interceptées et à leur compréhension.

Le concours technique des opérateurs des télécommunications se comprend par la nécessité de conformer le système de télécommunication de manière telle que des moyens d'interception soient possibles. C'est en tout cas réalisable dans des domaines économiques, tels les télécommunications avant Internet et avant la libéralisation, lorsqu'un nombre restreint d'acteurs se partagent le marché. C'est beaucoup moins évident sur Internet où la multiplication du nombre des fournisseurs de services risque de compliquer davantage les interceptions et les modalités de coopérations des opérateurs concernés.

Les autres observations formulées pour l'article 88*quater* peuvent être appliquées ici *mutatis mutandis*.

5.5. Ecoutes téléphoniques et interception des télécommunications

La loi nouvelle complète le régime de l'interception des télécommunications réglementé par la loi du 30 juin 1994 et figurant aux articles 90*ter* à *decies* du Code d'Instruction Criminelle principalement sur deux points. D'une part, la liste des infractions autorisant la surveillance et l'interception s'étend aux infractions informatiques introduites dans le Code Pénal, ce qui répond à une logique évidente. D'autre part, la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques se voit modifiée par une obligation d'enregistrement et de conservation des données d'appel et des données d'identification d'utilisateurs de services de télécommunications. Nous ne nous appesantirons que sur cette dernière question.

5.6. L'obligation de conservation des données de télécommunications

5.6.1. Le principe

L'article 109*ter* de la loi du 21 mars 1991, dite loi Belgacom, impose désormais aux opérateurs de réseaux de télécommunications et aux fournisseurs de services de télécommunications, sous peine de sanctions pénales, "*d'enregistrer et de conserver, pendant un certain délai en vue de l'investigation et de la poursuite d'infractions pénales, (...) les données d'appel de moyens de télécommunications et les données d'identification d'utilisateurs de services de télécommunications*".

La loi tente ainsi de répondre à une des difficultés essentielles de la poursuite d'infractions commises sur les réseaux de télécommunications, celle de l'identification de l'auteur du délit, problème amplifiée par l'anonymat potentiel qui caractérise les réseaux numériques.

5.6.2. Les sujets de l'obligation de conservation

La disposition nouvelle se distingue une fois de plus par le largesse des termes utilisés pour définir les personnes astreintes à une obligation pénalement sanctionnée. Il s'agit de nouveau des "opérateurs de réseaux de télécommunications et fournisseurs de services de télécommunications". Nous avons déjà eu l'occasion de commenter ce terme. Mais il va sans dire que l'inquiétude que nous avons exprimée quant à la multitude et à la diversité des acteurs que ce vocable recouvre, s'amplifie encore lorsqu'on parle d'une obligation permanente et détachée de toute recherche spécifique d'une infraction. En effet, la coopération technique dont nous avons parlé plus haut n'intervient que dans le cadre d'une investigation précise et déterminée. L'obligation dont il est question ici est d'une portée bien plus large. La conservation des données doit se faire indépendamment de toute poursuite, de manière générale, indifférenciée et, le mot est malheureusement à la mode, pro-active.

Non seulement, les opérateurs de réseaux de téléphone, de téléphonie mobile ou d'Internet devront conserver les données relatives aux appels, communications et connexions, mais également tout prestataire de services délivrés par ces réseaux, ce qui englobe, nous le répétons, les fournisseurs d'accès Internet, de courriers électroniques, de forums de discussions, de *chat*, de services de cryptographie ou de conservation des clés, etc… La définition donnée par la Recommandation R(95) du Conseil de l'Europe, à laquelle renvoient d'ailleurs les travaux préparatoires de la loi, est excessivement large : le fournisseur de services s'y entend de "*quelqu'un qui offre de transférer et d'acheminer des données sur un réseau de télécommunications entre un client et un nombre indéfini de tiers, défini par le client lui-même*"[61]. Ce qui permet d'englober, selon nous, les fournisseurs de moyens de paiement électroniques, de services d'anonymisation, ainsi que les intermédiaires du type Napster qui fournissent les moyens d'envoyer des données musicales ou autres à un nombre indéfini de personnes.

Les opérateurs de réseaux privés semblent tout autant concernés que les opérateurs et prestataires de services dans les réseaux publics.

5.7. L'objet de l'obligation de conservation

Tous ces acteurs sont désormais tenus de conserver, durant un certain délai, toutes les données d'appel et d'identification des utilisateurs recourant à leurs services. Ce qui appelle plusieurs remarques :

- Les cas dans lesquels cette obligation prendra place, ainsi que le type de données concernées doivent encore être déterminés par Arrêté Royal. S'agissant d'une restriction à la vie privée des personnes, nous regrettons, avec d'autres auteurs[62], que ce pouvoir n'ait pas été laissé à la loi, conformément au prescrit de la Convention Européenne des droits de l'homme.

- Les données d'appel et d'identification sont un concept très peu défini. L'exposé de motifs évoque, quant aux données d'appel, les données relatives à l'origine, la destination, la durée, la localisation des appels[63]. Transposés à l'environnement numérique, ces exemples

[61] Conseil de l'Europe, Problèmes de Procédure Pénale liés à la technologie de l'information, Recommandation R(95) 13, Exposé des motifs, p. 61

[62] Y. POULLET, op. cit., n°35. Le Conseil d'Etat a également été dans le même sens, voir Avis, *op. cit*., p. 56.

[63] Doc. Parl. Chambre, 0213/001, p. 30.

recouvrent également les adresses IP des ordinateurs émetteurs et récepteurs de la communication, le début et la fin de la connexion afin de pouvoir relier cette adresse IP à un utilisateur précis, le *log book* des prestataires de services, les adresses des sites visités, voire la durée de ces visites, les adresses emails des messages échangés, tant de l'émissaire que du destinataire. Nombre de ces données recoupent des éléments permettant d'identifier l'utilisateur de services. Mais les données d'identification de l'utilisateur visées par la loi recoupent également, selon nous, les mots de passe utilisés, l'identification des personnes relativement aux moyens de paiement concernés, lorsque le sujet de l'obligation de conservation est un prestataire de ces paiements électroniques, l'identité et adresse physique de l'abonné, l'identité réelle de la personne se cachant derrière un email ou une connexion anonyme.

♦ La plupart de ces données constituent, cela va sans dire, des données personnelles protégées par la législation belge relative à la vie privée. Or, la loi est relativement silencieuse sur l'application des principes de protection des données à cette obligation de conservation. L'oubli (ou l'abstention délibérée ?) de consulter la Commission de Protection de la Vie Privée dans la préparation du projet de loi est, à cet égard, très révélateur. La Commission, s'étant finalement invitée aux débats, a très vivement critiqué ce texte[64], arguant notamment que cette conservation de données se réalisait hors de tout principe de proportion essentiel à la collecte et au traitement de données personnelles. De manière plus générale, c'est l'instauration d'une surveillance policière généralisée et visant tout utilisateur d'un service de télécommunications qui fut reprochée au projet de loi. Que l'avis de la Commission soit désormais requis pour déterminer le type de données et le délai de conservation ne suffit pas à nous rassurer. Si la directive européenne sur la protection permet des dérogations à la limitation des collectes des données personnelles, précisément dans le cas de prévention, la recherche, la détection et la poursuite d'infractions pénales[65], cela ne donne pas un blanc-seing pour établir une surveillance exploratoire et pro-active des télécommunications, qui est en violation flagrante des principes de la Convention Européenne des Droits de l'Homme[66].

♦ L'accès au contenu des communications constitue une atteinte à la protection de la vie privée bien plus problématique que l'accès aux données de trafic ou d'appel. Les nouvelles technologies obscurcissent cependant la distinction entre les deux types de données et la rendent en tout cas plus délicate à tracer. Les exemples que nous avons donnés de données d'appel démontrent combien certaines informations glissent de l'identification de l'appel à l'identification du contenu. Il s'agit de veiller particulièrement à ce que de tels glissements soient évités ou à tout le moins entourés de garanties particulières.

♦ Le délai de conservation des données fut l'un des points les plus controversés lors des débats parlementaires. Il fut finalement décidé de laisser la fixation de ce délai au Roi après avis de la Commission de la Protection de la Vie Privée, tout en précisant que ce délai ne peut être inférieur à douze mois. A titre de comparaison, le délai conseillé par le Groupe de Protection des personnes physiques à l'égard du traitement des données à caractère personnel institué par la Commission Européenne, est de trois mois seulement. Ce délai de trois mois nous paraît à la fois déraisonnable et impraticable. De nombreux mois sont susceptibles de s'écouler entre la commission d'une infraction et sa recherche effective. Un certaine lenteur prudente de la procédure permet d'ailleurs de garantir le respect des droits des personnes. En outre, la situation de l'arriéré judiciaire et l'encombrement des juges d'instruction en Belgique est telle qu'on ne peut imaginer que des services de police puissent obtenir dans les trois mois de la commission de l'infraction un mandat leur permettant d'accéder aux données conservées par les opérateurs de télécommunications. La solution de la loi belge semble pour le moins raisonnable.

---

[64] Avis de la Commission de la Protection de la Vie Privée, Doc. Parl. Chambre, 0213/004.

[65] Directive 95/46, article 13

[66] Y. POULLET, *op.cit.*, n°33.

♦ Les conditions d'accès aux données ainsi conservées par les autorités policières et judiciaires ne sont pas autrement explicitées dans la loi. Or la protection de la vie privée requiert que cet accès aux données conservées par les opérateurs ne se réalise qu'au cas par cas et dans des conditions strictes de légalité[67].

♦ On peut également se demander dans quelle mesure cette obligation de conservation des données s'articulera avec la transposition belge de la directive sur le commerce électronique qui, au titre des dispositions relatives à la responsabilité des intermédiaires, exclut une obligation générale de surveillance. Bien sûr, il y a un pas de la conservation automatique des données à la surveillance active du contenu du réseau. Toutefois, la loi sur la criminalité informatique a pour résultat de sanctionner pénalement les intermédiaires qui ne procéderaient pas au stockage des données, qui permet une surveillance du réseau.

♦ L'obligation de conservation des données pose également un problème de coût très important. Les fournisseurs de services Internet, petites ou grandes entreprises, devront assumer le coût du stockage des données, de la formation de personnel, de la conformation de leurs services afin de pouvoir conserver les traces nécessaires, etc. Dans d'autres pays, les prestataires de services se sont déjà rebellés contre cette imposition d'un coût inattendu dans leurs activités[68]. Ils se sont jusqu'à présent peu manifestés dans le débat belge, mais tout laisse entrevoir que cette question finira par surgir…

5.8. L'application de la loi du 28 novembre 2000 aux infractions classiques et notamment aux contrefaçons

Les dispositions introduites par la loi sur la criminalité informatique s'appliquent à toutes les infractions, classiques ou spécifiques à des agissements informatiques. Dès lors, la saisie, la recherche sur les réseaux, l'extension de la recherche et l'intrusion collatérale dans des systèmes informatiques tiers, l'imposition d'obligations de coopération de la part de certaines personnes sont des avancées procédurales qui bénéficieront à de nombreux types de délit, et notamment aux contrefaçons de droit d'auteur et droits voisins commises dans l'environnement numériques. Seules les mesures d'interception de télécommunications sont limitées à un liste exhaustive d'infractions dans laquelle la contrefaçon en matière de propriété intellectuelle n'apparaît pas.

Un juge d'instruction chargé d'un dossier relatif à une contrefaçon, qu'il s'agisse de logiciels pirates, de liens vers des fichiers MP3[69], de chargement de musique via Napster, se verra doté d'un arsenal de mesures de recherche particulières allant notamment jusqu'à la possibilité de demander les données de communications conservées par tout prestataire de services sur Internet ou presque. Il va sans dire que la protection du droit d'auteur sur les réseaux s'en voit indirectement renforcée. Nous ne pourrions que nous en réjouir si nous ne gardions pas présentes à l'esprit les critiques formulées ci-avant sur les nombreuses approximations et disproportions de ces dispositions procédurales.

---

[67] Groupe de protection des personnes à l'égard du traitement des donnés à caractère personnel, Recommandation 3/99 relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit, Adoptée le 7 septembre 1999.

[68] Voir ECLIP Workshop on interception of computer crime, 24 Janvier 2001, Londres, présentations disponibles sur le site <http://www.jura.uni-muenster.de/eclip>

[69] Notre but n'est pas de trancher la question de la licéité des hyperliens vers du contenu pirate, mais uniquement de constater que de telles pratiques ont déjà fait l'objet en Belgique de plaintes pénales, voire de poursuites.

Conclusion

Elaborer une loi relative à la criminalité informatique n'est pas chose facile. Le législateur se trouve entre deux écueils : des termes trop vagues induisent une criminalisation excessive ou englobent des comportements non coupables; une terminologie trop précise ou trop liée à la réalité technique du moment risque de vieillir prématurément la loi, de ne pas lui permettre de passer le cap du développement technique.

Le législateur belge s'est trouvé pareillement entre Charybde et Scylla et la loi s'en ressent. Trop souvent, le choix s'est porté sur la nécessité de la neutralité technologique pour que la loi s'adapte sans mal à l'évolution technique. L'imprécision de certaines définitions, leur absence parfois, le démontrent. On parle ainsi de "représentations de l'information", d' "usage quelconque d'un système informatique", de "personnes dont on présume qu'elles ont une connaissance particulière du système informatique", "rechercher des données permettant de commettre une infraction", de "fournisseurs de services de télécommunications", notions extrêmement larges susceptibles de recouvrir tout et n'importe quoi. Aucune raison ne justifie l'absence de définitions de "systèmes informatiques", de "données informatiques". Or une loi pénale se doit d'être particulièrement claire et précise. A force de vouloir rendre la loi adaptable, on l'a rendu malléable, extensible à des situations que le législateur n'a sans doute pas entendu criminaliser.

On peut également regretter l'absence d'un dol spécial, d'une intention frauduleuse en ce qui concerne l'infraction d'accès non autorisé aux systèmes informatiques, ce qui ouvre la porte à l'incrimination de la simple curiosité; de la recherche ou d'autres types d'accès totalement légitimes. Dans certains cas, nous avons également souligné la rupture du principe d'égalité entre les infractions traditionnelles et leur correspondant dans l'environnement informatique.

Il reste à voir comment les tribunaux appliqueront cette loi. On compte sur leur clairvoyance et leur discernement pour gommer les quelques aspects de la loi que cet article a critiqués. Quoiqu'il en soit, la loi répondra enfin à l'impunité dont jouissaient les criminels informatiques dans notre pays et permettra de réprimer plus effectivement les crimes commis sur les réseaux.

Mais le travail du législateur ne devrait pas s'arrêter là. La répression n'est pas tout. La meilleure réponse à la criminalité informatique implique d'investir plus largement dans la sécurité des systèmes et réseaux informatiques, considérablement sous-estimée par les entreprises, les individus et par l'Etat. La vulnérabilité des systèmes informatiques actuels, *hardware* et *software* confondus, est telle que les *hackers* plaident souvent la provocation. La Communication Européenne abonde dans le sens d'une action préventive et envisage d'augmenter les fonds de la recherche en la matière. Le Gouvernement belge pourrait également décider de développer la recherche scientifique, universitaire et privée en matière de cryptographie et de sécurité informatique. Un tel effort compléterait idéalement la loi du 28 novembre 2000 et propulserait finalement la Belgique dans les premiers de la classe.

SéverineDusollier
severine.dusollier@fundp.ac.be

Florence de Villenfagne
florence.devillenfagne@fundp.ac.be